MEINBERG
RADIO CLOCKS

Technical Information
Operating Instructions

LANTIME / PZF

ETX 1HE V4

Impressum

Werner Meinberg
Auf der Landwehr 22
D-31812 Bad Pyrmont

Telefon: +49 (0) 52 81 / 9309-0
Telefax: +49 (0) 52 81 / 9309-30

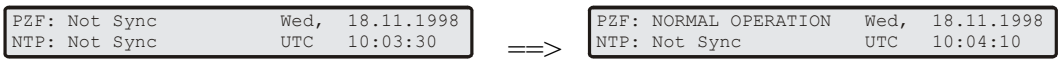
Internet: **http://www.meinberg.de**
Email: **info@meinberg.de**

10. Juni 2004

Table of Contents

Quick Start

- Approximately one minute after power up no display will be shown. After that the current state of the PZF receiver and the NTP will be displayed.



- If the PZF receiver remains asynchronous (FAIL LED is still on after 3 minutes) the Field and the Correlation (at least 60, optimum 75) are to check (press MENU once). The antenna has to be installed with the longer side to direction of Frankfurt in Germany.

- Enter TCP/IP address, netmask and default gateway:
  - Press Menu three times to enter the LAN PARAMETERS setup menu
  - Press CLR/ACK to see the TCP/IP address first

  - Press CLR/ACK once again to be able to enter the IPv4 TCP/IP address
  - With NEXT the respective digit is to select while INC is used to set the value
  - To take over the changes it is necessary to press CLR/ACK again
  - A wildcard '*' is displayed to confirm the changes
  - Pressing NEXT, the netmask and the default gateway can be entered in the same way.
  - Pressing MENU following by INC causes the changes to become active

NOTE: all 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”

Network Timeserver with GPS synchronized time base

LANTIME (Local Area Network Timeserver) provides a high precision time base to a TCP/IP network (Stratum-1-Server). The NTP (Network Time Protocol) is used to synchronize all NTP clients with the reference. The several LANTIME variants differ from each other by the time reference. A GPS receiver, a DCF77 receiver or an IRIG time code receiver can be integrated as an internal reference as well as a combination of this references (hybrid system). External references are also possible. LANTIME/PZF is a set of equipment composed of a DCF77 correlation receiver PZF509, a single-board computer with integrated network board and a power supply, all installed in a metal 19" modular chassis and ready to operate. A simplified LINUX operating system is installed on the single-board computers flash disk. Four push buttons and a 2 x 40 character LC display can be used to configure and monitor the time server. After the network connection has been established the time server can also be configured and monitored remotely from a workstation via TELNET or FTP. An integrated HTTP server enables access to the LANTIME by using an ordinary WEB browser.
Network Time Protocol (NTP)

NTP is a common method for synchronization of hardware clocks in local und global networks. The basic concept, version 1 [Mills88], was published in 1988 as RFC (Request For Comments). Experiences made from the practical use in Internet was followed by version 2 [Mills89]. The software package NTP is an implementation of the actual version 3 [Mills90], based on the specification RFC-1305 from1990 (directory doc/NOTES). Permission to use, copy, modify and distribute this software for any purpose and without fee is hereby granted (read File COPYRIGHT).

NTPs way of operation is basically different from that of most other protocols. NTP does not synchronize all connected clocks, it forms a hierarchy of timeservers and clients. A level in this hierarchy is called a *stratum*, and stratum-1 is the highest level. Timeservers of this level synchronizes themselves by a reference time source, such as a radio controlled clock, GPS-receiver or modem time distribution. Stratum-1-Servers distribute their time to several clients in the network which are called stratum-2.

A high precision synchronization is feasible because of the several time references. Every computer synchronizes itself by up to three valued time sources. NTP enables the comparison of the hardware times and the adjustment of the own clock. A time precision of 128ms, often better than 50ms, is possible.

NTP Target

The software package NTP was tested on different UNIX systems. Many UNIX systems have pre-installed a NTP client. Only some configurations have to be made (/etc/ntp.conf - see NTP Client Installation). NTP clients as freeware or shareware are also available for the most other operating systems like Windows XP/2000/NT/95/98/3x, OS2 or MAC. The following WEB site is recommended to get the latest version of NTP: "http://www.eecis.udel.edu/~ntp/". More information you can find on our web page at "http://www.meinberg.de/english/sw/ntp.htm".

NTP-Client Installation

The following example shows the installation of a NTP client under UNIX. First make sure that there is no NTP installed on your computer because many UNIX operating systems include NTP already.

The shipped source code of the NTP daemon has to be compiled on the target system. Using the enclosed script file configures the compilation of the NTP daemon and all tools.

```
configure
```

All necessary information from the system will be collected and the corresponding make files will be generated in the subdirectories.

After that the NTP daemon and all needed utilities will be generated. Therefore type:

```
make
```

While compiling the NTP daemon several warnings may appear. This warnings are mostly unimportant. In case of problems during the compilation read the system dependent notes in the subdirectory ‘html’.
Afterwards the generated programs and tools have to be moved in the corresponding directories. Therefore type:

```
make  install
```

The time adjustment can occur in different ways. Either the system time can be set once by using the tool "ntpdate lantime" or the NTPD daemon is started. In the first case it is recommended to set the time automatically with "cron" or once when booting the system. The second case is described below.

First a file named /etc/ntp.conf has to be generated with an editor. Adapting the file to Meinberg LANTIME it should contain the following:

```
# Example for /etc/ntp.conf for Meinberg LANTIME
server 127.127.1.0              # local clock
server 172.16.3.35              # TCPIP address of LANTIME
# optional: Driftfile
# driftfile /etc/ntp.drift
# optional: activate all messages in syslogfile
# logconfig =all
```

The NTP daemon is started with "ntpd" or, using "rc.local", while booting the system. Status messages during operation are saved in /var/adm/messages and /var/adm/syslog (corresponding to the syslog configuration).

e.g.: **tail /var/log/messages**

shows the last lines from the file "messages"

The status messages can also be redirected in a log file by using the following option:

ntpd -llogfile

The command "ntpq" in the directory "ntpq" requests the actual status of the NTP daemon (see also doc/ntpq.8).

e.g.: **ntpq/ntpq**

An interpreter appears; Type "?" for a list of all available commands. The command "peer" is used to list all active reference clocks:

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	.PPS.	0	l	36	64	1	0.00	60.1	15875

with the following meaning:

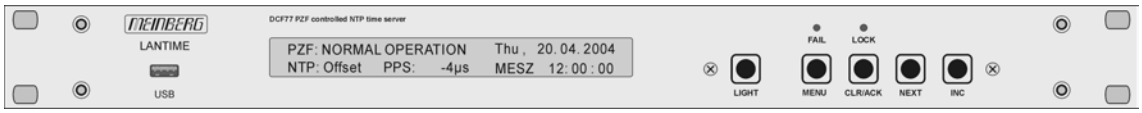
- remote: list of all valid time servers (ntp.conf)
- refid: reference number
- st: actual stratum value (hierarchy level)
- when: last request (seconds)
- poll: period of requesting the time server (seconds)
- reach: octal notation of the successful requests, shifted left
- delay: delay of the network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

Repeatedly "peer" commands lets the user observe the accuracy of the NTP daemon. Every 64 seconds (value of -poll) a new time string is red in from the radio clock. The NTP daemon needs approx. 3...5 minutes for initialisation. This is indicated by a wildcard (*) on the left side of the remote name.

The NTP daemon terminates itself if the system time differs from the UTC time by more than 1024 seconds. This often happens when the time zone is not correctly set (see also system manual "zic" or "man zic").

The Modular System LANTIME

LANTIME is a set of equipment composed of a DCF77 PZF controlled clock PZF509, a single-board computer SBC GEODE 266MHz with integrated network card, and a power supply unit T60B, all installed in a metal desktop case and ready to operate. The interfaces provided by LANTIME are accessible via connectors in the rear panel of the case. Details of the components are described below.



Front View LANTIME/PZF

The implemented NTPD distributes the reference time from the DCF77 PZF 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 LANTIME is very easy for the system/network administrator. The network address, the netmask and the default gateway have to be configured by the front panel of LANTIME. The network address or the equivalent name of LANTIME has to be announced to all NTP clients in the TCP/IP network.

Among NTP the Linux system supports also a number of further network protocols: HTTP(S), FTP, SSH and Telnet. Because of this remote configuration or status requests may occur via 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 emails 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 LANTIME NTP servers can be installed in the same network to obtain redundancy.

Supported Network Services

The following network services are provided via RJ45 10/100Base-T Ethernet (Auto sensing):

- NTP v2, v3, v4
- NTP broadcast mode
- NTP multicast
- NTP symmetric keys
- NTP Autokey
- Simple Network Time Protocol (SNTP)
- TIME
- SNMP v1,2,3 with extended SNMP-Agent and SNMP-TRAPs for NTP and reference clock status
- DHCP Client
- NFS
- TELNET
- FTP
- HTTP
- HTTPS with Openssl2
- SSH2 Secure Shell Login
- Alarm messages via mail
- IPv6
  - 3 global IPv6 addresses configurable
  - Autoconf Feature to be disabled
  - supported network services: NTP, HTTP, HTTPS, SNMP, SSH
- Windows „net time“ via NETBIOS
- Winpopup (Window Mail)

Additional Features and Options

- external NTP timeserver
- free configuration of NTP: thereby MD5 authentication and access control via address & mask restriction
- extended menu guidance for configuration and monitoring via Telnet, SSH or serial terminal interface
- optional up to 3 RJ45/10/100Mbit Ethernet interfaces
- extended HTTP statistic support with long-term graphic and access statistic to NTP
- alarm messages can be displayed on external large display VP100/20/NET
- USB memory stick slot for extended functionality: software update, transfer of secure certificates, log files and configurations, keypad locking

User Interface

- terminal connection via serial interface, status LED
- Web browser interface with graphical statistic of the one-day cycle offsets
- Telnet or Secure Shell Login for password protected operation of the Linux operating system
- FTP access for updating the operating system and downloading log files
- Simple Network Management Protocol for automatically SNMP Traps in case of alarm
- SYSLOG messages can be passed to different computers
- configurable email notification
- Simulation of a synchronous radio clock in order to operate without antenna

Options

- up to two further Ethernet RJ45 connectors
- Frequency and pulse outputs via BNC connectors (e.g. 10MHz, 2.048MHz, PPS)
- higher free running accuracy because of optional oscillators (OCXO-MQ, OCXO-HQ)
- IRIG-B outputs
- ANZ14/NET or VP100/20/NET as display connected via network

Why to use a Network Timeserver

A network timeserver should be used if accurate time is essential for undisturbed operation. In fact it is possible to synchronize the own computers via timeservers in the internet, bur for several reasons an own timeserver is to favour:

- the possibility to send notification via email or SNMP trap to an administrator in case of any synchronisation failure.
- the computers in the own network do not depend on a reliable internet connection
- the computers in the own network do not depend on the availability of an external timeserver. The most operators of internet timeservers do not guarantee neither a continuous availability nor the accuracy of their service.
- NTP is able to compensate the propagation delay of the network packets only in case of “usual” internet traffic. However, if unforeseen occurrences cause badly fluctuating propagation times it is possible that the time synchronisation is essential disturbed. Reasons for this may be: hacker attacks, numerous upcoming new viruses etc.
- an own timeserver can not be compromised externally as easily.

General information DCF77 PZF

The German long wave transmitter DCF77 started continuous operation in 1970. The introduction of time codes in 1973 build the basic for developing modern radio remote clocks.

The carrier frequency of 77.5kHz is amplitude modulated with time marks each second. The BCD-coding of the time telegram is done by shifting the amplitude to 25% for a period of 0.1s for a logical '0' and for 0.2s for a logical '1'. The receiver reconstructs the time frame by demodulating this DCF-signal. Because the AM-signal is normally superimposed by interfering signals, filtering of the received signal is required. The resulting bandwidth-limiting causes a skew of the demodulated time marks which is in the range of 10ms. Variations of the trigger level of the demodulator make the accuracy of the time marks worse by additional +/-3ms. Because this precision is not sufficient for lots of applications, the PTB (Physical and Technical Institute of Germany) began to spread time information by using the correlation technique.

The DCF-transmitter is modulated with a pseudo-random phase noise in addition to the AM. The pseudo-random sequence (PZF) contains 512 bits which are transmitted by phase modulation between the AM-time marks. The bit sequence is build of the same number of logical '0' and logical '1' to get a symmetrical PZF to keep the average phase of the carrier constant. The length of one bit is 120 DCF-clocks, corresponding to 1,55ms. The carrier of 77.5kHz is modulated with a phase deviation of +/-10° per bit. The bit sequence is transmitted each second, it starts 200ms after the beginning of an AM second mark and ends shortly before the next one.

Compared to an AM DCF77-receiver, the input filter of a correlation receiver can be dimensioned wide-bandwidth. The incoming signal is correlated with a reconstructed receiver-PZF. This correlation analysis allows the generation of time marks which have a skew of only some microseconds. In addition, the interference immunity is increased by this method because interference signals are suppressed by averaging the incoming signal. By sending the original or the complemented bit sequence, the BCD-coded time information is transmitted.

The absolute accuracy of the generated time frame depends on the quality of the receiver and the distance to the transmitter, but also on the conditions of transmission. Therefore the absolute precision of the time frame is better in summer and at day than in winter and at night. The reason for this phenomenon is a difference in the portion of the sky wave which superimposes the ground wave. To check the accuracy of the time frame, the comparison of two systems with compensated propagation delay is meaningful.

Features of PZF509

The PZF509 is a high precision receive module for the DCF77-signal build in euro card size (100mm x 160mm).

The micro controller of the system correlates its receiver-PZF with the incoming pseudorandom sequence and decodes the time information of the DCF-telegram simultaneously. The controller handles input and output functions of the PZF509 and synchronizes the internal real-time clock.

By evaluating the pseudorandom phase noise, the PZF509 is able to generate time frames with thousand times the accuracy of standard AM-time code receivers. The precise regulation of the main oscillator (TCXO, OCXO optional for higher accuracy) of the radio clock is possible therefore. So, the PZF509 can be used as a standard frequency generator besides the application as a time code receiver. Six fixed and one settable TTL-level standard frequencies are available at the rear VG-connector. The synthesizer frequency exists as an open drain output and a sine wave signal also.

The PZF509 delivers TTL-low and TTL-high active pulses per minute and per second further. To distribute information concerning date, time and status, two independent serial interfaces (RS232) are used which are configurable in a setup menu.

Like mentioned before, the PZF509 includes a battery-backed real-time clock which runs crystal-precise if the main power supply fails.

Important system parameters are stored in a battery-backed (RAM of the RTC) or non-volatile (EEPROM) memory.

If an update of system software becomes necessary, the new firmware can be loaded via serial interface (COM0) without removing the PZF509 for inserting a new EPROM.

Antenna

The PZF509 operates with a ferrite antenna which is damped to match the bandwidth needed for the correlation reception.

Assembly of antenna

The antenna has to be mounted as exactly as possible. Turning it out of the main receive direction will result in less accurate time frames. The antenna must be placed in longitudinal direction to the DCF-transmitter (Frankfurt). The nearness to microcomputers should be avoided and the antenna should be installed with a minimum distance of 30cm to all metal objects, if possible. A distance of several meters to TV- or computer monitors must be kept.

After switching the PZF509 to the menu 'PZF STATE', the adjustment of the antenna can be executed. The displayed value is proportional to the received field strength. The best method of mounting the antenna is to look for the minimum field strength and turn the antenna by 90° to maximum then. A high field strength on its own is no guarantee for good conditions of reception, because interfering signals within the bandwidth of the receiver also have an effect on the displayed value.

The maximum interference immunity can be found by looking at the autocorrelation coefficient (in percent) in the menu 'PZF-STAT'. The displayed value should be close to 75% for best reception.

Booting the DCF77 PZF receiver

If both the antenna and the power supply have been connected the system is ready to operate. About 10 seconds after power-up the receiver´s TCXO has warmed up and operates with the required accuracy. This is indicated by alternated blinking of the two LEDs in the front panel. This blinking stops after the single board computer is already booted.

Booting the Single Board Computer

The LINUX operating system is loaded from a packed file on the flash disk of the single board computer to a RAM disk. All files of the flash disk are stored in the RAM disk after booting. Because of that it is guaranteed that the file system is in a defined condition after restart. This boot process takes approx. one minute. After the LINUX system has started up already the network function is initiated and the driver software LANTIME is started. This driver tries to get a valid time from the PZF reference clock in order to set the LANTIMEs clock. If PZF clock is not connected the LANTIME is waiting for a valid time.

```
waiting for refclock on COM1
with 9600 Baud 7E2
```

After starting up the LINUX system the network function is initiated and the program for communication with the PZF and the NTPD (NTP daemon) is started. After that NTPD starts synchronisation with the reference clocks (usual the hardware clock of the single board computer and the DCF77 PZF receiver). Until synchronisation is finished the following message is displayed:

```
PZF: NORMAL OPERATION   Wed,  18.11.2002
NTP: Not Sync           MEZ   10:04:10
```

For the synchronisation of the NTPD with the PZF it is necessary that the DCF77 PZF receiver is synchronous with the DCF77 time (XTAL LED is turned off). In this case the following message is monitored on the display:

```
PZF: NORMAL OPERATION   Wed,  18.11.2002
NTP: Offset PZF:  1ms   MEZ   10:04:10
```

The second line shows the user that the NTPD is synchronized with the PZF with an offset of -1ms. Because of the internal time of the NTP which is adjusted by a software PLL (phase locked loop) it takes a certain time to optimise this offset. The NTPD tries to keep the offset below ±128ms; if the offset becomes to large the system time is set with the DCF77 time. Typically values for the offset are +-5ms after the NTPD has already synchronized.

Configuration User Interface

There are several ways to configure the LANTIME parameters:

Command Line Interface (CLI) via TELNET
Command Line Interface via SSH
Command Line Interface via serial interface terminal (BGT versions only)
HTTP Interface
Secure HTTP Interface (HTTPS)
Front panel LCD Interface
SNMP Management

To put LANTIME into operation for the first time an IP address is to enter via the front panels keys and LC display (refer to: DHCP IPv4 or AUTOCONF IPv6). LANTIME variants without LC display have to be given the IP address via the serial interface in the front panel, running a terminal software e.g. on a laptop. If once the IPv4 address, netmask and IPv4 GATEWAY is configured, or the network interface is initialised by IPv6 SCOPE-LINK, the LANTIME is accessible from any computer in the network (remote).

To set up a TELNET connection the following commands are to enter:

telnet 198.168.10.10 // LANTIME IP address
user: root
password: timeserver

With “setup” the configuration program is to start.

To set up a SSH connection the following commands are to enter:

ssh root@198.168.10.10 // LANTIME IP address
password: timeserver

With “setup” the configuration program is to start.

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

http://198.168.10.10 // LANTIME IP address
password: timeserver

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

https://198.168.10.10 // LANTIME IP address
password: timeserver

Configuration via LC Display

In case of the first installation of LANTIME the network parameters can only be configured by the front panels push buttons and the LC display. Press MENU as often until the SETUP menus appear on the display. The first setup menu are the LAN PARAMETERS. Pressing NEXT further setup menus appear. Pressing CLR/ACK the LAN PARAMETERS menu is entered. The submenu TCP/IP ADDRESS appears. Pressing NEXT the following submenus can be chosen: NET MASK, DEFAULT GATEWAY, IPv6 address, HOSTNAME, DOMAINNAME, NAMESERVER and REMOTE CONNECT. CLR/ACK lets the user enter the corresponding submenu to make changes with NEXT and INC. Pressing CLR/ACK after changing parameters acknowledges the changes. Leaving the menu with MENU all changes are discarded and the setup menu is displayed again. All changed settings of the LAN PARAMETER's sub menu come into affect not before MENU is pressed once again and the changes are confirmed.

The unique 32 bit TCP/IP address must be set by the network administrator. The net mask will be defined by the network. Possibly it is necessary to set the default gateway also.

The correct connection to the LANTIME can be reviewed from any other workstation in the network with the program PING.

REMOTE CONNECT lets the user enable or disable all connections via network (e.g. TELNET, FTP or HTTP). If changes occur via HTTP interface or setup program the message "REMOTE CONNECT: partial enabled" may appear. The NTP protocol will restarted after any change.

NOTE: Any HTTP, HTTPS, SSH or TELNET connection to the LANTIME is possible only if REMOTE CONNECT is enabled!

.

The Front Panel Layout

Field LED

The 'Field'-LED is switched on if a DCF-signal with at least minimum field strength needed for the correlation reception is detected at the input of the receiver.

Xtal LED

If the 'Xtal'-LED is on, it was not possible to synchronize the internal real-time clock to DCF-time. This condition occurs for at most two minutes after switching on the PZF509, because two DCF-telegrams are checked for plausibility before the data is taken over. Short disturbance of reception can cause this state too.

LC Display

The 2 x 40 character LC display is used to show the receiver's status and let the user edit parameters. The keys described below let the user select the desired menu. The next chapter lists all available menus in detail. A quick reference of the available menus and submenus can be found at the end of this document.

MENU Key

This key lets the user step through several display menus showing specific data.

CLR/ACK Key

This key has to be used when parameters are to be modified. When this key is pressed the parameters that have been edited are saved in the battery buffered memory. If the menu is left without pressing CLR/ACK all changes are discarded.

NEXT Key

When editing parameters (LCD cursor is visible) this key moves the cursor to the next digit rsp. to the next parameter to be edited. If the current menu just displays data (cursor not visible) pressing this key switches to a submenu (if available).

INC Key

When editing parameters this key increments the digit or letter at the cursor position.

The menus in Detail

Root Menu

The root menu is shown when the receiver has completed initialisation after power-up. The left side of the first line of the display shows the receiver's mode of operation as described above. If the antenna is disconnected or not working properly, the text "ANTENNA FAULTY" is displayed instead. The second line shows the offset of this reference clock to the local time (in this example the offset is 1ms).

```
PZF: NORMAL OPERATION   Wed,  18.11.2002
NTP: Offset GPS: -1ms   MEZ   10:04:10
```

On the right side of the display the current date, the name of the time zone (the time zone is always UTC) and time is monitored. If the "SYNC Simulation" option is enabled an "*" will be shown behind the time.

If the NEXT key is pressed from the root menu a submenu is displayed showing the receiver's software revision of the LANTIME software and the PZF509 flash software:

```
LANTIME:4.05  SN:000000000000
PZF509 :4.02  SN:9008890
```

If the NEXT key is pressed twice from the root menu a submenu is displayed showing the NTP software version, the operating system version and the MAC address of the integrated net card.

```
   NTP:4.0.99f  OS:2.2.14.06
   HWaddr: 00:00:00:00:00:00
```

Pressing NEXT the third time the fingerprint of the SSH key is displayed:

```
1024 b2:a7:95:c1:fa:eb:de:9a:92:05:33:e4
:47:68:eb:91  LanV4
```

Menu PZF STATE

The MENU key lets the user enter the state menu of the PZF. Informations about the decoding of the pseudo-random sequence are available in this menu. The following texts may be displayed:

GSYNC CORR: xx

```
PZF STATE:         GSYNC CORR: 50
                   FIELD: 106
```

This message indicates that the pseudo-random sequence is read into the internal RAM for one second and the system tries to achieve a coarse synchronisation. This procedure starts after power-up or worse receiption for more than ten seconds. The value for "GSYNC CORR" have to be greater than 30.

CORR.: xx

```
PZF STATE:          CORR.: 76
                    FIELD: 106
```

If the coarse synchronisation was successfull, the receiver enters the state of fine-correlation. The system tries to lock the received PZF as exact as possible to generate a precise time frame. The display shows the correlation coefficient at the end of each second, which can be in the range of 52% to 77%. A high value for the coefficient should be achieved by choosing a suitable position for the antenna.

The essential part of the tracking is completed five seconds after the appearence of 'CORR:xx%' and the generation of pulses per minute and per second starts. Tracking steps of three microseconds are possible each second until the internal realtime clock is synchronized (two minutes max.). Afterwards, corrections of the time frame are executed per minute only.

FIELD

The digitized value of the field strength is displayed in this menu. There is a logarithmic relation between this value and the field strength. This menu is useful for mounting the antenna, like described in chapter 'Assembly of antenna'.

Menu Reference Clock State

Pressing MENU in the main menu lets the user enter to the status menu of the reference clocks. The name of the reference clock, the actual state and the last four offsets to the NTP time are displayed (the left one is the newest).

```
PZF:    0000 clk_okay
filtoffset=  -8.42   -4.23  -10.25
```

The state of the refclock will be displayed like "0000". The first two numbers reflects the actually state and the second two numbers the last state of the refclock. The following states are possible:

00: clock okay
01: clock no reply
02: clock bad format
03: clock fault
04: clock bad signal
05: clock bad date
06: clock bad time

Menu SETUP

From this menu, several topics can be selected which let the user edit parameters or force special modes of operation. A specific topic can be selected using the NEXT key. Depending on the current topic, pressing the CLR/ACK key either enters edit mode with the selected set of parameters or switches to the selected mode of operation (after the user has acknowledged his decision). Once edit mode has been entered, the NEXT key lets the cursor move to the digit or letter to be edited whereas the INC key increments the digit or letter under the cursor. If changes have been made, the CLR/ACK key must be pressed. If all changes have been made in one setup submenu you have to press the MENU key. After that you will be asked to save the settings. Press INC to change and save the last changes. Otherwise all changes are discarded when the user presses the MENU key in order to return to the SETUP display.

SETUP LAN PARAMETERS

In this submenu the network parameters are configured. These parameters have to be adapted to the existing network when the LANTIME is installed the first time. The following parameters can be set: **TCP/IP ADDRESS, NETMASK, DEFAULT GATEWAY, IPv6 ADDRESS HOSTNAME, DOMAINNAME, NAMESERVER, SYSLOG SERVER, SNMP MANAGER, REMOTE CONNECT, RESET FACTORY SETTINGS und NET LINK MODE**. All settings are applied to the first Ethernet interface only. All further Ethernet interfaces have to be configured via HTTP or CLI interface. With the submenu REMOTE CONNECT you can enable or disable all network connections via TELNET, FTP or HTTP. When the network parameters have been changed the configuration file is updated and the NTPD is restarted.

With the submenu **RESET FACTORY SETTINGS** the following parameters will be set to the default values:

All configuration parameters of the timeserver are saved on the Flash Disk in the file /mnt/flash/global_configuration. It is recommended not to modify this file manually but to use the configuration interface (HTTP, CLI or SNMP). If this file does not exist, an empty file is generated. The default configuration file is part of the attachment.

The parameters for speed and mode of the net card can be changed with the menu item NET LINK MODE. There are 5 modes available: Autosensing, 10MBit/Half-Duplex, 100MBit/Half-Duplex, 10MBit/Full-Duplex, 100MBit/Full-Duplex. Default setting is Autosensing.

SETUP PZF PARAMETERS

In this submenu the PZF specific parameters can be edited. The distance to the transmitter is entered in the menu "DISTANCE OF TRANSMITTER" 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.

```
SETUP:        PZF PARAMETERS
     DISTANCE OF TRANSMITTER: 1000 km
```

The basic model of the PZF509 includes a voltage controlled temperature compensated oszillator (VCTCXO). Its nominal frequency of 10MHz is adjusted by using two digital-to-analog converters (DACs). One of them is responsible for the coarse tuning and the other one for the fine adjustment of the oszillator.

The value for the coarse-DAC is settable in the menu "OSCILL. AJUST" in the range of 0 to 4095. If the edited value exceeds 4095 the maximum value is storaged. This menu only lets the user modify the coarse-DAC (CAL). The fine-DAC (FINE) is displayed but not to edit. It can be cleared in the next menu.

```
SETUP:        PZF PARAMETERS
 OSCILL. ADJUST:  CAL:2341  FINE:3704
```

This value should only be changed by specialized personnel of company Meinberg and not by the user!

Using the menu "CLR FINE DAC" the DAC is set to its mid-scale value and the difference to its last value is added to the coarse DAC proportional.

```
SETUP:        PZF PARAMETERS
               CLR FINE DAC
```

This process is released automatically if the value of the fine DAC exceeds its limits (0...4095). Therefore the setting of the value to mid-scale by hand is reserved for service purposes only.

The menu "TIME" lets the user edit the time of the PZF509 in hours, minutes, seconds and set the daylight saving (MESZ) active or not. The LANTIME itself always runs on UTC based time. This UTC-time is displayed on the LCD.

```
SETUP:        PZF PARAMETERS
                    TIME
```

The menu "TIME" lets the user edit the date and the day of week of the PZF509 radio clock.

NOTE: Setting the time or date manually XNTPD may terminate itself because of the large deviation (>1024 sec). In this case a restart is necessary.

Enable the menu "SYNC Simulation" lets an asynchronous PZF509 behave like a DCF-synchronous one. This could be necessary to force synchronization of the NTP timeserver nevertheless the LANTIME runs without an antenna. Enabled SYNC Simulation is indicated in the main menu by a wildcard behind the displayed time. This property will not be saved, i.e. after restart the SYNC Simulation always is disabled.

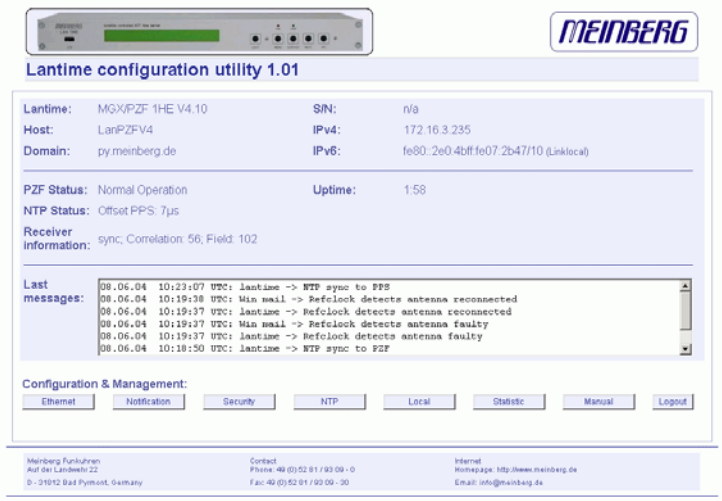
NOTE: Using the SYNC Simulation may cause a time jump (this is possible if the clock was asynchronous for a long time and then gets back synchronisation: this could not be handled by the NTP).

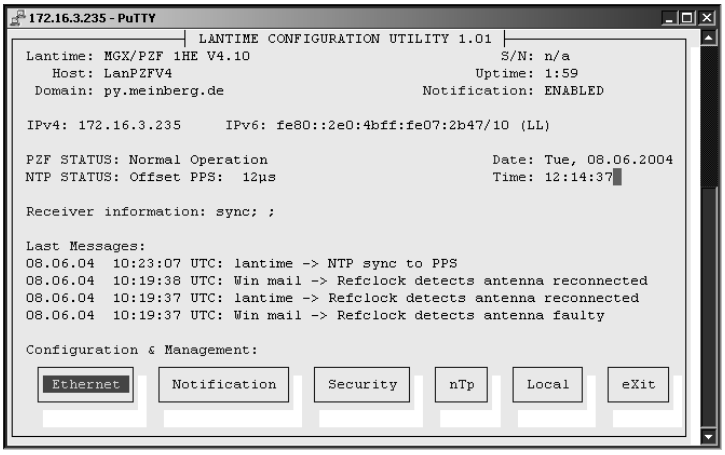
The LANTIME configuration interfaces

The LANTIME offers three different options for configuration and status management: Web interface, Command Line Interface Setup 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).

In addition to the SNMP and web interface, you can also manage your LANTIME configuration via a command line interface (CLI), which can be used via a TELNET or SSH connection. A setup tool can be started after login, just type “setup” and press ENTER at the prompt.

There are only a few differences between the web interface and the CLI, most options are accessible from both interfaces (the CLI has no statistical functions).





The above screenshots show the web interface and the Command Line Interface setup tool. The CLI setup tool can not be used by more than one user at a time, 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.

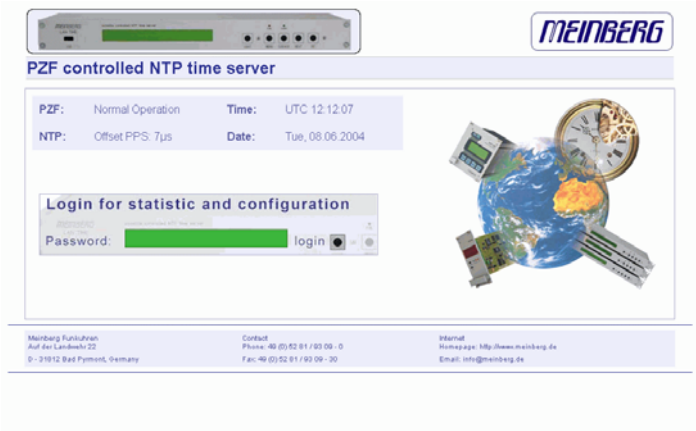
The web interface

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). If you want to use an encrypted connection, replace the http:// with https:// in the above address. You may be prompted to accept the SSL certificate of your LANTIME the first time you are connecting to the system via HTTPS.

In both HTTP and HTTPS mode, you will see the following login screen:



On this start page you see a short status display, which corresponds with the LC display on the front panel of the LANTIME unit. The upper line shows the operation mode of the DCF77 PZF receiver. If the connection to the antenna is broken, a "PZF: ANTENNA FAULTY" may appear.

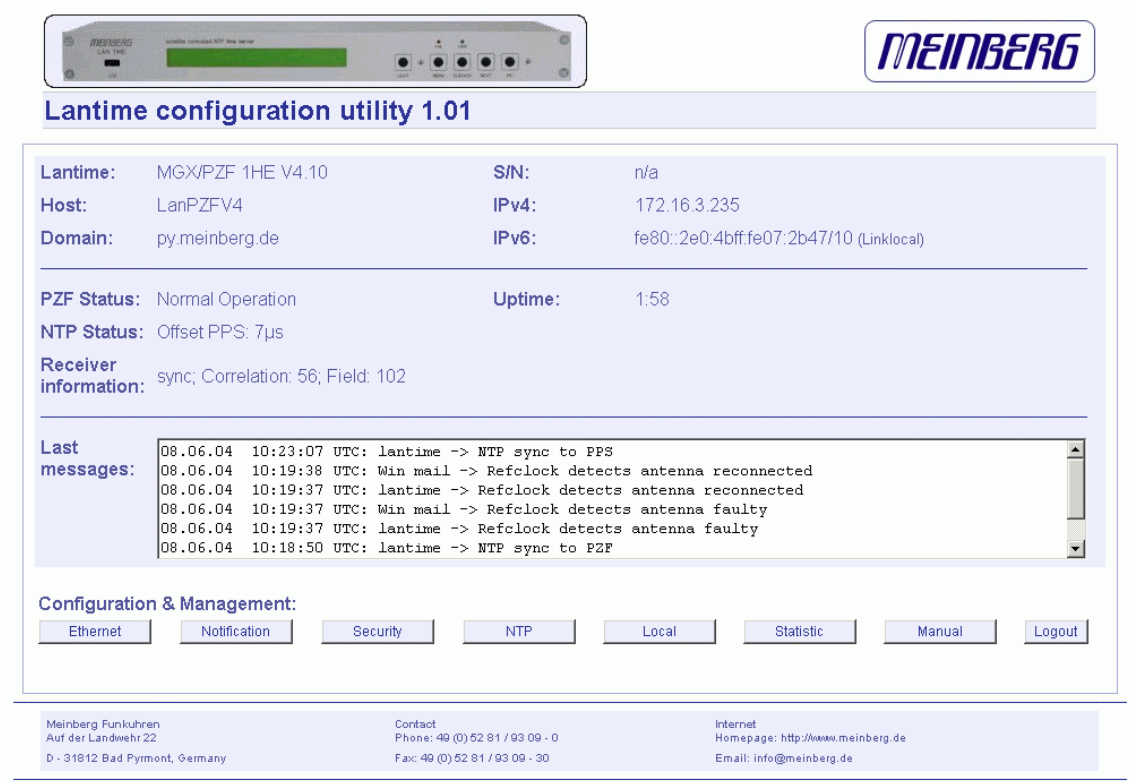
In the upper right corner of the LC display the time and time zone can be found, below that you will find the date and weekday.

On the second line the systems reports the NTP status, during the initial synchronisation process a "NTP: not sync" indicates that the NTP system is not synchronised, this can also appear if the PZF looses synchronisation and the NTP switches back to its "LOCAL CLOCK" time source .

The DCF77 PZF clock is connected to the LANTIME system internally by using a serial connection and additionally by using the second pulse. So, there are 2 reference clocks used by NTPD, the PZF and PPS time source. You will find the two time sources in the status information of the NTPD. After the NTP is synchronised, the Display shows "NTP: Offset PZF: x" or "NTP: Offset PPS: x" where "x" is the actual offset to the PZF or PPS time source.

This page will be reloaded every 30 seconds in order to reflect the current status of the unit. Please keep this in mind when you try to login and enter your password. If you do not press ENTER or the Login button within 30 seconds, the password field is cleared and you have to start over again.

Configuration: Main Menu



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.

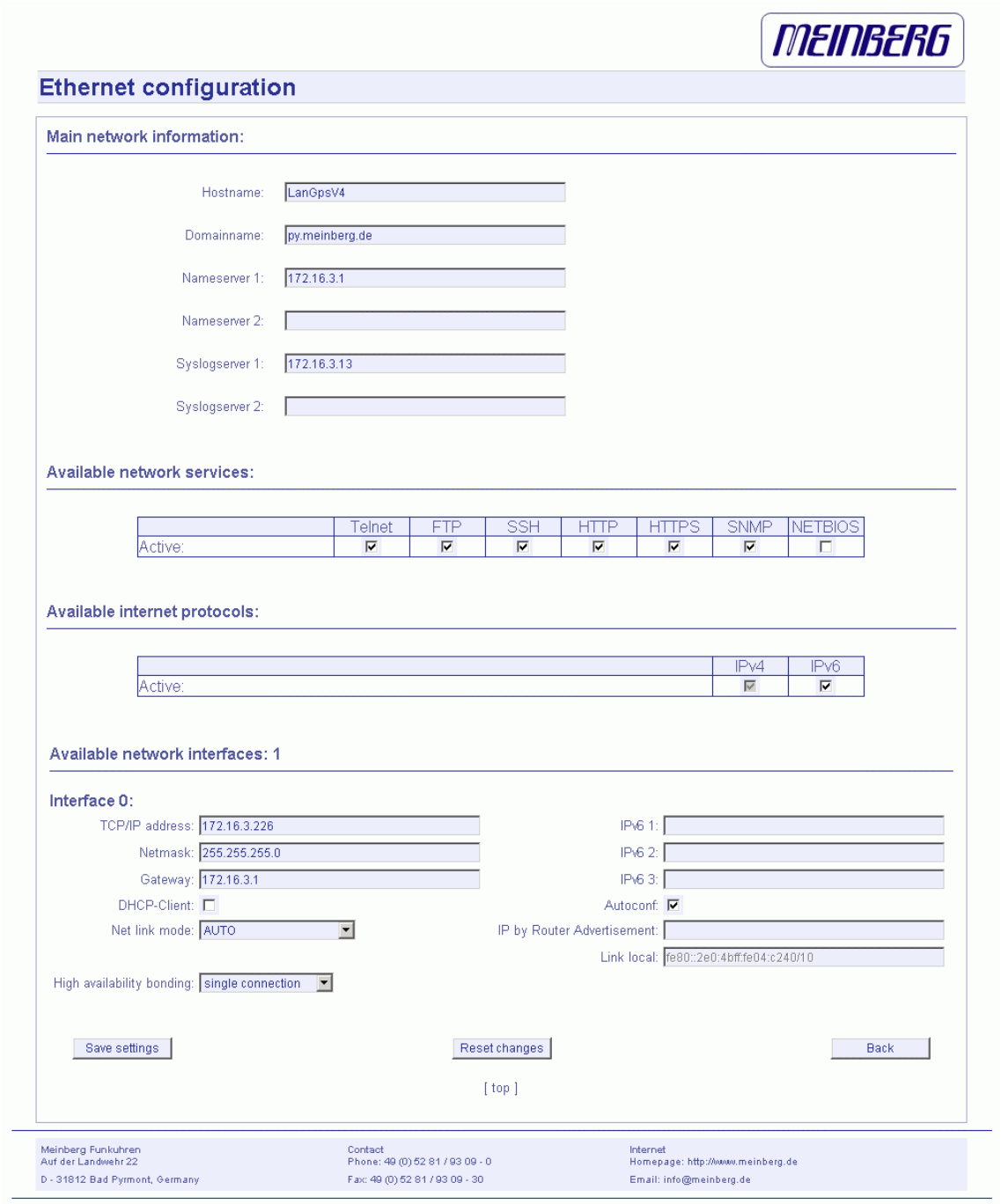
The start page gives a short overview of the most important configuration parameters and the runtime statistics of the unit. In the upper left corner you can read which LANTIME model and which version of the LANTIME software you are using. This LANTIME software version is a head version number describing the base system and important subsystems. Below the version you will find the actual hostname and domain of your LANTIME unit, the IPv4 and IPv6 network address of the first network interface and on the right side the serial number, the uptime of the system (time since last boot) and the notification status.

In the second section the actual status of the DCF77 PZF reference clock and the NTP subsystem is shown, additional information about the DCF77 PZF receiver are also found here. This includes the current mode of the DCF77 PZF receiver, the field strength and the correlation in per cent.

The third 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 buttons in the lower part of the screen, you can reach a number of configuration pages, which are described below.

Configuration: Ethernet



In the network configuration all parameters related to the network interfaces can be changed. In the first section you can change the hostname and domainname. You can also specify two nameserver and two SYSLOG server. In the nameserver and syslog server fields you may enter an IPv4 or IPv6 address (the syslog servers can be specified as a hostname, too).

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 SYSLOD 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.

In the second section the possible network protocols and access methods can be configured. You can enable/disable TELNET, FTP, SSH, HTTP, HTTPS, SNMP and NETBIOS by checking/unchecking the appropriate check boxes. After you saved your settings with the “Save” button, all these subsystems are stopped and eventually restarted (only if they are enabled, of course).

The third section allows you to select the IP protocol version 6. 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, FTP and NETBIOS can not be used over IPv6 in this version. It is no problem to use IPv4 and IPv6 in a mixed mode environment on your LANTIME.

Network interface specific configuration

The interface specific parameters can be found in the Interface section. If your LANTIME is equipped with only one network interface, you will find only one sub section (Interface 0). Otherwise you see a sub section for each installed Ethernet port.

Here, the parameters for the network port can be changed. In the upper section of the page you can enter the IPv4 parameters, the lower part gives you access to the IPv6 parameters of the interface.

IPv4 addresses and DHCP

IPv4 addresses are built of 32bits, 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 you network administrator, who can provide you with the settings suitable for your specific network.

If you 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.

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

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)

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.

The last parameter in this sub section is “Netlink mode”. This controls the port speed and duplex mode of the selected Ethernet port. Under normal circumstances, you should leave the default setting (“autosensing”) untouched, until your network administrator tells you to change it.

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.

A separate use of the same driver allows the kernel to present a single logical interface for two physical links to two separate switches. Only one link is used at any given time. By using media independent interface signal failure to detect when a switch or link becomes unusable, the kernel can, transparently to userspace and application layer services, fail to the backup physical connection. Though not common, the failure of switches, network interfaces, and cables can cause outages. As a component of high availability planning, these bonding techniques can help reduce the number of single points of failure.

At this menu point it is possible to add each Ethernet port to a bonding group. 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 provide the IP-Address and the net mask of this new virtual device.

Configuration: Notification

MEINBERG

Notification management

Email information:

To address:

From address:

Smarthost:

Windows mail information (WinPopup):

Mail address 1: pc-udo2

Mail address 2:

SNMP information:

SNMP manager 1: Community:

SNMP manager 2: Community:

VP100/NET display information:

Display 1: Serial number:

Display 2: Serial number:

User defined notification:

Show user defined notification script | Edit user defined notification script

Notification conditions :

Condition:	Triggers:				
	Email	Wmail	SNMP	VP100/NET	User
NTP not sync	☐	☑	☐	☐	☐
NTP stopped	☐	☑	☐	☐	☐
Server boot	☐	☑	☐	☐	☐
Receiver not responding	☐	☐	☐	☐	☐
Receiver not sync	☐	☑	☐	☐	☐
Antenna faulty	☐	☑	☐	☐	☐
Antenna reconnect	☐	☑	☐	☐	☐
Config changed	☐	☐	☐	☐	☐

Edit messages

Save settings | Reset changes | Back

[top]

Meinberg Funkuhren
Auf der Landwehr 22
D - 31812 Bad Pyrmont, Germany

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

Internet
Homepage: http://www.meinberg.de
Email: info@meinberg.de

Alarm events

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 four 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 and DISPLAY shows the alarm message on a wall mount display model VP100/NET, which is an optional accessory you can obtain for your LANTIME.

Here is a table of supported events:

"NTP not sync"	NTP is not synchronised to a reference time source
"NTP stopped"	NTP has been stopped (mostly when very large time offsets occur)
"Server boot"	System has been restarted
"Receiver not responding"	No contact to the internal DCF77 PZF receiver
"Receiver not sync"	Internal DCF77 PZF clock is not synchronised to DCF77 time
"Antenna faulty"	DCF77 PZF antenna disconnected
"Antenna reconnect"	DCF77 PZF antenna reconnected
"Config changed"	Configuration was changed by a user

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.
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.

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

- the LANTIME hostname 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

Windows Popup Messages

Most Microsoft Windows operating systems provide you with a local notification tool. You can send messages via the special Windows protocol in your local network. It is not necessary to enable the NETBIOS protocol of the LANTIME in order to use this notification. On the Windows client side it is necessary to activate the “Microsoft Client for Windows” in the network configuration.

You can enter the Windows computer name of up to two Windows PCs in the appropriate fields. Every message contains a time stamp and a plain text message:

SNMP-TRAP messages

Up to two 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).

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 (10/100Mbit) 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 it’s 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.

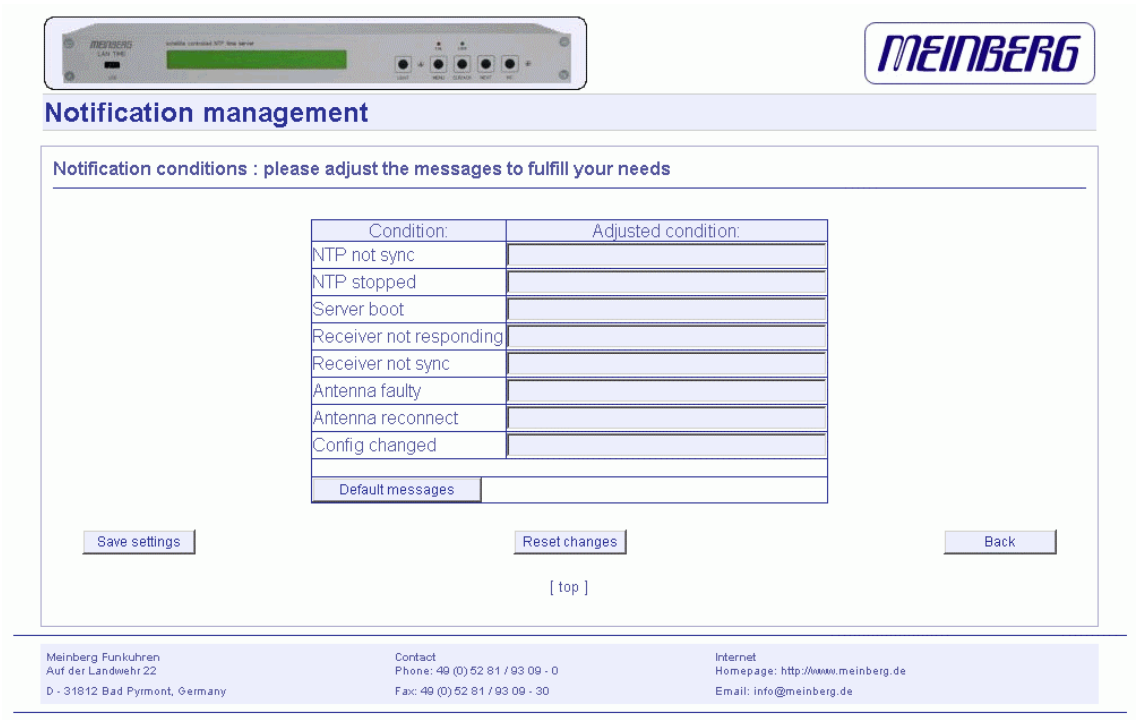
If you want to use the display for other purposes, you can send text messages to it by using our command line tool send2display, which can be found on the LANTIME. This allows you to use the display by CRON jobs or your own shell scripts etc. If you run the tool without parameters, a short usage screen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

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. 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.

Alarm messages

You can change the alarm message text for every event by using the „Edit messages“ button, the messages are stored in a file /mnt/flash/notification_messages on the flash disk of your timeserver.



Configuration: Security

MEINBERG

Security management

Login:

New password:

Re-enter:

Change Lantime password

Config HTTP access control

SSH key generation:

Generate SSH key

Show SSH key

HTTPS certificate generation:

Generate SSL certificate for HTTP

Show SSL certificate for HTTP

NTP autokey generation:

Generate new NTP public key

Generate groupkey

Browse...

Upload groupkey

NTP autokey password: timeserver

NTP symmetric keys:

Show NTP MD5 keys

Edit NTP MD5 keys

SNMP:

Read community String: public

Read/Write community string:

SNMP contact: Meinberg

SNMP location: Germany

User name : root

Authentication passphrase:

Re-enter passphrase:

Change SNMP v3 authentication

Save settings

Reset changes

Back

[top]

Meinberg Funkuhren
Auf der Landwehr 22
D - 31812 Bad Pyrmont, Germany

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

Internet
Homepage: http://www.meinberg.de
Email: info@meinberg.de

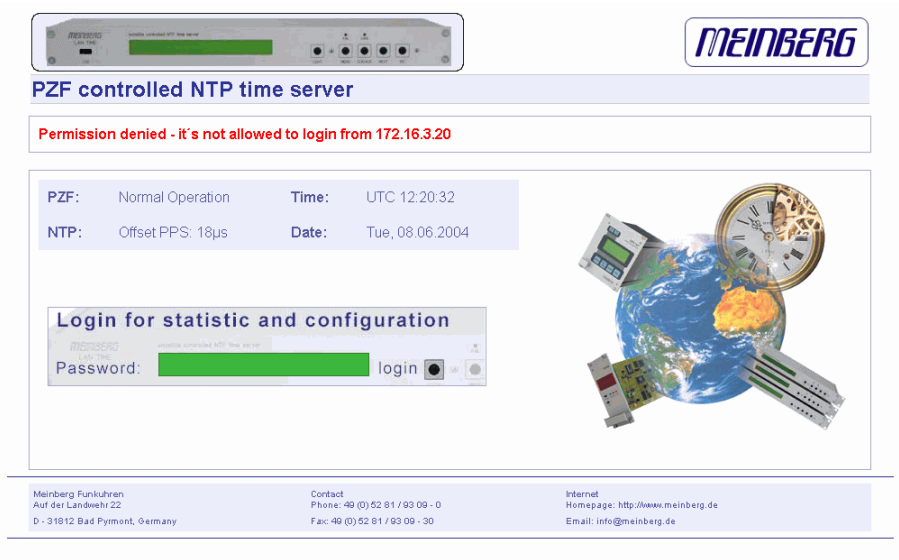
Password

On the „Security“ page you can manage all security relevant parameters for your timeserver. In the first section “Login” the administration password can be changed, which is used for SSH, TELNET, FTP, HTTP and HTTPS access. The password is stored encrypted on the internal flash disk and can only be reset to the default value “timeserver” by a “factory reset”, changing all settings back to the factory defaults. Please refer to the LCD configuration section in this manual.

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.

If a non-allowed host tries to login, the following message appears:



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).

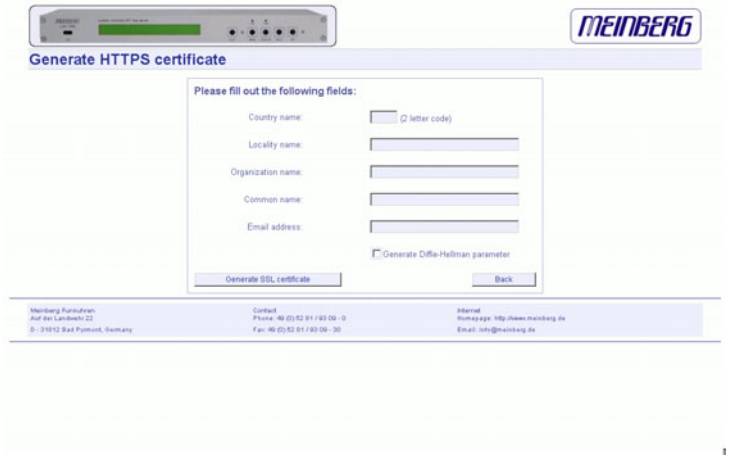
If you generate a new SSH key, you can copy and paste it into your SSH client configuration afterwards in order to allow you to login without being prompted for a password. We strongly recommend to use SSH for shell access, TELNET is a very insecure protocol (transmitting passwords in plain text over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

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.

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 authenticates 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.

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.



After the successful generation of the certificate, it is shown to you:

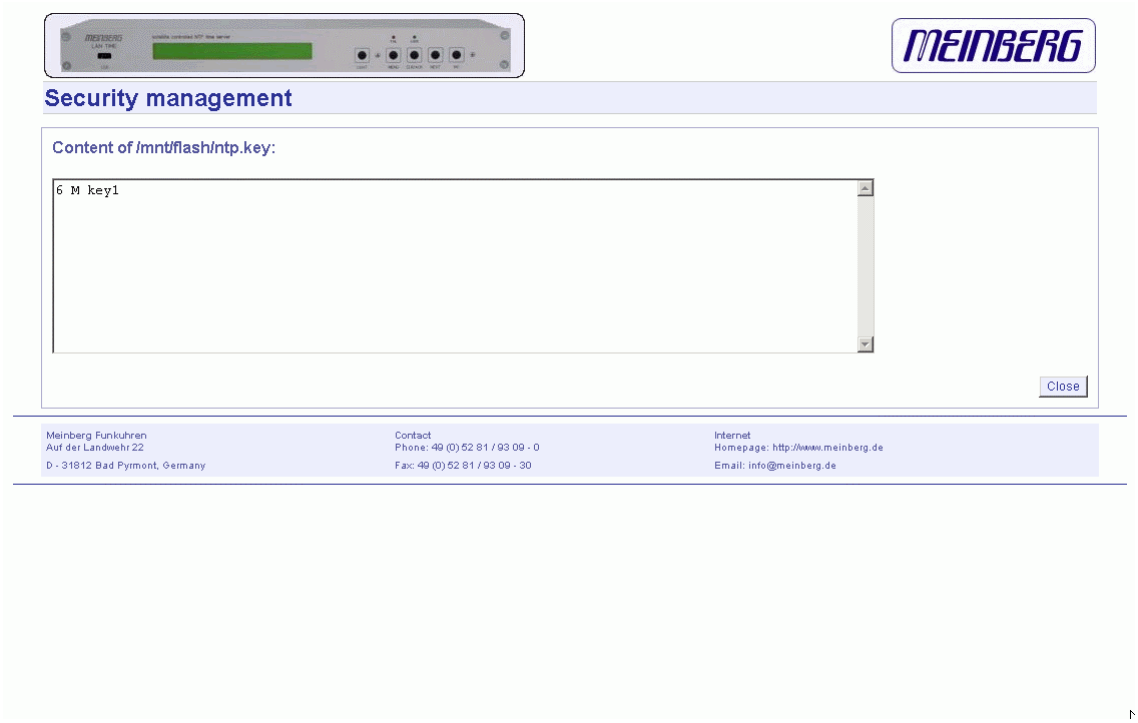
NTP keys and certificates

The fourth and fifth section of the „Security" page allow you to create the needed crypto keys and certificates for secure NTP operation (please see NTP authentication below).

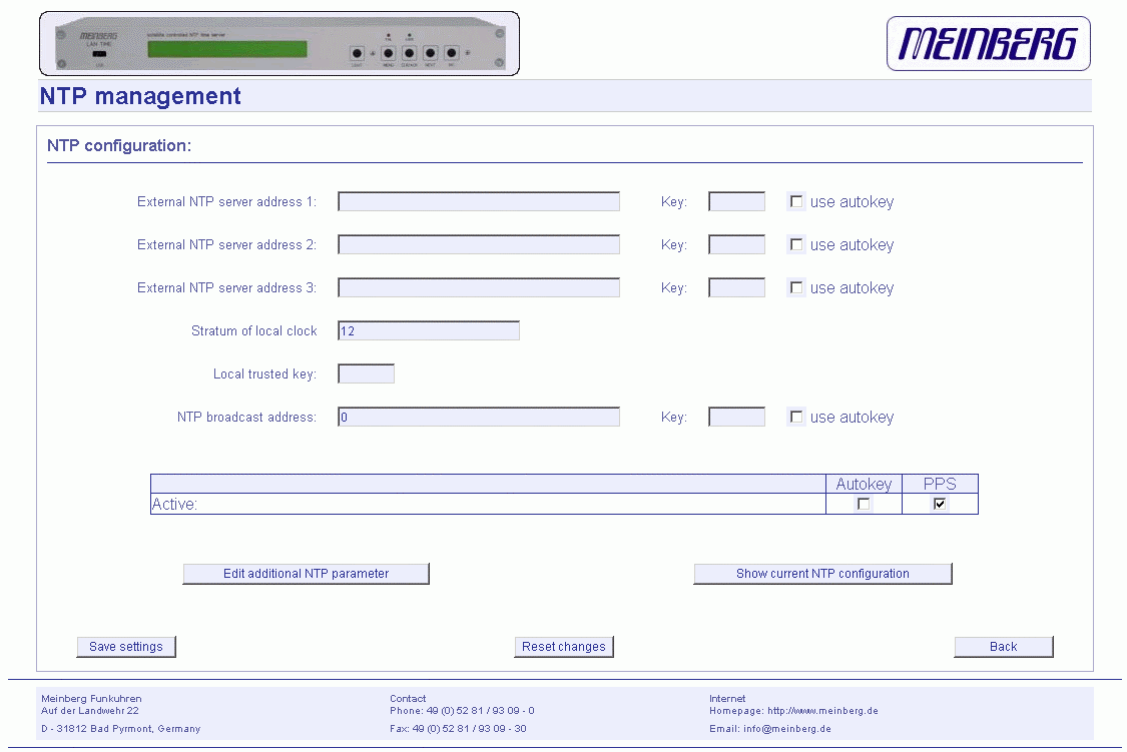
The function „Generate new NTP public key" is creating a new self-signed certificate for the timeserver, which is automatically marked as „trusted".

Important note: This certificate is depending on the hostname of your LANTIME, it is mandatory to re-create the certificate after changing the hostname. The certificates are build with the internal command "ntp-keygen -T" (ntp-keygen is part of the installed NTP suite). Your LANTIME is using the /etc/ntp/ directory for storing its private and public keys (this is called the "keysdir"). Please refer to the chapter "NTP Autokey" for further information (below).

The two options „Show NTP MD5 key" and „Edit NTP MD5 keys" allow you to manage the symmetric keys used by NTP. More about that can be found in the chapter about symmetric keys (below).



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.

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your LANTIME system and the DCF77 PZF reference clock. The local clock is only chosen as the NTP time reference after the PZF 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.

Because the DCF77 PZF 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 ATOM driver of the NTP subsystem, which is directly interpreting the PPS (pulse per second) of the CDF77 PZF reference clock. The default configuration looks like this:

```
#  ***  lantime  ***
# NTP.CONF for PZF509

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

server  127.127.8.0 mode 130 prefer  # PZF509
fudge   127.127.8.0 time1 0.0099     # 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
```

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 three 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.

The field “Stratum of local clock” is used to change the stratum level of the local clock (see above), default is 12.

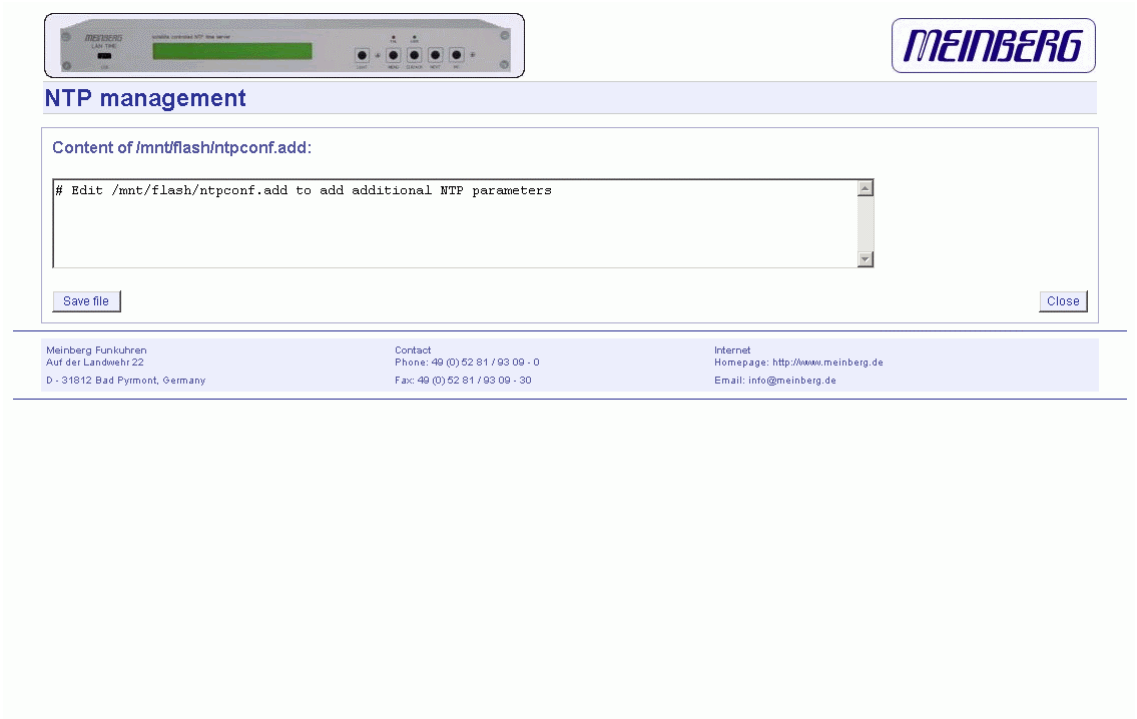
The „Local trusted key“ field holds a list of all trusted symmetric keys (comma separated), which have to be accepted by the NTPD of your LANTIME.

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:

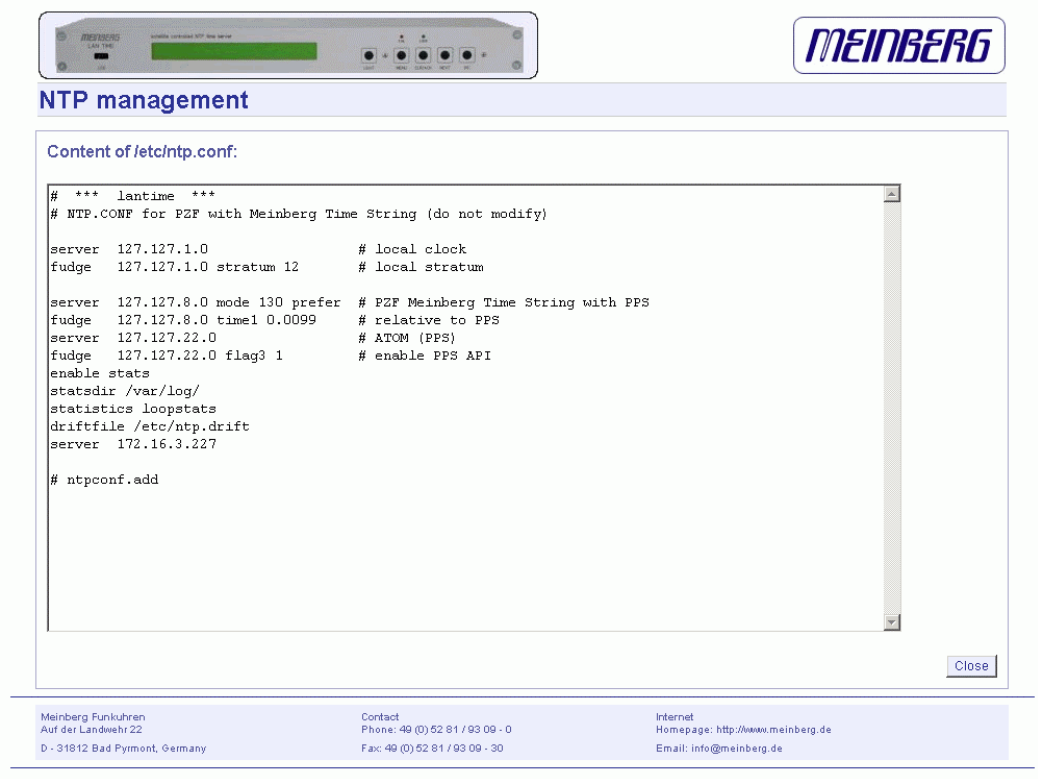
```
broadcastclient yes
broadcastdelay 0.05    # depends on your network
authenticate yes
keys /etc/ntp/keys
trustedkey 6 15
requestkey 15
controlkey 15
```

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.

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”.



By choosing „Show current 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.



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 ntpdc 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    RIrop8KPPvQvYotM    # 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.

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.

NTP AUTOKEY

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

c) Client

One ore 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 new NTP public key” in section “NTP Autokey” 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, it 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").

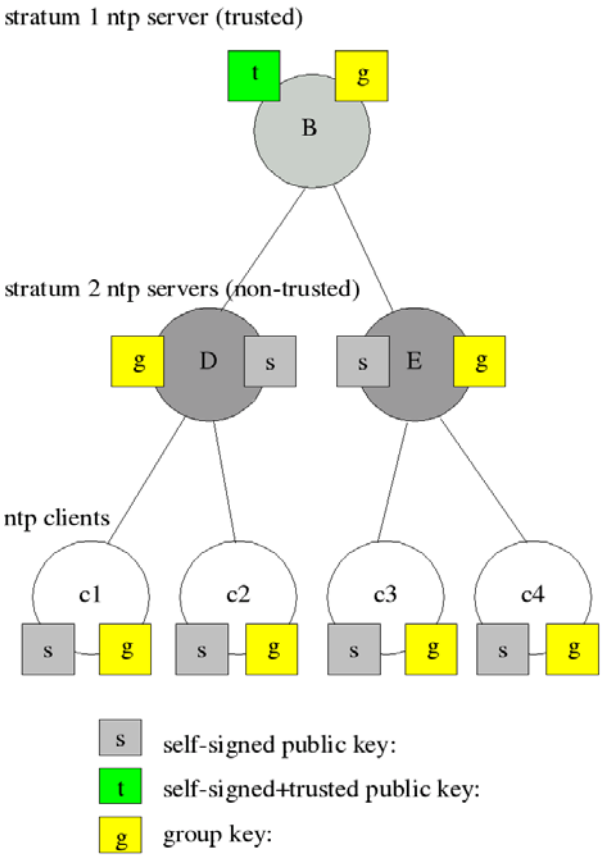
If you want to setup the LANTIME as a "non-trusted" NTP server, you have to upload the group key of your secure group ("Security Management" / "NTP autokey" / "Upload groupkey") and create your own, self-signed certificate (without marking it as "trusted"). Because every certificate which is creating 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.

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

Example:



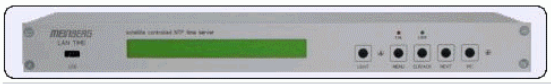
This autokey group is formed by one stratum 1 server (B), two stratum 2 servers (D and E) and a number of clients (in the diagram there are 4 clients shown, c1 – c4). B is the trusted host, he holds the group key and a self-signed certificate marked as “trusted”.

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).

Configuration: Local



MEINBERG

Local configuration

Lantime services:

Reboot Lantime

Manual configuration

Send test notification

Save NTP drift file

Reset to factory defaults

Download SNMP MIB files

Show Lantime information:

List all messages

List detailed version information

List Lantime options

List detailed PZF information

Lantime firmware update:

Browse...

Start firmware update

Lantime configuration:

Check configuration

Web interface language: English

Save settings | Reset changes | Back

[top]

Meinberg Funkuhren
Auf der Landwehr 22
D - 31812 Bad Pyrmont, Germany

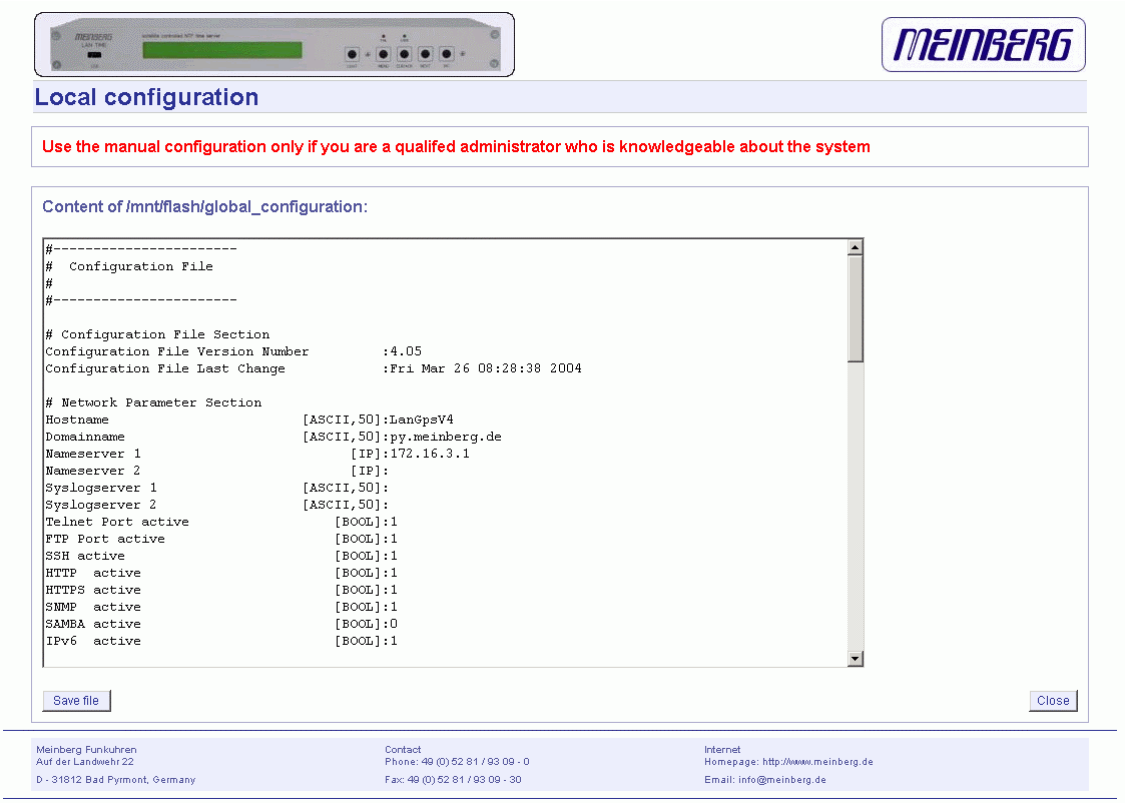
Contact
Phone: 49 (0) 52 81 / 93 09 - 0
Fax: 49 (0) 52 81 / 93 09 - 30

Internet
Homepage: http://www.meinberg.de
Email: info@meinberg.de

Administrative functions

In the first section there are several functions which may be used by the administrator. The button “Reboot Lantime” 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 synchronised 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 re-created 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.

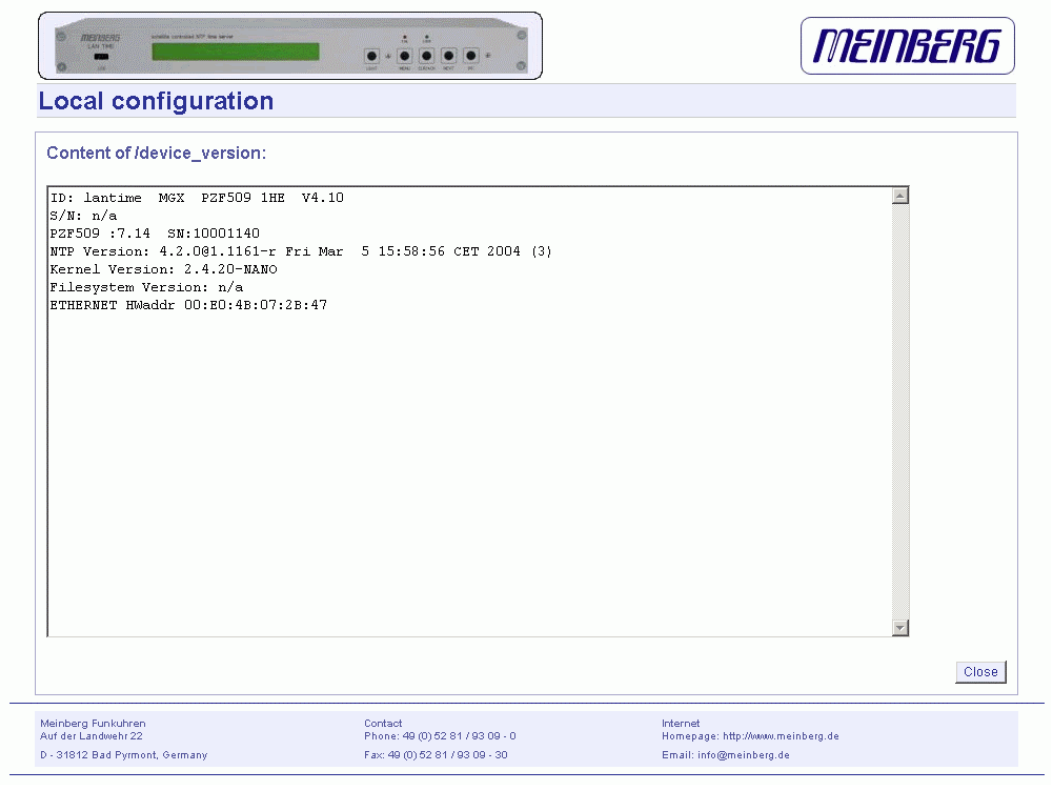
The point „Download SNMP MIB files“ can be used to download all Meinberg specific SNMP MIB files to your workstation. They can be distributed to all SNMP management clients afterwards.

Administrative Information

The button „List all messages“ displays the SYSLOG of the LANTIME completely. In this log all subsystems create their entries, even the os 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.

```
Mar 15 13:35:17 LanV4 ntpd[12948]: ntpd 4.2.0@1.1161-r Fri Mar  5
15:58:48 CET 2004 (3)
Mar 15 13:35:17 LanV4 ntpd[12948]: signal_no_reset: signal 13 had
flags 4000000
Mar 15 13:35:17 LanV4 ntpd[12948]: precision = 3.000 usec
Mar 15 13:35:17 LanV4 ntpd[12948]: kernel time sync status 2040
Mar 15 13:35:17 LanV4 ntpd[12948]: frequency initialized 45.212 PPM
from /etc/ntp.drift
Mar 15 13:38:36 LanV4 lantime[417]: NTP sync to PZF
Mar 15 13:38:36 LanV4 lantime[417]: NTP restart
Mar 15 13:45:36 LanV4 proftpd[14061]: connect from 172.16.3.2
(172.16.3.2)
Mar 15 14:01:11 LanV4 login[15711]: invalid password for `root' on
`ttyp1' from `172.16.3.45'
Mar 15 14:01:17 LanV4 login[15711]: root login  on `ttyp1' from
`172.16.3.45'
```

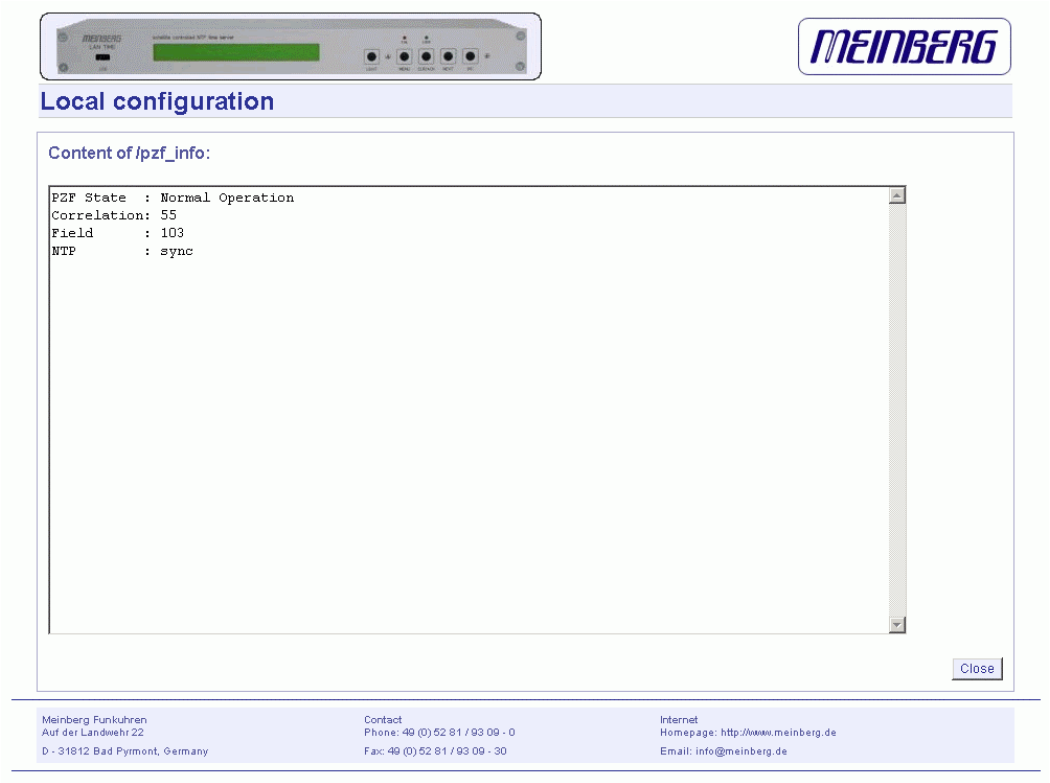
With „List detailed version information“ a number of version numbers (including LANTIME software, operating system and NTPD) are shown in a textbox.



The function „List LANTIME Options“ shows the hardware options installed in your LANTIME.

Using the button „List detailed PZF information“ gives you the possibility to check detailed PZF status information. The first parameter indicates the state of the DCF77 PZF clock. The next parameter is correlation of the PZF in per cent. The correlation

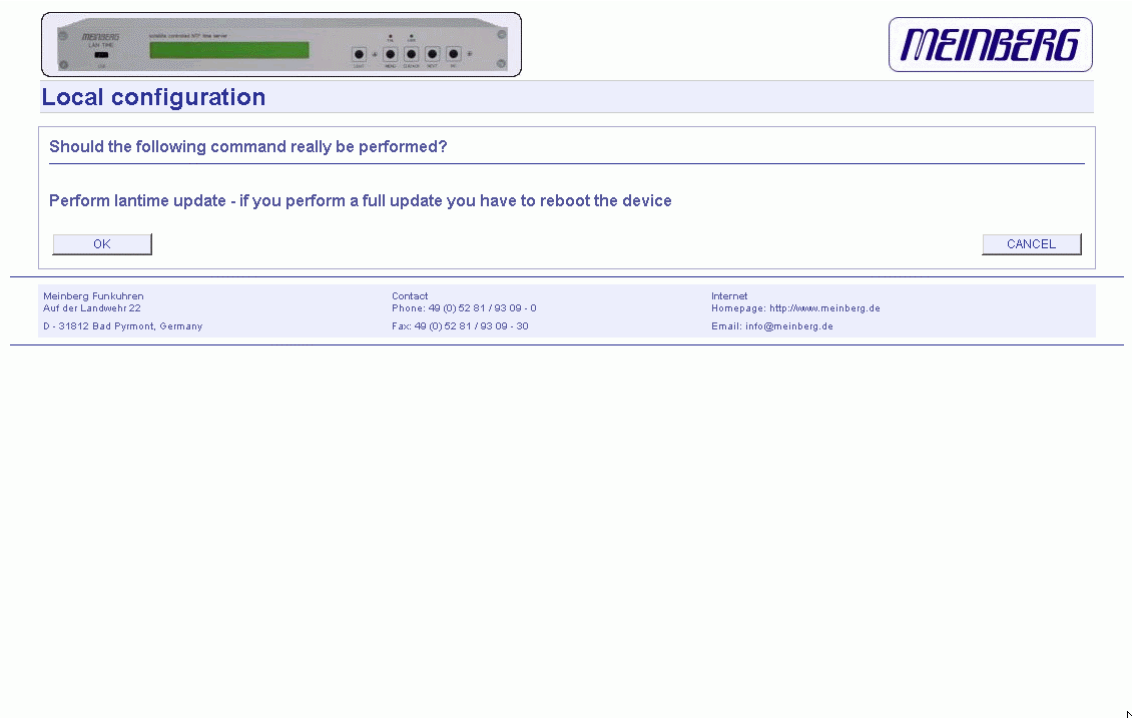
value should be in the range of 60 to 75 per cent. The next parameter is the signal field strength of the DCF77. The last parameter will reflect the state of the internal NTP.



Software Update

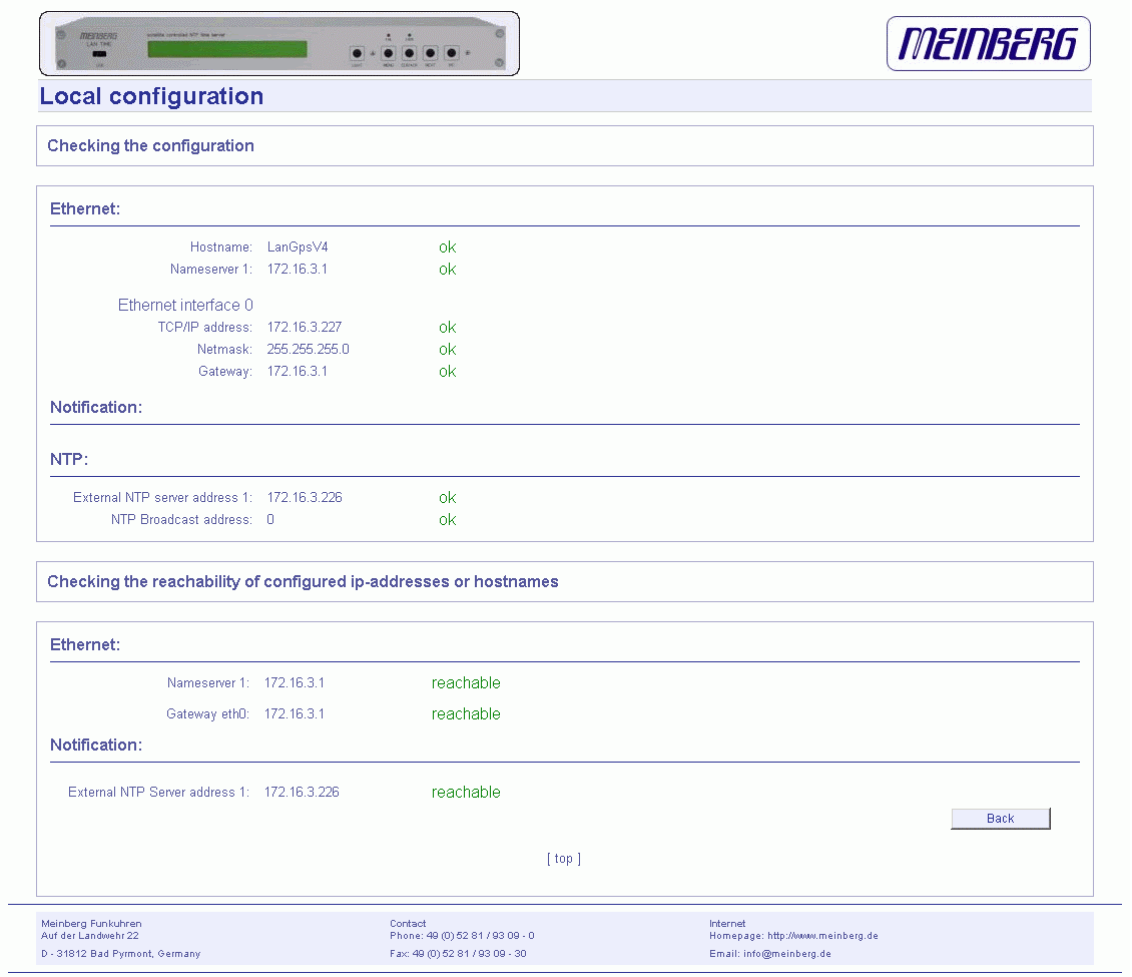
If you need to update the software of your LANTIME, you need a special file from Meinberg, which can be uploaded to the LANTIME by first choosing the file on your local computer with the “Browse” button and then press “Start firmware update”.

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.



Automatic configuration check

All parameters of the LANTIME can be checked for plausibility and all configured servers (e.g. SYSLOG servers, nameservers) are tested for reachability. All red coloured values should be reviewed by the administrator. Because all configured hostnames / IP addresses of the servers are processed during the reachability-tests, the whole check process may take a while.



Web interface language

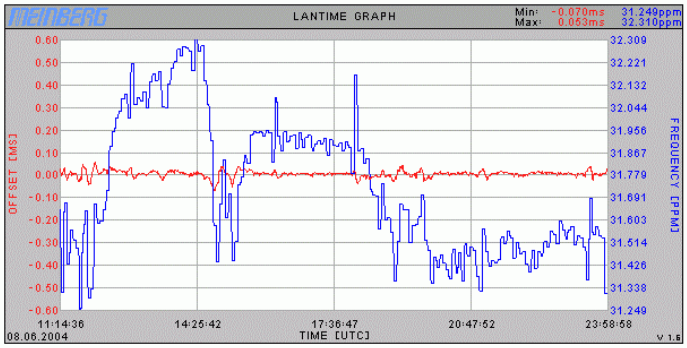
With the selector box “Web interface language” you can change the displayed language of the WEB interface.

Configuration: Statistics

MEINBERG

Statistic

Statistic information:



Available logfiles: loopstats.20040608 Generate statistic

merge loopstats

Lantime information:

S/N: n/a
PZF509 :7.14 SN:10001140
NTP Version: 4.2.0@1.1161-r Fri Mar 5 15:58:56 CET 2004 (3)
Kernel Version: 2.4.20-NANO
Filesystem Version: n/a
ETHERNET HWaddr 00:E0:4B:07:2B:47
Uptime: 22 h
Mem free: 4960 kB
Disk free: 24567 kb

NTP access information:

remote address	port	local address	count	m	ver	code	avglen	first
127.0.0.1	1482	127.0.0.1	13579	7	2	0	0	0
172.16.3.227	123	172.16.3.235	71	4	4	0	64	3

Back

[top]

Meinberg Funkuhren
Auf der Landwehr 22
D - 31812 Bad Pyrmont, Germany

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

Internet
Homepage: http://www.meinberg.de
Email: info@meinberg.de

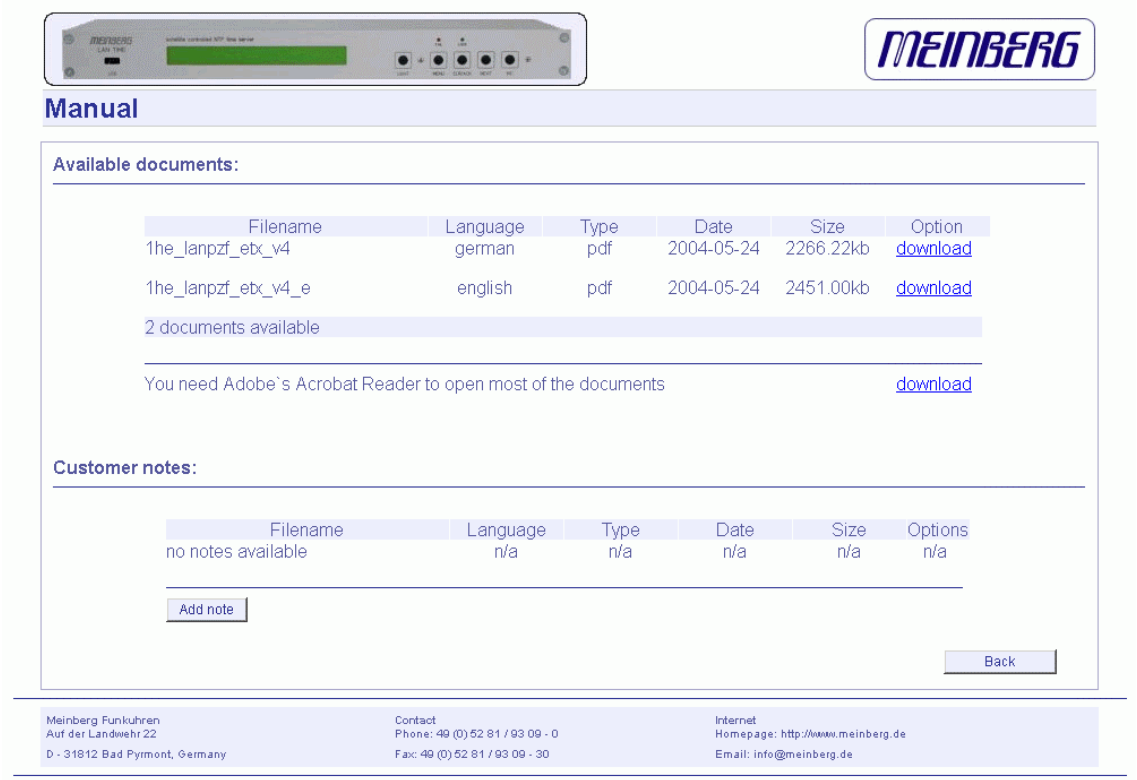
Statistical Information

In the first section a graphical diagram shows the running synchronisation process. NTP is storing these 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 (PZF) 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 PZF 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 16 MB (each). The Uptime parameter displays the time since the last boot process of the unit.

In the last 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.

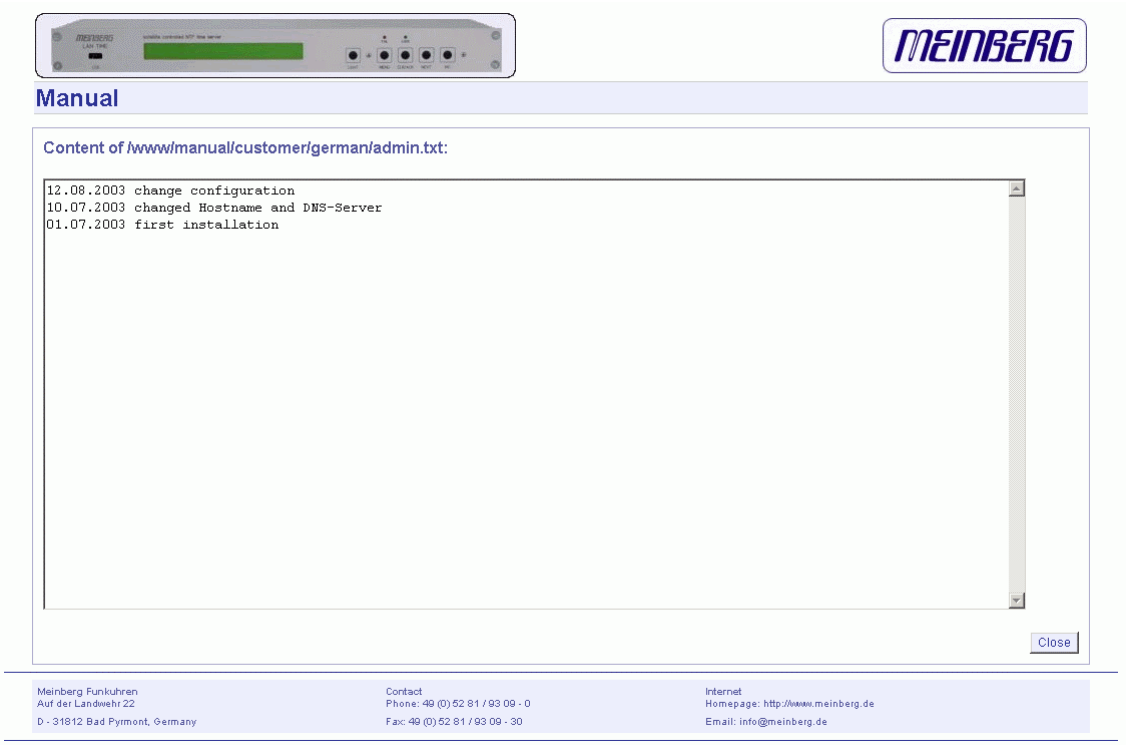
Configuration: Manual



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.

The LANTIME documents can be downloaded from here in order to read / print them on your workstation.

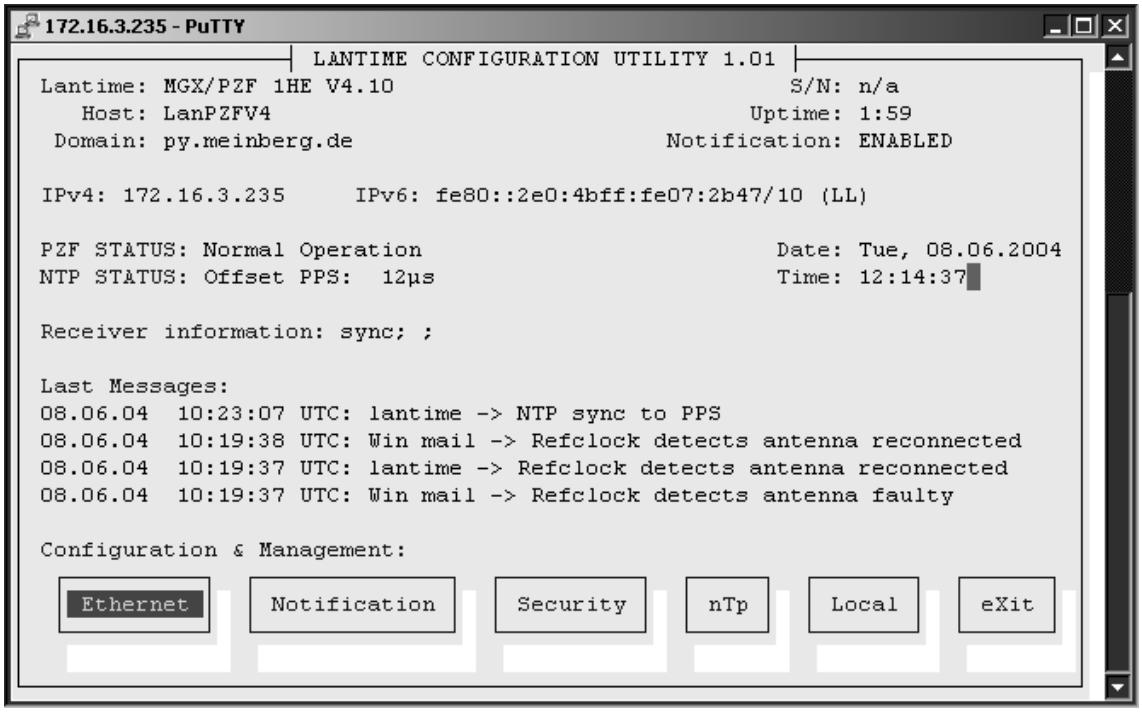
The customer notes are a way of storing small pieces of information on your LANTIME, for example if you want to keep track of configuration changes and want to comment them, you can create a note called “config_changes” and show or edit it from here. If you want to get rid of one of your notes, you are 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.

The Command Line Interface

The command line interface (CLI) can be used within a TELNET or SSH session. After login, just enter “setup” to start the CLI setup tool.



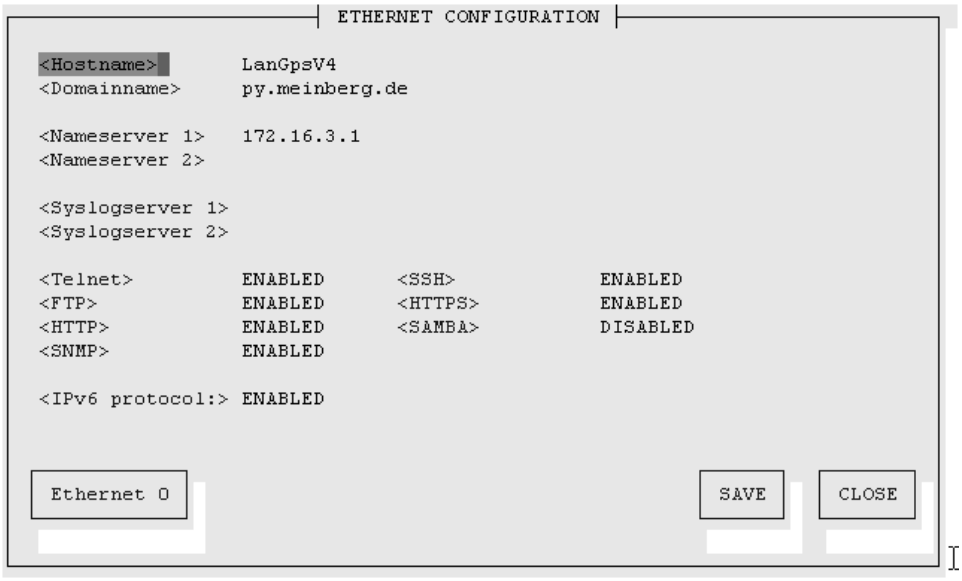
The start page gives a short overview of the most important configuration parameters and the runtime statistics of the unit. In the upper left corner you can read which LANTIME type and version of the LANTIME software you are using. This LANTIME software version is a head version number describing the base system and important subsystem. Below the version you will find the actual hostname and domain of your LANTIME unit, the IPv4 and IPv6 network address of the first network interface and on the right side the serial number, the uptime of the system (time since last boot) and the notification status is reported.

In the second section the actual status of the DCF77 PZF reference clock and the NTP subsystem is shown, additional information about the PZF receiver can also be found here. This includes the current state of the DCF77 PZF, the signal field strength and the correlation of the PZF in per cent.

The third section shows the last messages of the system, each with a timestamp added. The newest messages are placed at the top of the list. This reflects 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, see “Syslog server” to learn how to save the entries of your SYSLOG).

By using the buttons in the lower part of the screen, you can reach a number of configuration pages, which are described below.

CLI Ethernet



In the network configuration all parameters related to the network interfaces can be changed. In the first section you can change the hostname and domainname. You can also specify two nameservers and two SYSLOG servers. In the nameserver and SYSLOG server fields you may enter an IPv4 or IPv6 address (the SYSLOG servers can be specified as a hostname, too).

All information which is 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” for 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 started 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 them automatically, if their size is exceeding a limit.

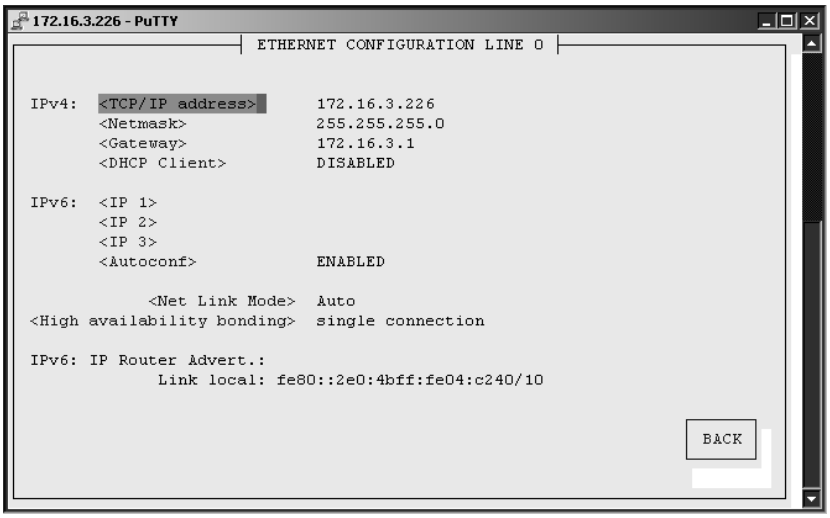
By specifying one or two remote SYSLOG servers, you can preserve the SYSLOG information even when you have to reboot or switch off the LANTIME.

In the second section the possible network protocols and access methods can be configured. You can enable/disable TELNET, FTP, SSH, HTTP, HTTPS, SNMP and NETBIOS by checking/unchecking the appropriate check box. After you saved your settings with the “Save” button, all of these subsystems are stopped and restarted (if they are enabled).

The third section allows you to select the IP protocol 6. In this version the IPv4 protocol is mandatory and cannot be disabled, but a standalone IPv6 mode can be

reached 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, FTP and NETBIOS can not be used over IPv6 in this version. IPv4 and IPv6 can be used together on one LANTIME.

To manage the interface specific parameters, you can enter the Ethernet Configuration Line page by using one of the ETHERNET buttons. If your LANTIME is equipped with only one network interface, you will find only one button (ETHERNET 0). Otherwise you see one button for each installed Ethernet port.



Here, the parameters for the network port can be changed. In the upper section of the page you can enter the IPv4 parameters, the lower part gives you access to the IPv6 parameters of the interface.

IPv4 addresses are built of 32bits, 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 you network administrator, who will provide you with the settings suitable for your specific network.

If you are running a DHCP (Dynamic Host Configuration Protocol) server in your network, the LANTIME system can obtain its IPv4 settings automatically from this server. If you want to use this feature (you should also ask your network administrator if 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. This is the default 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 used by the network

administrator when setting up the DHCP parameters for your LANTIME at the DHCP server.

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

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)

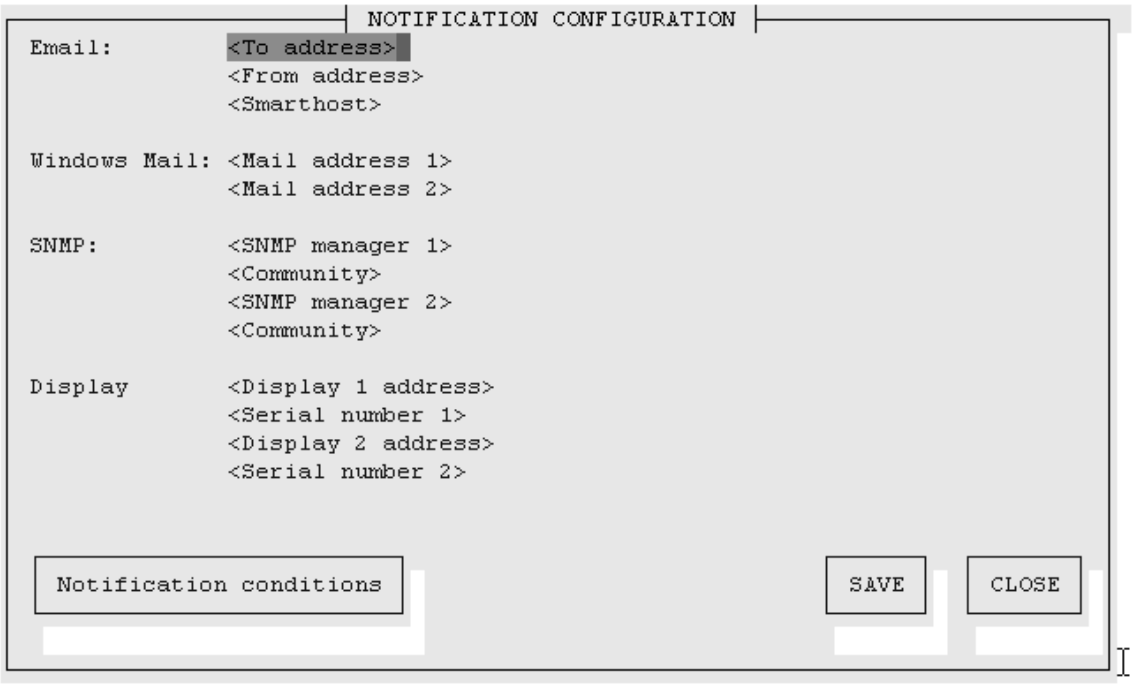
If you enabled the IPv6 protocol, the LANTIME always gets a link local address in the format "fe80:: ..", which is based upon the MAC address of the interface. If a IPv6 router advertiser is available in your network and if you enabled the IPv6 AUTOCONF feature, your LANTIME will be set up with up to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

The next parameter in this sub section is "Netlink mode". This controls the port speed and duplex mode of the selected Ethernet port. Under normal circumstances, you should leave the default setting ("autosensing") untouched, until your network administrator tells you to change it.

High Availability Bonding is the last parameter in this section. 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. A separate use of the same driver allows the kernel to present a single logical interface for two physical links to two separate switches. Only one link is used at any given time. By using media independent interface signal failure to detect when a switch or link becomes unusable, the kernel can, transparently to userspace and application layer services, fail to the backup physical connection. Though not common, the failure of switches, network interfaces, and cables can cause outages. As a component of high availability planning, these bonding techniques can help reduce the number of single points of failure.

At this menu point it is possible to add each Ethernet port to a bonding group. 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 provide the IP-Address and the net mask of this new virtual device.

CLI Notification



Alarm events

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 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 four different ways of informing the administrator or a responsible person about nine different events: EMAIL send an email 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 and DISPLAY shows the alarm message on a wall mount display model VP100/NET, which is an optional accessory you can obtain from us.

Here is a table of all events:

"NTP not sync"	NTP is not synchronised to a reference time source
"NTP stopped"	NTP has been stopped (mostly when very large time offsets occur)
"Server boot"	System has been restarted
"Receiver not responding"	No contact to the internal DCF77 PZF receiver
"Receiver not sync"	Internal PZF clock is not synchronised to DCF77 time
"Antenna faulty"	DCF77 PZF antenna disconnected
"Antenna reconnect"	DCF77 PZF antenna reconnected
"Config changed"	Configuration was changed by a user

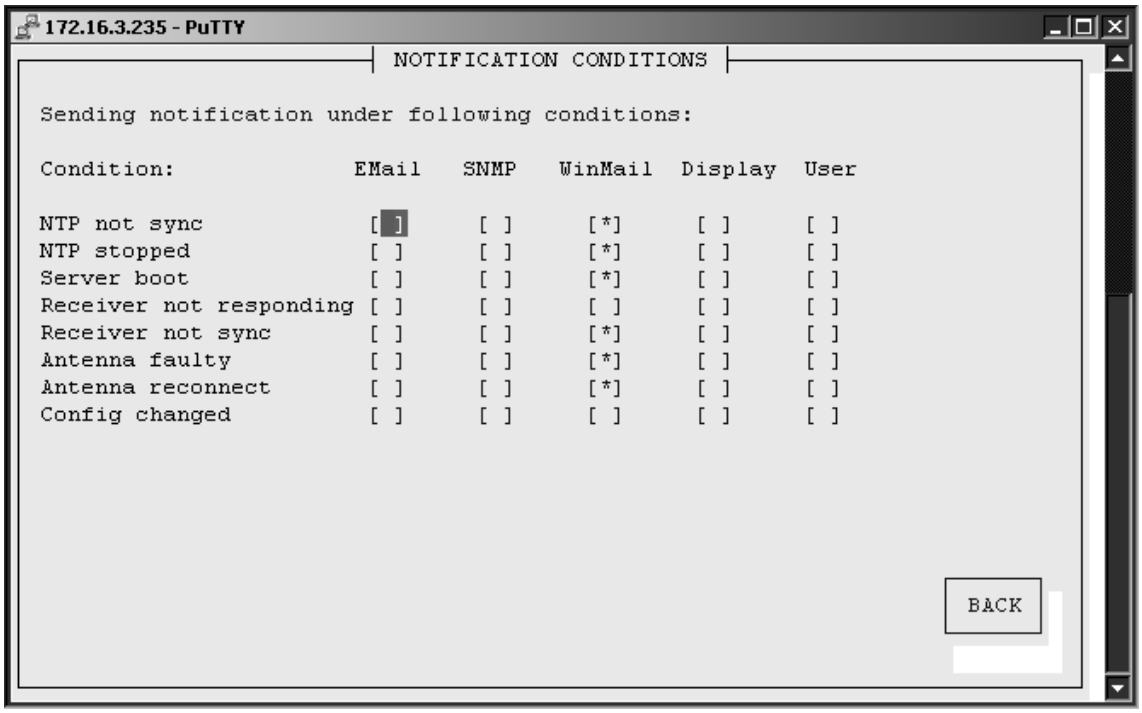
Every event can use a combination of those four notification types, of course you can disable notification for events by disabling all notification types. The configuration of the four notification types can be changed in the upper section of the page, you can control which notification is used for which event by using the button “notification conditions” in the lower part of the page.

Email 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 who is forwarding your mail to the receiver. If your LANTIME system is connected to the internet, it can deliver those e-mails itself.

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

- the LANTIME hostname and domainname should be known to the SMTP smarthost
- a valid nameserver entry is needed
- the domain part of the From: address has to be valid



Windows Popup Messages

Most Microsoft Windows operating systems provide you with a local notification tool. You can send messages via the special Windows protocol in your local network. It is not necessary to enable the NETBIOS protocol of the LANTIME in order to use this notification. On the Windows client side it is necessary to activate the “Microsoft Client for Windows” in the network configuration.

You can enter the Windows computer name of up to two Windows PCs in the appropriate fields. Every message contains a time stamp and a plain text message:

SNMP-TRAP messages

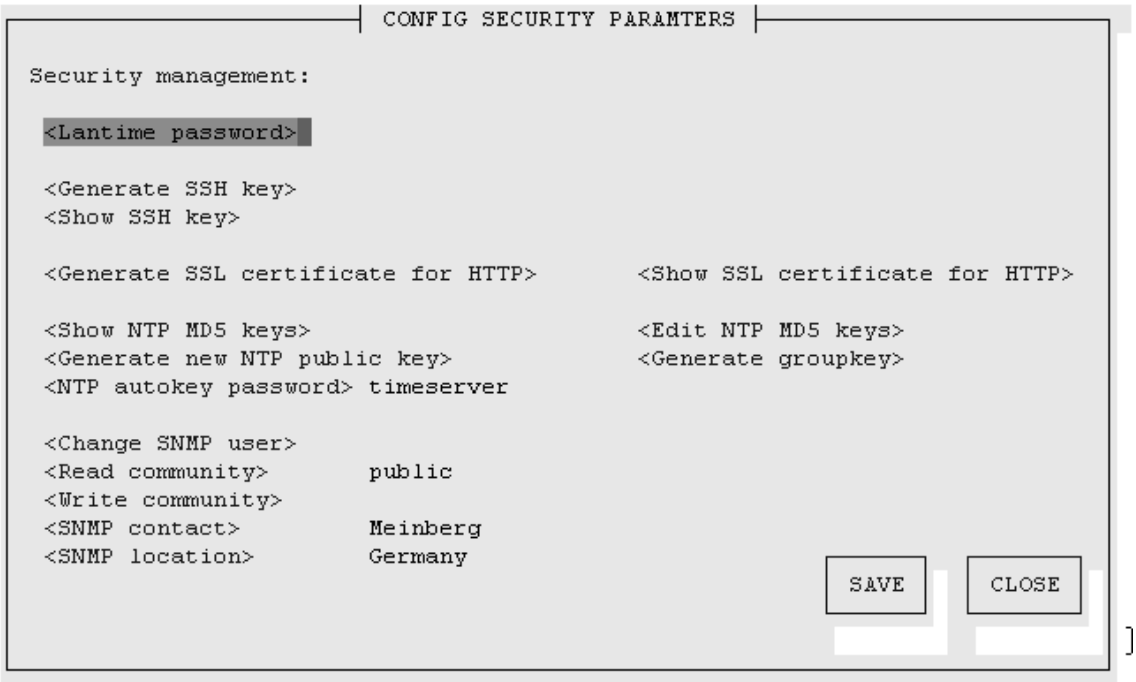
Up to two SNMP trap receiver hosts can be configured in this subsection, you may use IPv4 or IPv6 addresses or specify a hostname. Additionally you have to enter a valid SNMP community string for your trap receiving community. These are mostly independent from the SNMP community strings used for status monitoring and configuration (see SNMP configuration on the “Security” page).
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 (10/100Mbit) and a SNTP client. The time of the display can be received from any NTP server using the SNTP protocol, additionally the display is able to show text messages, which are sent by using special software. 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. An alarm message is shown three times as a scrolling message.

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

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.

CLI Security



Password

On the „Security“ page you can manage all security relevant parameters for your timeserver. In the first section “Login” the administration password can be changed, which is used for SSH, TELNET, FTP, HTTP and HTTPS access. The password is stored encrypted on the internal flash disk and can only be reset to the default value “timeserver” by a “factory reset”, changing all settings back to the factory defaults. Please refer to the LCD configuration section in this manual.

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).

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).

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.

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 authenticates 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.

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.

NTP keys and certificates

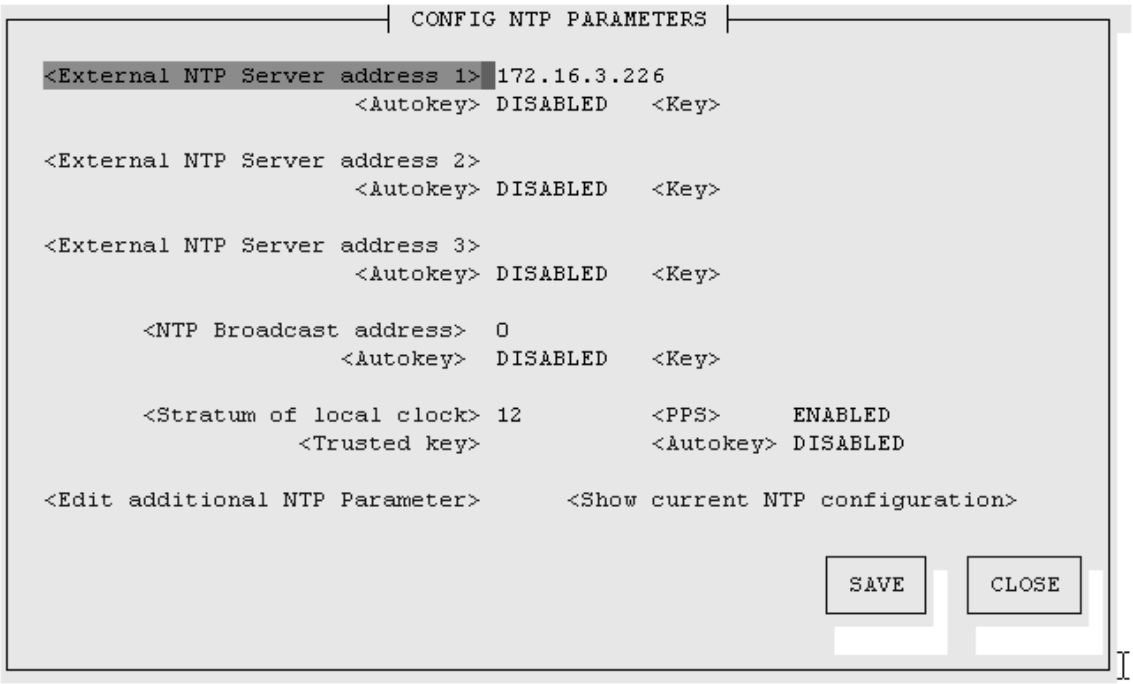
The fourth and fifth section of the „Security” page allow you to create the needed crypto keys and certificates for secure NTP operation (please see NTP authentication below).

The function „Generate new NTP public key“ is creating a new self-signed certificate for the timeserver, which is automatically marked as „trusted“.

Important note: This certificate is depending on the hostname of your LANTIME, it is mandatory to re-create the certificate after changing the hostname. The certificates are build with the internal command “ntp-keygen -T” (ntp-keygen is part of the installed NTP suite). Your LANTIME is using the /etc/ntp/ directory for storing its private and public keys (this is called the “keysdir”). Please refer to the chapter “NTP Autokey” for further information (below).

The two options „Show NTP MD5 key“ and „Edit NTP MD5 keys“ allow you to manage the symmetric keys used by NTP. More about that can be found in the chapter about symmetric keys (below).

CLI NTP Parameter



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

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your LANTIME system and the GPS reference clock. The local clock is only chosen as the NTP time reference after the GPS 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.

Because the GPS 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 ATOM driver of the NTP subsystem, which is directly interpreting the PPS (pulse per second) of the GPS reference clock. The default configuration looks like this:

```
#  ***  lantime  ***
# NTP.CONF for PZF509

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

server  127.127.8.0 mode 130 prefer  # PZF509
fudge   127.127.8.0 time1 0.0099     # 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
```

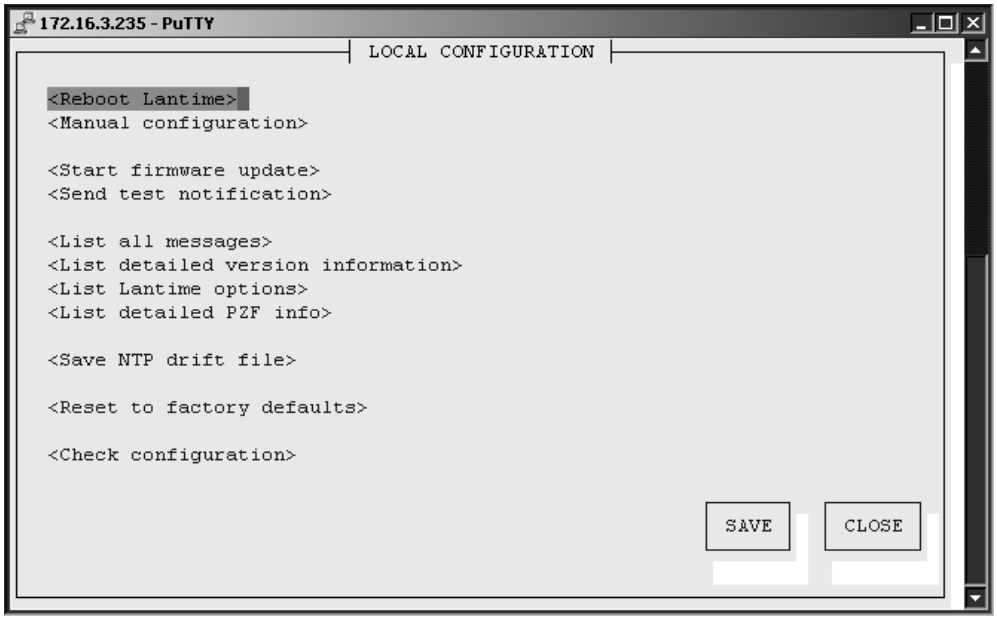
CLI NTP Authentication

Please see the corresponding chapter in the web interface description.

CLI NTP Autokey

Please see the corresponding chapter in the web interface description.

CLI Local



Administrative functions

In the first section there are several functions which may be used by the administrator. The button “Reboot LANTIME” 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 (email, 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 synchronised 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 re-created 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.

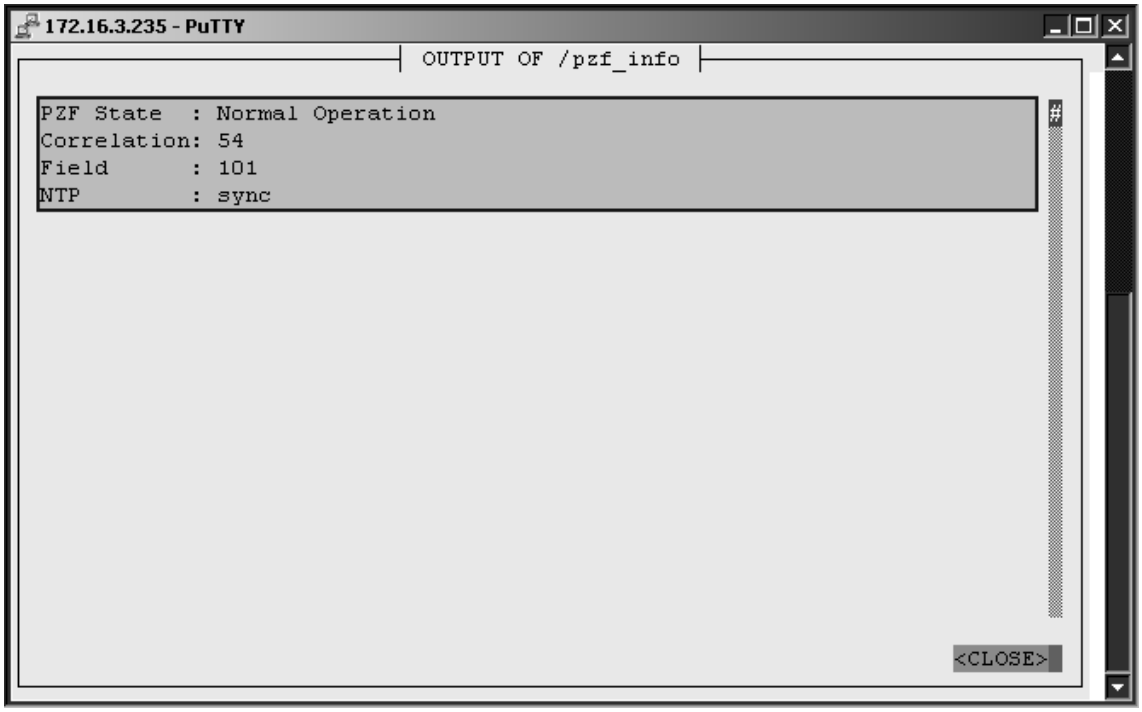
Administrative information

The button „List all messages" displays the SYSLOG of the LANTIME completely. In this log all subsystems create their entries, even the OS 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.

```
Mar 15 13:35:17 LanV4 ntpd[12948]: ntpd 4.2.0@1.1161-r Fri Mar  5
15:58:48 CET 2004 (3)
Mar 15 13:35:17 LanV4 ntpd[12948]: signal_no_reset: signal 13 had
flags 4000000
Mar 15 13:35:17 LanV4 ntpd[12948]: precision = 3.000 usec
Mar 15 13:35:17 LanV4 ntpd[12948]: kernel time sync status 2040
Mar 15 13:35:17 LanV4 ntpd[12948]: frequency initialized 45.212 PPM
from /etc/ntp.drift
Mar 15 13:38:36 LanV4 lantime[417]: NTP sync to PZF
Mar 15 13:38:36 LanV4 lantime[417]: NTP restart
Mar 15 13:45:36 LanV4 proftpd[14061]: connect from 172.16.3.2
(172.16.3.2)
Mar 15 14:01:11 LanV4 login[15711]: invalid password for `root' on
`ttyp1' from `172.16.3.45'
Mar 15 14:01:17 LanV4 login[15711]: root login  on `ttyp1' from
`172.16.3.45'
```

With „List detailed version information" a number of version numbers (including LANTIME software, operating system and NTPD) are shown in a textbox.

The function „List LANTIME Options" shows the hardware options installed in your LANTIME.



Using the button „List detailed PZF information“ gives you the possibility to check detailed PZF status information. The first parameter indicates the state of the DCF77 PZF clock. The next parameter is correlation of the PZF in per cent. The correlation value should be in the range of 60 to 75 per cent. The next parameter is the signal field strength of the DCF77. The last parameter will reflect the state of the internal NTP.

If you need to update the software of your LANTIME, you need a special file update.tgz from Meinberg, which has to be uploaded to the LANTIME by using ftp, SCP or SFTP to the root dir (/update.tgz), after the file transfer is complete, press “Start firmware update”.

Afterwards you are prompted to confirm the start of the update process. The scope of the update only depends on the chosen file.

SNMP Support

The Simple Network Management Protocol (SNMP) has been created to achieve a standard for the management of different networks and the components of networks. SNMP is operating on the application layer and uses different transport protocols (like TCP/IP and UDP), so it is network hardware independent. The SNMP design consists of two types of parties, the agent and the manager. SNMP is a client-server architecture, where the agent represents the server and the manager represents the client. The LANTIME has an integrated SNMP agent, who is designed especially to handle SNMP requests for LANTIME specific status information (including status variables for the internal reference clock). The LANTIME SNMP agent is also capable of handling SET requests in order to manage the LANTIME configuration via SNMP, if your SNMP management software is also supporting this feature. The elements (objects / variables) are organised in data structures called Management Information Base (MIB). The LANTIME includes the standard NET-SNMP MIB and is based on SNMPv1 (RFC 1155, 1157), SNMPv2 (RFC 1901-1908) and SNMPv3. The following SNMP version is installed on the timeserver:

Net-SNMP Version:	5.0.8
Network transport support:	Callback Unix TCP UDP TCPIPv6 UDPIPv6
SNMPv3 Security Modules:	usm
Agent MIB code:	mibII, ucd_snmp, snmpv3mibs, notification, target, agent_mibs, agentx agent_mibs, utilities, meinberg, mibII/ipv6
Authentication support:	MD5 SHA1
Encryption support:	DES

By using the special Meinberg SNMP-agent all important status variables can be read with a SNMP conformant client software. Where applicable, a variable is implemented as string and numeric value, for example allowing SNMP client software to use the information for drawing diagrams or monitor threshold levels.

When using the NET-SNMP suite, you can read all status information your LANTIME offers via SNMP by using the snmpwalk command:

```
snmpwalk –v2c –c public timeserver enterprises.5597
```

```
...mbgLtNtp.mbgLtNtpCurrentState.0 = 1 : no good refclock (->local)
...mbgLtNtp.mbgLtNtpCurrentStateVal.0 = 1
...mbgLtNtp.mbgLtNtpStratum.0 = 12
...mbgLtNtp.mbgLtNtpActiveRefclockId.0 = 1
...mbgLtNtp.mbgLtNtpActiveRefclockName.0 = LOCAL(0)
...mbgLtNtp.mbgLtNtpActiveRefclockOffset.0 = 0.000 ms
...mbgLtNtp.mbgLtNtpActiveRefclockOffsetVal.0 = 0
...mbgLtNtp.mbgLtNtpNumberOfRefclocks.0 = 3
...mbgLtNtp.mbgLtNtpAuthKeyId.0 = 0
...mbgLtNtp.mbgLtNtpVersion.0 = 4.2.0@1.1161-r Fri Mar  5 15:58:56 CET 2004 (3)

...mbgLtRefclock.mbgLtRefClockType.0 = Clock Type: GPS167 1HE
...mbgLtRefclock.mbgLtRefClockTypeVal.0 = 1
...mbgLtRefclock.mbgLtRefClockMode.0 = Clock Mode: Normal Operation

...mbgLtRefclock.mbgLtRefClockModeVal.0 = 1
...mbgLtRefclock.mbgLtRefGpsState.0 = GPS State: sync
...mbgLtRefclock.mbgLtRefGpsStateVal.0 = 1
...mbgLtRefclock.mbgLtRefGpsPosition.0 = GPS Position: 51.9834° 9.2259° 181m
...mbgLtRefclock.mbgLtRefGpsSatellites.0 = GPS Sattelites: 06/06
...mbgLtRefclock.mbgLtRefGpsSatellitesGood.0 = 6
...mbgLtRefclock.mbgLtRefGpsSatellitesInView.0 = 6
...mbgLtRefclock.mbgLtRefPzfState.0 = PZF State: N/A
...mbgLtRefclock.mbgLtRefPzfStateVal.0 = 0
...mbgLtRefclock.mbgLtRefPzfKorrelation.0 = 0
...mbgLtRefclock.mbgLtRefPzfField.0 = 0
```

Please note that you only see the object names (like “mbgLtRefclock.mbgLtRefPzfField”) if you installed the Meinberg MIB files on your client workstation first (please see the web interface or CLI setup tool chapters to find out how to do this).

By using the standard MIB, no NTP get requests are allowed. Only the standard system and network parameters can be accessed (e.g. using the NET-SNMP command “snmpget”).

Only by using the Meinberg MIB the change of configuration parameters is possible (the command „snmpset“ is used to alter a variable, for example).

Configuration over SNMP

The LANTIME timeserver can be configured via several user interfaces. Besides the possibility to setup its parameters with the web interface (HTTP and/or HTTPS) and the direct shell access via telnet or SSH, a SNMP based configuration interface is available.

In order to use the SNMP configuration features of the timeserver, you need to fulfil the following requirements (the system has to be reachable over the network, of course):

a) SNMP has to be activated in the timeservers setup by setting up a RWCOMMUNITY

b) In the SNMP configuration the read-write-access needs to be activated

c) The timeserver-specific MIB files must be present on the clients, they have to be included in the SNMP setup of the client software

a) and b) can be achieved by using the web interface or the shell access, please see the appropriate chapters in this manual. The mentioned MIB files can be found directly on the timeserver unThe /usr/local/share/snmp/mibs, all files with names starting with „MBG-SNMP-“ have to be copied onto the SNMP clients by using the timeservers ftp access (for example). You may also use the web interface, on the page „Local“ you will find a button „Download MIB files“. You will get a tar-archive if you are using the download button, which you have to unpack first. Afterwards, copy all MIB files to the MIB directory on your client(s) and configure your SNMP client software to use them.

Examples for the usage of the SNMP configuration features

The following examples are using the software net-snmp, a SNMP open source project. You will find detailed information at www.net-snmp.org !

To browse the configuration branch of the timeserver-MIB, you could use the following command on a unix system with net-snmp snmp tools installed:

```
root@testhost:/# snmpwalk -v2c -c public timeserver.meinberg.de mbgLtCfg

MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfghostname.0 = STRING: LantimeSNMPTest
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgDomainname.0 = STRING: py.meinberg.de
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgNameserver1.0 = STRING: 172.16.3.1
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgNameserver2.0 = STRING:
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgSyslogserver1.0 = STRING:
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgSyslogserver2.0 = STRING:
[...]
```

To alter a parameter, with net-snmp you would use the snmpset command:

```
root@testhost:/# snmpset -v2c -r 0 -t 10 -c rwsecret timeserver.meinberg.de
mbgLtCfghostname.0 string „helloworld“

MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfghostname.0 = STRING: helloworld

root@testhost:/#
```

Please note that your SNMP request has to be sent with a sufficient timeout (in the above snmpset example this was achieved by using the „-t 10“ option, choosing a timeout of 10 seconds), because after each parameter change, the timeserver reloads its configuration, which takes a few seconds. The request is acknowledged by the SNMP agent afterwards.

To change a group of parameters without reloading the configuration after each parameter, you have to send all parameter changes in one single request. You can do this with the net-snmp snmpset command by specifiying multiple parameters in one command line:

```
root@testhost:/# snmpset -v2c -r 0 -t 10 -c rwsecret timeserver.meinberg.de
mbgLtCfghostname.0 string „helloworld“ mbgLtCfgDomainname.0 string
„internal.meinberg.de“

MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfghostname.0 = STRING: helloworld
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgDomainname.0 = STRING: internal.meinberg.de

root@testhost:/#
```

The available SNMP variables are described in detail in the „SNMP configuration reference“ part of this manual. Additionally, it is recommended to also read the mentioned MIB files.

Further configuration possibilities

Because the timeserver uses a standard version of the net-snmp SNMP daemon (with extended features covering the timeserver-specific functions), all configuration parameters of the SNMPD can be used. The configuration file of the SNMP daemon is located at /usr/local/share/snmp after boot time, the filename is snmpd.conf .

During the boot sequence, this file is created dynamically by using a template file and appending the SNMP parameters stored in the timeserver setup.

If you need to customize the configuration of the timeservers SNMPD (for setting up detailed access control rights for example), you may edit

/mnt/flash/packages/snmp/etc/snmpd_conf.default (which is the mentioned template file). Please note that some lines are appended to this file (as described above), before it is used as /usr/local/share/snmp/snmpd.conf by the snmpd process.

Send special timeserver commands with SNMP

The timeserver is capable of receiving special commands by SNMP in order to reboot the unit or reload its configuration after you manually changed it. A special SNMP variable is reserved for this (mbgLtCmdExecute) and has to be set to a special integer value for each command. The following commands are available:

Reboot(1)
Setting the mbgLtCmdExecute variable to value 1 will reboot the timeserver after a short waiting period of approximately 3-5 seconds.

FirmwareUpdate(2)
This command installs a previously uploaded (with FTP for example) firmware version.

ReloadConfig(3)
The parameters of the timeserver configuration (stored in /mnt/flash/global_configuration) are re-read and afterwards a number of subsystems (e.g. NTPD, HTTPD/HTTPSD, SMBD) will be restarted in order to use those eventually changed settings. Please note that the SNMPD will not be restarted by this command (you have to use reboot instead or restart it manually by killing the process and starting it again in the shell).

GenerateSSHKey(4)
A new SSH key will be generated.

GenerateHTTPSKey(5)
A new HTTPS key will be generated.

ResetFactoryDefaults(6)
The configuration of the timeserver is reset to factory defaults, afterwards an automatic ReloadConfig is executed in order to use these default settings.

GenerateNewNTPAutokeyCert(7)
A new key is generated, it can be used with the NTP AUTOKEY feature.

SendTestNotification(8)
A test message is sent by using all notification methods the timeserver has a configuration for (e.g. mail, winpopup, SYSLOG etc.).

A few examples:
(we are again using the snmpset command which comes with the net-snmp tools).

```
root@testhost:/# snmpset -v2c -r 0 -t 10 -c rwsecret timeserver.meinberg.de
mbgLtCmdExecute.0 int 1

MBG-SNMP-LANTIME-CMD-MIB::mbgLtCmdExecute.0 = INTEGER: Reboot(1)
root@testhost:/#
```

The command shown above is forcing the timeserver to reboot. Instead of using the integer value, you may also enter the command name, as it is defined in the MIB file MBG-SNMP-LANTIME-CMD.txt (and in the command list above).

If you want the timeserver to reload it's configuration file (which you previously uploaded via FTP probably), you would enter this command:

```
root@testhost:/# snmpset -v2c -r 0 -t 10 -c rwsecret timeserver.meinberg.de
mbgLtCmdExecute.0 int ReloadConfig

MBG-SNMP-LANTIME-CMD-MIB::mbgLtCmdExecute.0 = INTEGER: ReloadConfig(3)
root@testhost:/#
```

Please pay attention to the options „-r 0“ (meaning „no retries“) and „-t 10“ (meaning „timeout of 10 secs“) in the above examples. These options avoid multiple executions of the desired command, additionally they give your snmpset command enough time to wait for an acknowledgement from the timeservers snmp agent.

Configuration of the timeserver with SNMP: Reference

The MIB of the timeserver includes the following parts:

SNMP Object	*Name*	*Description*
enterprises.5597	mbgSNMP	Root node of the Meinberg-MIB
mbgSNMP.3	mbgLantime	Root node of the LANTIME MIB
mbgLantime.1	mbgLtNtp	LANTIME NTP status variables
mbgLantime.2	mbgLtRefclock	LANTIME reference time source status variables
mbgLantime.3	mbgLtTraps	LANTIME SNMP traps
mbgLantime.4	mbgLtCfg	LANTIME configuration variables
mbgLantime.5	mbgLtCmd	LANTIME control commands

Further detailed information can be found in the Meinberg MIB files.

Reference of LANTIME SNMP configuration variables:

SNMP branch	*Variable*	*Data type*	*Description*
mbgLtCfgNetwork	mbgLtCfghostname	string	The hostname of the timeserver
	mbgLtCfgDomainname	string	The Domainname of the timeserver
	mbgLtCfgNameserver1	string (IPv4 or IPv6-address)	IP-address of first nameserver
	mbgLtCfgNameserver2	string (IPv4 or IPv6-address)	IP-address of second nameserver
	mbgLtCfgSyslogserver1	string (IPv4 or IPv6-address or hostname)	IP-address or hostname of first syslog-server
	mbgLtCfgSyslogserver2	string (IPv4 or IPv6-address or hostname)	IP-address or hostname of second syslog-server
	mbgLtCfgTelnetAccess	integer (0 = disabled, 1 = enabled)	Telnet access activated?
	mbgLtCfgFTPAccess	integer (0 = disabled, 1 = enabled)	FTP-access activated?
	mbgLtCfgHTTPAccess	integer (0 = disabled, 1 = enabled)	Webinterface activated?
	mbgLtCfgHTTPSAccess	integer (0 = disabled, 1 = enabled)	Encrypted webinterface activated?
	mbgLtCfgSNMPAccess	integer (0 = disabled, 1 = enabled)	SNMP-daemon activated?
	mbgLtCfgSambaAccess	integer (0 = disabled, 1 = enabled)	LANManager-access activated?
	mbgLtCfgIPv6Access	integer (0 = disabled, 1 = enabled)	IPv6-protocol enabled?
	mbgLtCfgSSHAccess	integer (0 = disabled, 1 = enabled)	SSH-access activated?

SNMP branch	*Variable*	*Data type*	*Description*
mbgLtCfgNTP	mbgLtCfgNtpServer1IP	string (IPv4 or IPv6-address or hostname)	First external NTP-server
	mbgLtCfgNtpServer1KEY	integer	Link to the key which should be used for the first NTP-server
	mbgLtCfgNtpServer2IP	string (IPv4 or IPv6-address or hostname)	Second external NTP-server
	mbgLtCfgNtpServer2KEY	integer	Link to the key which should be used for the second NTP-server
	mbgLtCfgNtpServer3IP	string (IPv4 or IPv6-address or hostname)	Third external NTP-server
	mbgLtCfgNtpServer3KEY	integer	Link to the key which should be used for the third NTP-server
	mbgLtCfgStratumLocalClock	integer(0..15)	Stratum-value of the internal system clock of the timeserver
	mbgLtCfgNTPTrustedKey	integer	Link to the key which should be used for the internal reference time source
	mbgLtCfgNTPBroadcastIP	string (IPv4 or IPv6-address)	IP-address, which has to be used for NTP-broadcasts (or multicasts)
	mbgLtCfgNTPBroadcastKey	integer	Link to the key which should be used for outgoing NTP-broadcasts
	mbgLtCfgNTPBroadcastAutokey	integer (0 = disabled, 1 = enabled)	Use autokey for NTP broadcasts?
	mbgLtCfgAutokeyFeature	integer (0 = disabled, 1 = enabled)	Use autokey feature of the NTP server?
	mbgLtCfgAtomPPS	integer (0 = disabled, 1 = enabled)	Atom PPS (pulse per second) activated?
mbgLtCfgEMail	mbgLtCfgEMailTo	string (Liste von EMail-addressn)	One or more (semicolon separated) email address(es). which should receive warnings and alarm notifications from the timeserver
	mbgLtCfgEMailFrom	string (EMail-address)	The EMail-address which is used as the senders address for email notifcations
	mbgLtCfgEMailSmarthost	string (IPv4 or IPv6-address or hostname)	The SMTP-host, which is used for sending mails
mbgLtCfgSNMP	mbgLtCfgSNMPTrapReceiver1	string (IPv4 or IPv6-address or hostname)	First host, which receives notifications sent as SMTP-traps
	mbgLtCfgSNMPTrapReceiver1Community	string	The SNMP community used when sending SNMP-Traps to the first host
	mbgLtCfgSNMPTrapReceiver2	string (IPv4 or IPv6-address or hostname)	Second host, which receives notifications sent as SMTP-traps
	mbgLtCfgSNMPTrapReceiver2Community	string	The SNMP community used when sending SNMP-Traps to the second host
	mbgLtCfgSNMPROCommunity	string	The SNMP community, which has read-only access and therefore can be used to only monitor status variables or configuration values (SNMP V2c)
	mbgLtCfgSNMPRWCommunity	string	The SNMP community, which has read-write access and there for can be used to monitor status variables and get/set configuration values (SNMP V2c)
	mbgLtCfgSNMPContact	string	Contact information (e.g. name of a contact person) of the timeserver
	mbgLtCfgSNMPLocation	string	Location (e.g. building/room number) of the timeserver

SNMP branch	*Variable*	*Data type*	*Description*
mbgLtCfgWinpopup	mbgLtCfgWMailAddress1	string	First receiver of notifications sent as windows popup messages
	mbgLtCfgWMailAddress2	string	Second receiver of notifications sent as windows popup messages
mbgLtCfgWalldisplay	mbgLtCfgVP100Display1IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the first wallmount display used for showing notifications
	mbgLtCfgVP100Display1SN	string (Hexstring)	The serial number of the first wall mount display used for showing notifications (can be found in the setup menu of the display)
	mbgLtCfgVP100Display2IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the second wall mount display used for showing notifications
	mbgLtCfgVP100Display2SN	string (Hexstring)	The serial number of the first wall mount display used for showing notifications (can be found in the setup menu of the display)
mbgLtCfgNotify	mbgLtCfgNotifyNTPNotSync	string(combination)	Exactly one, none or a combination of the following notification types: email=sending an email wmail=sending a winpopup-message snmp=sending a SNMP-trap, disp=showing on wall mount display, syslog=sending a syslog-entry for the event „NTP not synchronized“
	mbgLtCfgNotifyNTPStopped	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „NTP Daemon stopped“
	mbgLtCfgNotifyServerBoot	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Timeserver reboot“
	mbgLtCfgNotifyRefclockNotResponding	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not ready“
	mbgLtCfgNotifyRefclockNotSync	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not synchron“
	mbgLtCfgNotifyAntennaFaulty	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna not connected or dammaged“
	mbgLtCfgNotifyAntennaReconnect	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna reconnected“
	mbgLtCfgNotifyConfigChanged	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Configuration changed“
	mbgLtCfgNotifyLeapSecondAnnounced	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Leap second announced“
mbgLtCfgEthernet	mbgLtCfgEthernetIf0IPv4IP	string (IPv4 IP-address)	IPv4-address of first network interface of the timeserver
	mbgLtCfgEthernetIf0IPv4Netmask	string (IPv4 Netzmaske)	IPv4-netmask of first network interface of the timeserver
	mbgLtCfgEthernetIf0IPv4Gateway	string (IPv4 IP-address)	IPv4-address of the default gateway of the timeservers first network interface
	mbgLtCfgEthernetIf0DHCPClient	integer (0 = disabled, 1 = enabled)	Configure the first network interface of the timeserver with DHCP?

SNMP branch	*Variable*	*Data type*	*Description*
	mbgLtCfgEthernetIf0IPv6IP1	string (IPv6 IP-address)	First IPv6-IP-address of the timeservers first network interface
	mbgLtCfgEthernetIf0IPv6IP2	string (IPv6 IP-address)	Second IPv6-IP-address of the timeservers first network interface
	mbgLtCfgEthernetIf0IPv6IP3	string (IPv6 IP-address)	Third IPv6-IP-address of the timeservers first network interface
	mbgLtCfgEthernetIf0IPv6Autoconf	integer (0 = disabled, 1 = enabled)	Activate autoconf for the IPv6 - configuration of the timeservers first network interface?
	mbgLtCfgEthernetIf0NetlinkMode	integer (0..4)	Configuration of the network-speed and duplex settings of the timeservers first network interface 0 = autosensing, 1 = 10Mbit/s half duplex, 2= 10Mbit/s full duplex, 3=100Mbit/s half duplex, 4=100Mbit/s full duplex

For all additional Ethernet interfaces of the timeserver, „If0“ only has to be replaced with „Ifx“, where „x“ is substituted by the number of the desired Ethernet interface. Example: The IPv4-address of the timeservers third Ethernet interface can be set with mbgLtCfgEthernetIf2IPv4IP !

SNMP Traps

If configured, the LANTIME is sending SNMP traps, which can be received by up to 2 SNMP management systems. These traps can be received by using the NET-SNMP suite tool “snmptrapd”, you can start it on a unix system with “snmptrapd –p” (-p is for output to stdout, -s would use the syslog for output). The corresponding MIB files can be found on the LANTIME at /usr/local/share/snmp/mibs/ , all Meinberg specific MIB files are named “MBG-SNMP…” . Theses MIB files can be downloaded by using the web interface (see “Local” page, “Download MIB files” button), after unpacking the archive file you can import the MIB files into your management system.

The following SNMP-traps are available:

"NTP not sync"	NTP not synchronised to refclock
"NTP stopped"	NTP stopped
"Server boot"	System has rebooted
"Receiver not responding"	no answer from PZF
"Receiver not sync"	DCF77 PZF receiver not synchronised
"Antenna faulty"	DCF77 PZF antenna not connected
"Antenna reconnect"	DCF77 PZF antenna reconnected
"Config changed"	System parameter changed by user

See the „Notification“ page at the web interface and Command Line Interface description to learn how to configure the SNMP trap receivers.

SNMP Trap Reference

All traps can be found under the mbgLtTraps section in the Meinberg MIB. A special trap exists for every notification event the timeserver knows. Please note that the traps are only sent if you configured the notification type “SNMP trap” for the event, otherwise no trap is generated. All traps have a string parameter included, which contains the plain text event message for the appropriate event (you are able to change the default text messages, see web interface and/or CLI setup section to find out how to do this).

Here is a list of all traps the timeserver knows:

mbgLtTrapNTPNotSync (mbgLtTraps.1): Whenever the NTP daemon (ntpd) looses sync, it will generate this trap and send it to the configured SNMP trap receivers.

mbgLtTrapNTPStopped (mbgLtTraps.2): This trap is sent when the NTP daemon stopped, manually or because of an error condition.

mbgLtTrapServerBoot (mbgLtTraps.3): After finishing the boot process, this trap is generated.

mbgLtTrapReceiverNotResponding (mbgLtTraps.4): Trap to be sent when the internal receiver of the timeserver is not responding.

mbgLtTrapReceiverNotSync (mbgLtTraps.5): If the internal receiver looses sync, the SNMP trap receivers will receive this trap.

mbgLtTrapAntennaFaulty (mbgLtTraps.6): This trap will be sent whenever the timeserver recognises a broken connection to the antenna of the receiver.

mbgLtTrapAntennaReconnect (mbgLtTraps.7): After the connection to the antenna has been re-established, this trap is sent.

mbgLtTrapConfigChanged (mbgLtTraps 8): After reloading its configuration, the timeserver generates this trap.

mbgLtTrapLeapSecondAnnounced (mbgLtTraps 9): If a leap second has been announced by the internal GPS receiver, this trap will be sent.

mbgLtTrapTestNotification (mbgLtTraps 99): This trap is sent whenever you are requesting a test notification; it is only used for testing the connection between the timeserver and your SNMP trap receivers.

Attachment

Technical Information

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!

Danger of explosion in case of inadequate replacement of the lithium battery. Only identical batteries or batteries recommended by the manufacturer must be used for replacement. The waste battery must be disposed as proposed by the manufacturer of the battery.

Technical Specifications LANTIME Multipac

HOUSING:	Metal desktop case, Schroff EUROPAC lab HF Front panel: 1U/84HP (43mm high / 483mm wide)
PROTECTION RATING:	IP20
PHYSICAL DIMENSIONS:	483mm wide x 43mm high x 286mm deep

Rear Panel Connectors

Name	Type	Signal	Cable
Network	RJ-45	Ethernet	shielded data line
Time Sync Error	DFK		
2 x Network (Option)	RJ-45	Ethernet	shielded data line
PPS, PPM,	9 pin SUB-D	TTL	shielded line
10MHz		TTL	shielded line
Antenna	BNC	77,5kHz	shielded coaxial line
Power supply	power cord receptacle		power supply cord

Safety instructions for building-in equipment

This building-in equipment has been designed and tested in accordance with the requirements of Standard IEC 950 "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 IEC 950 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 16A fuse in the power installation system.
- Disconnection of the equipment from mains is done by pulling the mains plug.

CE-Label

CE

EN 60950

Safety of Information Technology Equipment,
including Electrical Business Equipment

Electromagnetic compatibility

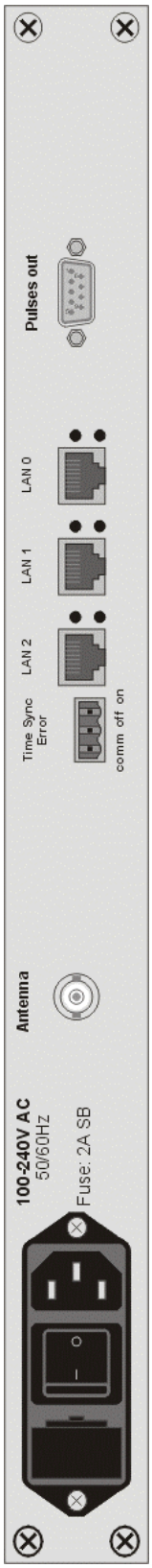
EN50081-1

Electromagnetic compatibility (EMC). Generic emission standard. Part 1: Residential, commercial and light industry

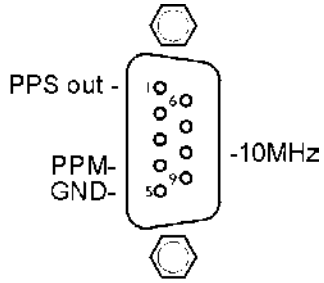
EN50082-2

Electromagnetic compatibility (EMC). Generic immunity standard. Part 2: Industrial environment

Rearview LANTIME



SUB-D Connector Assignments



Pulses out

Technical specifications PZF509

RECEIVER:	Preamplifier with two post-connected receiver channels for best aquisition and tracking of the DCF-signals.
CONTROL OF RECEPTION:	The DCF-signal is checked for minimum field strength by microprocessor. The result is indicated by LED. In addition, the value of the digitized field strength is displayed in menu 'FIELD'.
BATTERY-BACKUP:	In case of power failure an internal realtime clock runs crystal-precise. Important parameters are stored in the system-RAM. Life time of lithium battery: 10 years minimum Option: capacitance-backup for about 150 hours
INTERFACES:	Two independant asynchronous serial ports (internal RS232)
PULSE OUTPUTS:	Active-high and active-low pulses per minute and per second, TTL-level, pulse duration 200ms
ACCURACY OF PULSES:	Time delay of two systems PZF509 with a maximum distance of 50km: typ. 20µs, max. 50µs Time shifting of successive pulses: max. 1.5µs
PROPAGATION-TIME COMPENSATION:	The signal delay is compensated if the distance of the receiver to the transmitter is given.
STANDARD FREQUENCIES:	10 MHz are synchronized to DCF by a digital PLL. Accuracy in synchronized state: $+/- 5 \cdot 10^{-9}$ (short term stability) Accuracy in unsynchronized state: $1 \cdot 10^{-8}$ for one hour 77.5 kHz, 155 kHz und 310 kHz derived from receiver-PLL Accuracy in synchronous state: $+/- 5 \cdot 10^{-7}$ (short term stability)
TERMINAL CONNECTION:	Blade-connector strip VG64, DIN 41612 Sub-miniatur coaxial HF-connector (SMB internal)
BOARD DIMENSIONS:	Eurocard size 100mm x 160mm, Epoxy 1,5mm Front panel 12TE (61mm)
ANTENNA:	Ferrite antenna in plastic housing
HUMIDITY:	Relativ humidity 85% max.
TEMPERATURE RANGE:	0° - 60° Celsius
POWER SUPPLY:	+ 5V, approx. 330mA.

Signal description PZF509

Name	Pin	Function
GND	32a+c	Reference potential
VCC in (+5V)	1a+c	+5V power supply
VDD in (+12V)	2a+c	+12V power supply, reserved
DCF_MARK out	4c	DCF77 Emulation, TTL level, active high pulse duration: 100ms or 200ms
P_SEC out	6c	Pulse per second, TTL-level, active high
/P_SEC out	6a	Pulse per second, TTL-level, active low
P_MIN out	8c	Pulse per minute, TTL-level, active high
/P_MIN out	8a	Pulse per minute, TTL-level, active low
77,5kHz out	10c	77.5kHz frequency output, TTL-level
155kHz out	11c	155kHz frequency output, TTL-level
310kHz out	12c	310kHz frequency output, TTL-level
100 kHz out	10a	100kHz frequency output, TTL-level
1 MHz out	11a	1MHz frequency output, TTL-level
10 MHz out	12a	10MHz frequency output, TTL-level
F_SYNTH out	21c	Synthesizer frequency, TTL-level
F_SYNTH_OD out	22c	Synthesizer frequency, open-drain
F_SYNTH_SIN out	23c	Synthesizer frequency, sinewave
COM0 TxD out	26c	COM0 RS-232 output
COM0 RxD in	30c	COM0 RS-232 input
COM1 TxD out	24c	COM1 RS-232 output
COM1 RxD in	29c	COM1 RS-232 input
/BOOT in	4a	Input for activating the bootstrap-loader
TIME_SYN out	19c	Status output, TTL-level, high if synchronous
/RESET in/out	9c	RESET-pin, reserved for expansions Do not connect
SDA, SCL, SCL_EN	Serial bus for expansions, do not connect	
Reserved		Reserved for future expansions, do not connect

Rear Connector Pin Assignments PZF509

	a	c
1	VCC in (+5V)	VCC in (+5V)
2	VDD in (+12V)	VDD in (+12V)
3		
4	/BOOT in	DCF_MARK out
5		reserved
6	/P_SEC out	P_SEC out
7		
8	/P_MIN out	P_MIN out
9		/RESET in/out
10	100 kHz out	77,5 kHz out
11	1 MHz out	155 kHz out
12	10 MHz out	310 kHz out
13		SCL
14		SCL_EN
15		SDA
16		
17		reserved
18		
19		TIME_SYN out
20		
21		F_SYNTH out
22		F_SYNTH_OD out
23		F_SYNTH_SIN out
24		COM1 TxD out
25		
26		COM0 TxD out
27		reserved
28		reserved
29		COM1 RxD in
30		COM0 RxD in
31		
32	GND	GND

DIN 41612 connector, Typ C 64, row a + c

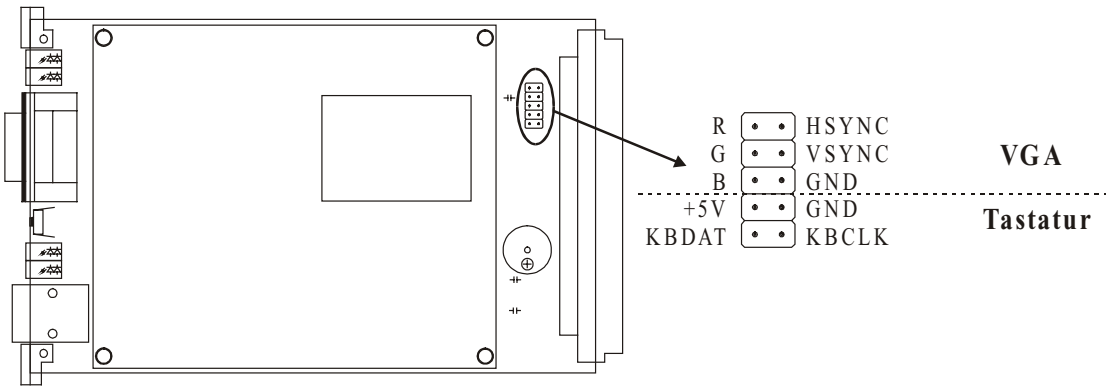
Technical Specifications LAN CPU

PROZESSOR:	Geode^{TM} GX1 with 266MHz
MAIN MEMORY:	32 MB (to 64 MB upgradeable)
CACHESPEICHER:	16 KB 2nd Level Cache
FLASHDISK:	8 MB (until max. 72 MB)
NETZWORK CONNECTOR:	10/100MBIT with RJ45-Jack DAVICOM DM9102AEthernet NIC Controller
SERIAL - INTERFACE:	Four serial RS232-Ports 16550 compatible to FIFO - RS232 9-pol. DSUB-male connector - three RS232 male connector according to DIN 41612, type C 96 (only TxD, RxD, DCD)
PARALLEL INTERFACE :	One LPT-Port male connector type C 96
IDE-BUS:	Primary IDE-Bus male connector type C 96
VGA-CONNECTION:	10-pol pin contact strip
KEYBOARD CONNECTION:	10-pol pin contact strip
STATE LED´s:	- power supply - 'Connect', 'Activity' and 'Speed' of the network connection
POWER REQUIREMENTS:	5V ± 5%, @1A
FRONTPANEL:	3 HE / 4 TE (128 mm high x 20,3 mm wide)
CONNECTOR:	according to DIN 41612, type C 96, rows a+b+c (male) DSUB-plug (9-pol) RJ45-jack
AMBIENT TEMPERATURE:	0 ... 50°C
HUMIDITY:	85% max.

Rear Connector Pin Assignments LAN CPU

	c	b	a	
1	VCC in (+5V)	VCC in (+5V)	VCC in (+5V)	
2	VCC in (+5V)	VCC in (+5V)	VCC in (+5V)	
3	GND	GND	GND	
4	PPS in	/AFD out	/STB out	
5	/ERR in	/SLIN out	/INIT out	
6	D5 in/out	D6 in/out	D7 in/out	LPT1
7	D2 in/out	D3 in/out	D4 in/out	
8	/ACK in	D0 in/out	D1 in/out	
9	/SLCT in	PE in	/BUSY in	
10	GND	GND	GND	
11	GND	GND	GND	
12	DIAG_S in/out	/CS1 out	/CS3 out	
13	A0 out	A1 out	A2 out	
14	RDY in	/AK out	INTRQ in	
15	DRQ in	/IOW out	/IOR out	
16	D15 in/out	D0 in/out	D14 in/out	Primary IDE
17	D1 in/out	D13 in/out	D2 in/out	
18	D12 in/out	D3 in/out	D11 in/out	
19	D4 in/out	D10 in/out	D5 in/out	
20		D9 in/out	D7 in/out	
21	D6 in/out	D8 in/out	/HDRST out	
22	GND	GND	GND	
23	Rx+ in	Tx- out	Tx+ out	
24	Rx- in	LED LINK out	LED ACTIVITY out	Ethernet
25		LED SPEED 100M out	LED SPEED10M out	
26	GND	GND	GND	
27	RxD4 in	TxD4 out	DCD4 in	
28	RxD3 in	TxD3 out	DCD3 in	RS232
29	RxD2 in	TxD2 out		
30	RxD1 in	TxD1 out	DCD1 in	
31	GND	GND	GND	
32	GND	GND	GND	

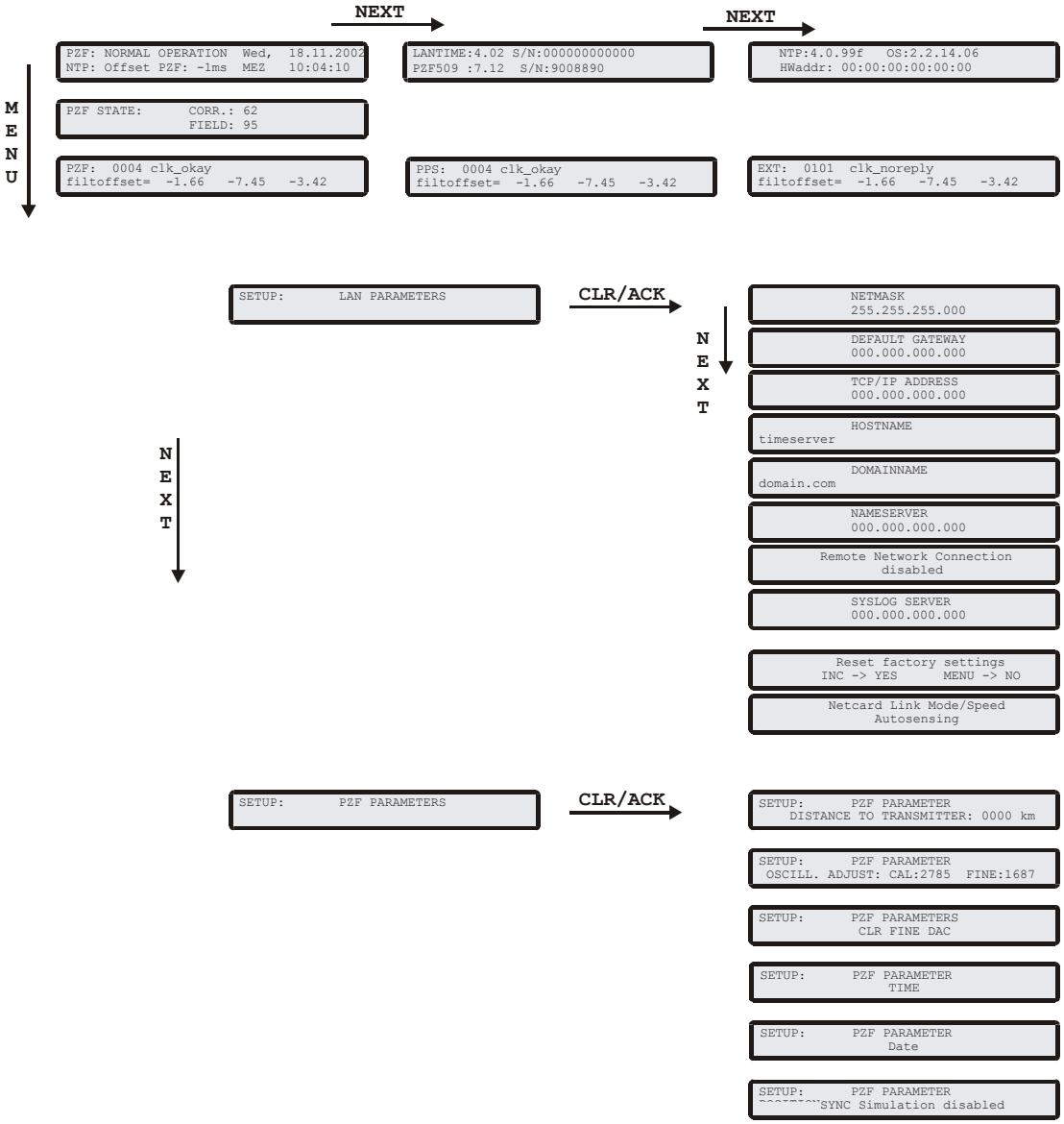
VGA, Keyboard Connector Pin Assignments



Technical Specifications Power Supply

INPUT:	85 ... 264V AC, 47 ... 63Hz, 1A/230V, 2A/115V	
FUSE:	electronic	
CURRENT LIMITING:	105 - 150% $I_{out\ nom}$	
OUTPUTS:	$V_{out}1$:	5.05V / 5A
	$V_{out}2$:	+12V / 2.5A
	$V_{out}3$:	-12V / 0.5A
TOTAL LOAD:	max. 61Watt	
CONNECTORS:	screw terminal	
HOUSING:	metal housing : 159mm x 97mm x 38mm	
AMBIENT TEMPERATURE:	-10°C ... +60°C	
HUMIDITY:	90% max.	

Menu Quick Reference



Declaration of Conformity

Hersteller Manufacturer	**Meinberg Funkuhren** **Auf der Landwehr 22** **D-31812 Bad Pyrmont**

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

Produktbezeichnung Product Name	**NTP Timeserver**
Modell / Typ Model Designation	**LANTIME/PZF**

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

EN55022, 5/99, Class B	Grenzwerte und Meßverfahren für Funkstörungen von informationstechnischen Einrichtungen Limits and methods of measurement of radio interference characteristics of information technology equipment
EN55024, 5/99	Grenzwerte und Meßverfahren für Störfestigkeit von informationstechnischen Einrichtungen Limits and methods of measurement of Immunity characteristics of information technology equipment
EN 61000-3-2, 3/96	Elektromagnetische Verträglichkeit (EMV) Grenzwerte für Oberschwingungsströme EMC limits for harmonic current emissions
EN 61000-3-3, 3/96	Elektromagnetische Verträglichkeit (EMV) Grenzwerte für Spannungsschwankungen und Flicker in Niederspannungsnetzen Limitation of voltage fluctuation and flicker in low-voltage supply systems
EN 60950/96	Sicherheit von Einrichtungen der Informationstechnik Safety of information technology equipment

gemäß den Bestimmungen der Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit.
following the provisions of Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Bad Pyrmont, den 08.05.2002

Manual Display configuration

send2display Version 0.1

usage:
send2display -h hostname -s serialnumber [options]

Valid options are:
-h, --host H Uses H as the hostname of the display unit
-s, --serialnumber S Uses S as the serialnumber of the display (e.g. 03A00C7F)
-c, --clear M Clear message M (0-31)
-b, --beep Beeper sound while showing the message
-a, --clearall Clear all messages of the display
-m, --message M Create/change message M (0-31, default = 0)
-e, --executions E Sets number of consecutive executions to E (1-9, default = 1)

-q, --quiet Quiet mode (no program output to stdout/stderr)
-v, --verbose Verbose mode (output of debugging info on stdout)
-?, --help Show help message

Defining messages
==========

a) Static or flashing text:
You can define a maximum of 9 lines for a message.
Start with -(x) "text", where (x) represents the line number.

-1, --line1 "text" Set text for line 1
-2, --line2 "text" Set text for line 2
...

You can set the duration and mode for each line separately. Specifiy the following options
directly after the text-definition of a line:
-f, --noflash Change line mode to static (default is flashing)
-d, --duration X Set the duration of the line to x seconds (default is 3 seconds)

b) Scrolling text:
You can define a maximum of 241 characters per scrolling message. If you want the message to "softly" end,
simply add some spaces to the end of your text (attention: text and spaces must be no more than
241 chars in length).
-t, --scrolltext "text" Set scrolltext

If you want the message (any type) to appear periodically, you can set the time interval with:

-D, --periodday D Display message every D days
-H, --periodhour H Display message every H hours
-M, --periodminute M Display message every M minutes

(You can combine these options. Default is: message is displayed only once)

Possible error codes: 1=parameter error, 2=no ACK from display, 3=network error

Examples:

send2display -h 172.16.3.251 -s 0a03007f -m1 -e2 -1"Hello World" -d5 -2"what a nice day" -d3
(shows two lines of text (2 times), 1st line is shown for 5 seconds and 2nd line for 3 seconds)

send2display -h 172.16.3.251 -s 0a03007f -m1 -e1 -1"Oops" -H2 -M30
(shows one line of text every 2 hours and 30 minutes, a sound (beep) can be heared while
the message is displayed)

send2display -h 172.16.3.251 -s 0a03007f -c1
(deletes the message 1, so no more beeps every 2:30 hrs ...)

send2display -h 172.16.3.251 -s 0a03007f -t"Hello world... " -e3
(shows a scrolling message with soft end, repeating it 3 times.

Global Configuration File

This file contain all global parameter of the LANTIME. You can find this file on the write protected flash disk at /mnt/flash/global_configuration:

```
#-----------------------
#  Configuration File
#
#-----------------------

# Configuration File Section
Configuration File Version Number         :4.05
Configuration File Last Change            :Mon Mar 15 07:44:21 2004

# Network Parameter Section
Hostname                          [ASCII,50]:LanV4
Domainname                        [ASCII,50]:py.meinberg.de
Nameserver 1                            [IP]:
Nameserver 2                            [IP]:
Syslogserver 1                    [ASCII,50]:
Syslogserver 2                    [ASCII,50]:
Telnet Port active                    [BOOL]:1
FTP Port active                       [BOOL]:1
SSH active                            [BOOL]:1
HTTP  active                          [BOOL]:1
HTTPS active                          [BOOL]:1
SNMP  active                          [BOOL]:1
SAMBA active                          [BOOL]:0
IPv6  active                          [BOOL]:1

# NTP Section
External NTP Server 1 IP          [ASCII,50]:
External NTP Server 1 KEY               [NUM]:
External NTP Server 1 AUTOKEY         [BOOL]:
External NTP Server 2 IP          [ASCII,50]:
External NTP Server 2 KEY               [NUM]:
External NTP Server 2 AUTOKEY         [BOOL]:
External NTP Server 3 IP          [ASCII,50]:
External NTP Server 3 KEY               [NUM]:
External NTP Server 3 AUTOKEY         [BOOL]:
NTP Stratum Local Clock         [NUM,0..15]:12
NTP Trusted Key                         [NUM]:
NTP AUTOKEY feature active            [BOOL]:0
NTP ATOM PPS active                   [BOOL]:1
NTP Broadcast TCPIP                     [IP]:0
NTP Broadcast KEY                      [NUM]:0
NTP Broadcast AUTOKEY                 [BOOL]:

# EMail Section
EMail To Address                  [ASCII,50]:
EMail From Address                [ASCII,50]:
EMail Smarthost                   [ASCII,50]:

# SNMP Section
SNMP Trap Receiver Address 1      [ASCII,50]:
SNMP Trap Receiver Community 1    [ASCII,50]:
SNMP Trap Receiver Address 2      [ASCII,50]:
SNMP Trap Receiver Community 2    [ASCII,50]:
SNMP V3 User Name                 [ASCII,50]:root
SNMP Read Community String        [ASCII,50]:public
SNMP Write Community String       [ASCII,50]:
```

```
SNMP Contact String             [ASCII,50]:Meinberg
SNMP Location String            [ASCII,50]:Germany

# Windows Messages Section
WMail Address 1                 [ASCII,50]:
WMail Address 2                 [ASCII,50]:

# VP100 Display Section
VP100 Display Address 1         [ASCII,50]:
VP100 Display Sernum  1         [ASCII,50]:
VP100 Display Address 2         [ASCII,50]:
VP100 Display Sernum  2         [ASCII,50]:

# Notification Section
Notification on NTP_not_sync        [CASE]:
Notification on NTP_stopped         [CASE]:
Notification on Server_boot         [CASE]:
Notification on Refclock_not_respon.[CASE]:
Notification on Refclock_not_sync   [CASE]:
Notification on Antenna_faulty      [CASE]:
Notification on Antenna_reconnect   [CASE]:
Notification on Config_changed      [CASE]:
Notification on Leap second announ. [CASE]:

# Ethernet Parameter Section
ETH0 IPv4 TCPIP address               [IP]:0
ETH0 IPv4 NETMASK                     [IP]:0
ETH0 IPv4 GATEWAY                     [IP]:0
ETH0 DHCP CLIENT                    [BOOL]:1
ETH0 IPv6 TCPIP address 1             [IP]:
ETH0 IPv6 TCPIP address 2             [IP]:
ETH0 IPv6 TCPIP address 3             [IP]:
ETH0 IPv6 Autoconf                  [BOOL]:1
ETH0 Net Link Mode                [NUM,0:4]:
ETH0 Bonding Group                [NUM,0:4]:
```

Global Option File

This file contain all global options for special hardware configuration of the LANTIME. Do not modify this file. You can find this file on the write protected flash disk at /mnt/flash/global_options:

```
#GLOBAL OPTIONS

NUMBER ETHERNET INTERFACES: 1
SYSTEM LAYOUT: 0
SYSTEM ADV LAYOUT: 0
SYSTEM LANGUAGE: 0
SYSTEM PARAMETER:
```

Third party software

The LANTIME network timeserver is running a number of software products created and/or maintained by open source projects. A lot of people contributed to this and we explicitly want to thank everyone involved for her/his great work.

The used open source software comes with its own license which we want to mention below. If one of the licenses for a third party software product is violated, we will as soon as possible apply any changes needed in order to be conform with the corresponding license after we acknowledged about that violation.

If a license for one of the software products states that we have to provide you with a copy of the source code or other material, we will gladly send it to you on data media via normal post or by email upon request. Alternatively we can provide you with a link to a download location in the internet, allowing you to download the most actual version. Please note that we have to charge you for any incurred expenses if you choose to receive the source code on data media.

Operating System GNU/Linux

The distribution of the GNU/Linux operating system is covered by the GNU General Public License (GPL), which we included below.

More informations about GNU/Linux can be found on the GNU website (www.gnu.org) and on the website of GNU/Linux (www.linux.org).

Our version of the Linux kernel has been optimized for the time server application by applying the so-called PPSkit-patch from Ulrich Windl.

Samba

The Samba software suite is a collection of programs, which implement the Server Message Block (SMB) protocol for unix systems. By using Samba your Lantime is capable of sending windows popup messages and serves request for network time by clients using the NET TIME command.

The distribution of Samba is covered – like GNU/Linux – by the GNU General Public License, see below.

The website of the Samba project (or a mirror) can be reached at www.samba.org !

Network Time Protocol Version 4 (NTP)

The NTP project, lead by David L. Mills, can be reached in the internet at www.ntp.org. There you will find a wealthy collection of documentation and informations covering all aspects of the application of NTP for time synchronization purposes. The distribution and usage of the NTP software is allowed, as long as the following notice is included in our documentation:

```
*********************************************************************
*                                                                   *
* Copyright (c) David L. Mills 1992-2004                            *
*                                                                   *
* Permission to use, copy, modify, and distribute this software     *
* and its documentation for any purpose and without fee is hereby   *
* granted, provided that the above copyright notice appears in all  *
* copies and that both the copyright notice and this permission     *
* notice appear in supporting documentation, and that the name      *
* University of Delaware not be used in advertising or publicity    *
* pertaining to distribution of the software without specific,      *
* written prior permission. The University of Delaware makes no     *
* representations about the suitability this software for any       *
* purpose. It is provided "as is" without express or implied        *
* warranty.                                                         *
*                                                                   *
*********************************************************************
```

mini_httpd

For our web based configuration tool (HTTP and HTTPS) we use mini_httpd from ACME Labs. The distribution and usage of this program is free provided that the following notice appears in the documentation:

```
Copyright © 2000 by Jef Poskanzer <jef@acme.com>.  All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.
```

Find out more regarding mini_httpd at the ACME Labs homepage (www.acme.com).

GNU General Public License (GPL)

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in

the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

  1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

  2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

    a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

    b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

    c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

  3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

    a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

    b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the

integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Reference

[Mills88] Mills, D. L., "Network Time Protocol (Version 1) - specification and implementation", DARPA Networking Group Report RFC-1059, University of Delaware, July 1988

[Mills89] Mills, D. L., "Network Time Protocol (Version 2) - specification and implementation", DARPA Networking Group Report RFC-1119, University of Delaware, September 1989

[Mills90] Mills, D. L., "Network Time Protocol (Version 3) - specification, implementation and analysis", Electrical Engineering Department Report 90-6-1, University of Delaware, June 1989

Kardel, Frank, "Gesetzliche Zeit in Rechnernetzen", Funkuhren, Zeitsignale und Normalfrequenzen, Hrsg. W. Hilberg, Verlag Sprache und Technik, Groß-Bieberau 1993

Kardel, Frank, "Verteilte Zeiten", ix Multiuser-Multitasking-Magazin, Heft 2/93, Verlag Heinz Heise, Hannover 1993