MANUAL

LANTIME M600 MRS PTP

Multi Reference Source NTP Server with PTP Option

12th November 2010

Meinberg Radio Clocks GmbH & Co. KG

Table of Contents

1 Impressum

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

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

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

Date: 2010-11-11

2 Quick Start

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

Approximately one minute after power up display will change to the following screen to wait for OCXO HQ oscillator warmed up:

```
        MEINBERG LANTIME
  is booting...  please wait...
  .......
```

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

```
                              F]
12:00:00  UTC               ↵
          Tue, 01.01.2008

NTP: Offs. 1ms        Stratum: 1
MRS: sync to GPS      XTL:SYNC  SVs:9/10
PTP: ok  PTP_SLAVE    GM:00:00:00:00:00:00
Press F1 for help or F2 for setup overview
```

The internal reference clock (HQ OCXO) is either controlled by an installed GPS receiver or by external time sources (depending on Options like IRIG in or PPS in). The priorities for this regulation can be defined in the settings. Press the following buttons to set up the MRS mode: ''i,g,g,g''

```
     MRS Status
  -> Setup Input Priorities <-
     Setup Fixed Offsets
     Setup Precisions
```

The priorities for the external reference sources will be setup in the next menu. The reference source with the highest priority and has been synchronized will be the master to discipline the internal OCXO of the GPS/MRS module:

```
   MRS Input Priorities      F]
                             ↵
1.GPS          is master   : -10ns
2.PPS in       is available : -20ns
3.IRIG         no signal    : n/a
4.NTP          is available : -30.000us
2.PTP (IEEE1588)is available : -300ns
```

If the GPS receiver remains asynchronous the number of satellites in view and the good satellites are to check

(press buttons „i,g,i,g,i,g" from main menu). The antenna has to be installed without any obstructions to the sky.

```
     GPS Receiver Position
  -> Satellite Constellation <-
     GPS Status & Version
```

```
     SATELLITE CONSTELLATION
     satellites in view: 5
      good satellites  : 5
     selected set: 04 09 21 17
```
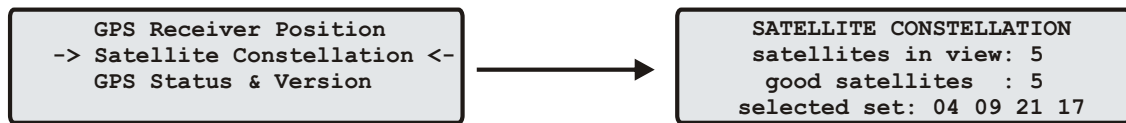
For first time installation enter TCP/IP address, netmask and default gateway. To get an overview of the current configuration press F2 from main menu. Press F2 again to enter SETUP configuration page. Please ask your administrator for proper TCP/IP configuration:

```
     Global Configuration
  ->Network Interfaces  <-
     Network Services

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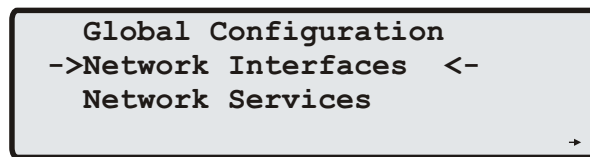
Then press 3 times the OK button to change to IPV4 ETH0 configuration page to enter the IP address, netmask and the default gateway:

```
ETH0: -> DHCP:disable <-
        ADDRESS: 192.168.10.20
        NETMASK: 255.255.255.000
   DEF.GATEWAY: 192.168.10.1
```
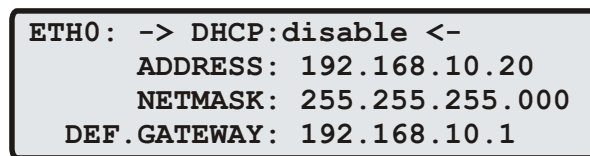
NOTE: These settings are related to the first Ethernet connection (ETH0).

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

Default user: root
Default password: timeserver

3 Network Timeserver synchronized by multiple reference time sources

A 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 these references (hybrid system). External references are also possible. Up to 7 NTP timeservers, external 1PPS or 10 MHz signals, external IRIG Time Code signals or optionally a PTP IEEE1588 grandmaster can be used to control the internal oscillator.

The LANTIME M600/MRS is a set of equipment composed of a GPS satellite controlled clock, a single-board computer with integrated network board, and a power supply, all installed in a metal 19 inch modular chassis and ready to operate. Optionally a additional network card with hardware timestamping for the Precision Time Protocol (PTP) IEEE 1588 will be integrated. A simplified LINUX operating system is installed on the single-board computers flash disk. Eight push buttons and a VFD display can be used to configure and monitor the timeserver. After the network connection has been established the timeserver 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.

4 The Modular System LANTIME

LANTIME is a set of equipment composed of a satellite controlled clock GPS170, a single-board computer SBC LX800 500 MHz with integrated network card, and a power supply unit, 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.

1. VF Display
2. Function keys: 4 - way buttons;
                      F1, F2, OK, ESC
3. Status LEDs: Ref. Time, Time Service,
                      Network, Alarm
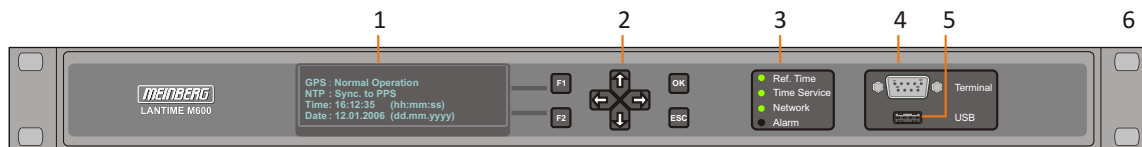
4. Terminal port, RS232 timestring output
5. USB connector
6. Bracket for 19" rack mount

1. Power switch
2. Mains socket (see chapter power supply)
3. GPS antenna, BNC
4. RS232 output, serial interface, time telegram
5. RS422 output, serial interface, PPS
6. Error relais output
7. PPS / Frequency input - 10MHz, TTL via BNC connector
8. Time Code (AM and DCLS) input, BNC connector
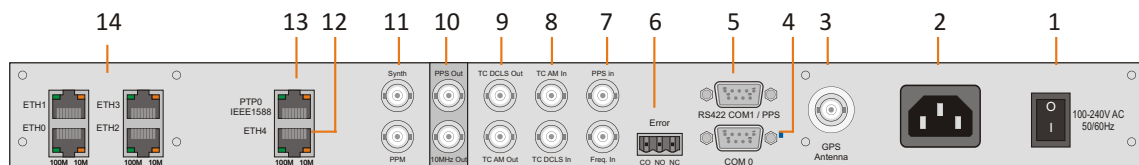
9. IRIG-B Time Code (AM and DCLS) output, BNC
10. PPS (PulsePerSecond) / 10MHz Freq. output, BNC
11. Frequency Synth. (0.1 - 10MHz) and
    PPM (PulsePerMinute) output, BNC
12. IEEE1588 PTPv2, RJ-45 connector
13. 1 x Network connector: ETH4 - 10/100 Mbit, RJ45
14. 4 x Network connectors: ETH0 - ETH3,
                              10/100 Mbit, RJ45

The implemented NTPD distributes the reference time from the GPS 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 from the front panel of LANTIME. The network address or the equivalent name of LANTIME has to be shown to all NTP clients in the TCP/IP network.

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

4.1 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 e-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)

4.2 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 RJ45/10/100 MBit 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

4.3 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 e-mail notification

- Simulation of a synchronous radio clock in order to operate without antenna

4.4 Options

- Additional Ethernet RJ45 connectors available (eight in 3U housing, four in 1U housing and eight additional connectors in HS - XL railmount housing)

- Frequency and pulse outputs via BNC connectors (e.g. 10 MHz, 2.048 MHz, PPS)

- Higher free running accuracy with optional oscillators (OCXO)

- IRIG-B outputs

- ANZ14NET or VP100/20/NET as display connected via network

4.5 Why to use a Network Time Server?

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

- Particularly in the case of our LANTIME you or a responsible person can be notified by mail or SNMP trap if there is a malfunction in your time synchronization.

- The clients on the network do not depend on an active internet connection.

- The clients on the network do not depend on the availability of an external time server.

- A test of other freely available time servers reported that many NTP servers distributed a significantly wrong time, although they were classified as stratum-1 time servers. This is the responsibility of the server's administrators.

- If an internet connection is working properly then NTP can determine and account for the packet transmission delays quite reliable. However, if the internet connection is at its capacity limit, time synchronization can be significantly degraded due to high dispersion in packet transmission delays. Reasons for this may be hacker attacks, which must not address your own network, or new viruses causing a huge flood of emails, like it has already happened in the past.

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

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

5 Network Time Protocol (NTP)

NTP is a common method for the synchronization of hardware clocks in local and global networks. The basic concept, version 1 [Mills88], was published in 1988 as RFC (Request For Comments). Experiences acquired from its practical use on the Internet was followed by version 2 [Mills89]. The NTP software package is an implementation of the actual version 3 [Mills90], based on the specification RFC-1305 from 1990 (directory doc/NOTES). Permission to use, copy, modify and distribute this software for any purpose and without fee is hereby granted (read File COPYRIGHT).

NTP operates in a way that is basically different from that of most other timing protocols. NTP does not synchronize all connected clocks; instead it forms a hierarchy of timeservers and clients. Each level in this hierarchy is called a stratum, and Stratum 1 is the highest level. Timeservers at this level synchronize themselves by means of 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.

Highly precise synchronization is feasible because of the several time references. Every computer synchronizes itself with up to three valued time sources. NTP enables the comparison of the hardware times and the adjustment of the internal clock. A time precision of 128 ms, and often better than 1 ms, is possible.

5.1 NTP Target

The NTP software package was tested on different UNIX systems. Many UNIX systems have an NTP client pre-installed. Only some basic configurations need to be done (/etc/ntp.conf). NTP clients as freeware or shareware are also available for most other operating systems like Windows 7/Vista/XP/NT/2000/98/95/3x, OS2 or MAC. The following WEB site is recommended to get the latest version of NTP:
http://www.eecis.udel.edu/ ntp/

You can find more information on our web page at:
http://www.meinberg.de/english/sw/ntp.htm

5.2 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. These 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 "ntp-date 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       .GPS.        0     l     36     64      1      0.00    60.1      15875
```

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

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").

6 Precision Time Protocol (PTP) / IEEE1588

Precision Time Protocol (PTP or IEEE 1588) is a time synchronization protocol that offers sub-microsecond accuracy over a standard Ethernet connection. This accuracy can be achieved by adding a hardware timestamping unit to the network ports that are used for PTP time synchronization. The timestamping unit captures the exact time when a PTP synchronization packet is sent or received. These timestamps are then taken into account to compensate for transfer delays introduced by the Ethernet network.

In PTP networks there is only one recognized active source of time, referred to as the Grandmaster Clock. If two or more Grandmaster Clocks exist in a single network, an algorithm defined in the PTP standard is used to determine which one is the „best" source of time. This „Best Master Clock" algorithm must be implemented on every PTP/IEEE1588 compliant system to insure that all clients („Slave Clocks") will select the same Grandmaster. The remaining deselected Grandmaster Clocks will „step back" and enter a passive mode, meaning that they do not send synchronization packets as long as that is being done by the designated Grandmaster.

The existing network infrastructure components play a big role in a PTP network and directly influence the level of accuracy that can be achieved by the clients. Asymmetric network connections degrade the accuracy, therefore classic layer 2 and 3 Ethernet switches with their "store and forward" technology are not suitable for PTP networks and should be avoided. Simple Ethernet hubs with fixed pass-through times are not a problem. In large networks, special switches with built-in PTP functionality help to maintain high accuracy even over several subnets and longer distances. These components act as "Boundary Clocks" (BC) or "Transparent Clocks" (TC). They compensate their internal packet processing times by using timestamping units on each port. When acting as a Boundary Clock, they synchronize to the Grandmaster clock, and in turn act as a Master to the other subnets they are connected to. When acting as a Transparent Clock, then the "residence time" of the Masters' Sync-Packet is measured and added to the packet as a correction value.

6.1 General Information

The internal PTP card acts as a network interface card (10/100MBit) with an integrated hardware time stamp unit to obtain time stamps in PTP compatible networks. In conjunction with a single board computer running the PTP protocol stack and a reference time source (PTP master only) the module is capable of building a PTP Master or Slave system:
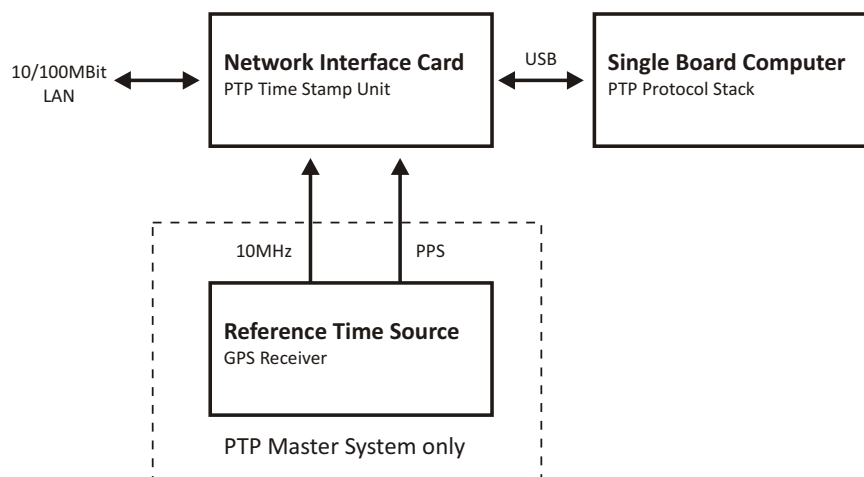
The Time Stamp Unit, integrated in an FPGA (Field Programmable Gate Array, a programmable logic device),

checks the data traffic on the MII-interface between the PHY receiver (physical connection to the network) and the Ethernet controller (MAC) on the PTP module. If a valid PTP packet is detected, the time stamp unit takes a time stamp of that packet which is read by a single board computer (SBC) running the PTP software. The configuration and status traffic between the PTP board and main SBC is done over a USB connection.

6.2 Functionality in Master Systems

Time Stamp Unit PTP Master
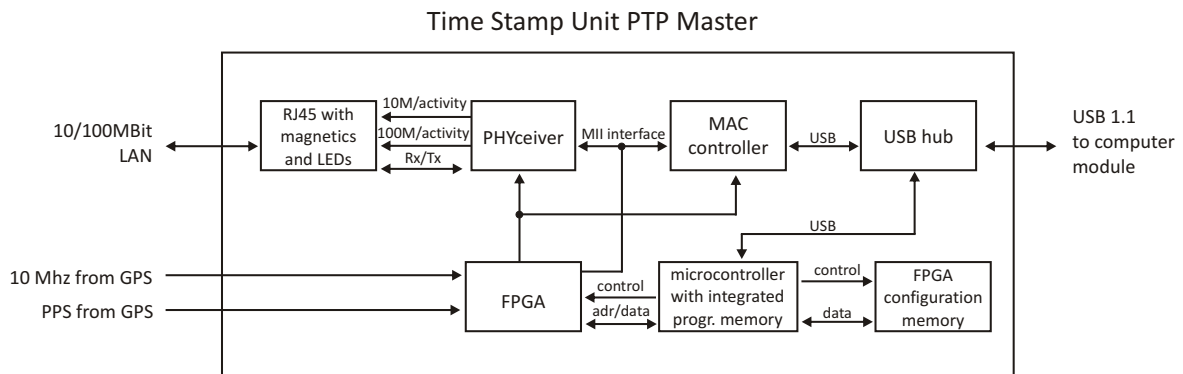
After power up, the module accepts the absolute time information (PTP seconds) of a reference time source (GPS reference clock) only once, and the PTP nanoseconds are set to zero. If the oscillator frequency of the reference time source has reached its nominal value, the nanoseconds are reset again. This procedure leads to a maximum deviation of 20 nsec of the pulse per second (1PPS) of the PTP Master compared to the 1PPS of the GPS reference clock. The reference clock of the PTP board's time stamp unit (50 MHz) is derived from the GPS disciplined oscillator of the reference time source using a PLL (Phase Locked Loop) of the FPGA. The achieves a direct coupling of the time stamp unit to the GPS system.

6.3 Functionality in Slave Systems

Time Stamp Unit PTP Slave
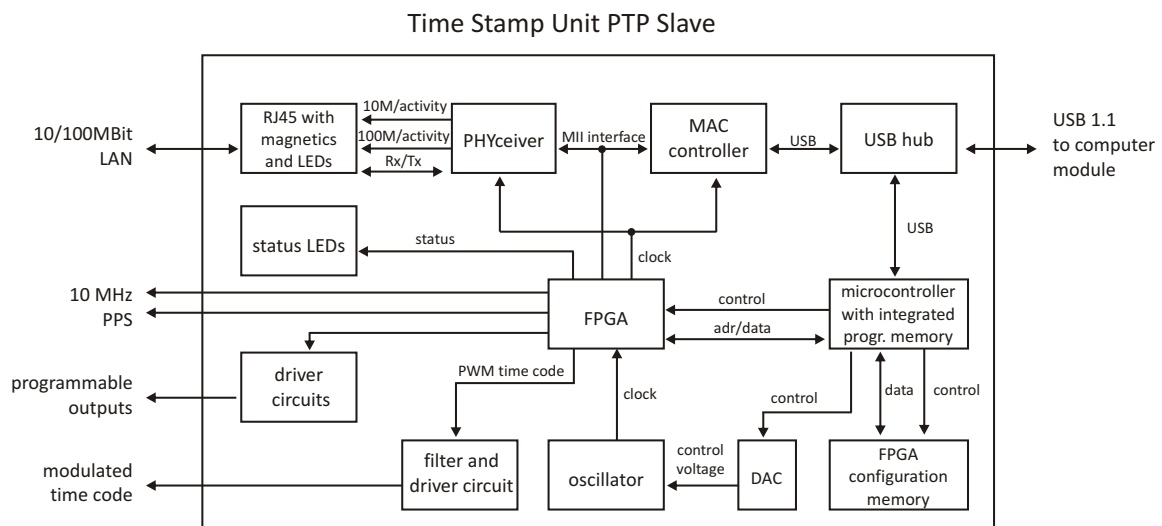
After decoding valid time information from a PTP Master, the system sets its own PTP seconds and nanoseconds accordingly. The PTP offset calculated by the PTP driver software of the single board computer is used to adjust the master oscillator of the TSU-USB. This allows the PTP Slave to generate very high accuracy output signals (10 MHz/1PPS/IRIG).

6.4 PTPv2 IEEE 1588-2008 Configuration Guide

Setting up all devices in a PTP synchronization infrastructure is one of the most important parts in a network time synchronization project. The settings of the involved Grandmaster clocks as the source of time and the end devices ("Slaves") have to match in order to allow them to synchronize and avoid problems later, when the PTP infrastructure is deployed to production environments. In addition to that, the use of PTP aware network infrastructure components, namely network switches, introduces another set of parameters that have to be harmonized with the masters and slaves in a PTP setup.

It is therefore very important to start with making decisions how the to-be-installed PTP synchronization solution should operate, e.g. should the communication between the devices be based on multicast or unicast network traffic or how often should the masters send SYNC messages to the slaves.

This chapter lists the most important options and their implications on a synchronization environment in general. A detailed explanation of the configuration settings within the LANTIME configuration interfaces can be found later within this documentation.

6.4.1 General Options

The following general mode options have to be decided before deploying the infrastructure:

1) Layer 2 (Ethernet) or Layer 3 (UDP/IPv4) connections
2) Multicast or Unicast
3) Two-Step or One-Step Operation
4) End-to-End or Peer-to-Peer Delay Mechanism

 The above options need to be defined for the whole setup, if devices do not stick to the same settings, they will not be able to establish a working synchronization link.

6.4.2 Network Layer 2 or Layer 3

PTP/IEEE 1588-2008 offers a number of so-called mappings on different network communication layers. For Meinberg products you can choose between running PTP over IEEE 802.3 Ethernet connections (network Layer 2) or UDP/IPv4 connections (Layer 3).

Layer 3 is the recommended mode, because it works in most environments. For Layer 2 mode the network needs to be able to provide Ethernet connections between master and slave devices, which is often not the case when your network is divided into different network segments and you have no layer 2 routing capabilities in your network infrastructure.

The only benefit of using Layer 2 mode would be a reduced traffic load, because the transmitted network frames do not need to include the IP and UDP header, saving 28 bytes per PTP packet/frame. Due to the fact that PTP is a low traffic protocol (when compared to other protocols), the reduced bandwidth consumption only plays a role when low-bandwidth network links (e.g. 2Mbit/s) have to be used or in pay-per-traffic scenarios, for example over leased-line connections.

6.4.3 Multicast or Unicast

The initial version of PTP (IEEE 1588-2002 also known as PTPv1) was a multicast-only protocol. Multicast mode has the great advantage that the master clock needs to send only one SYNC packet to a Multicast address and it is received by all slave devices that listen to that multicast address.

In version 2 of the protocol (IEEE 1588-2008) the unicast mode was introduced in addition to the multicast mode. In unicast mode, the master has to send one packet each to every slave device, requiring much more CPU performance on the master and producing orders of magnitudes more traffic.

On the other hand, some switches might block multicast traffic, so that in certain environments, Unicast mode has to be used.

6.4.4 Two-Step or One-Step

The PTP protocol requires the master to periodically send SYNC messages to the slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by either sending this time stamp in a separate packet (a so-called FOLLOW-UP message) or by directly manipulating the outgoing SYNC message, writing the hardware time stamp directly into the packet just before it leaves the network port.

At the time of delivery of this product, Meinberg devices support only the former approach, called Two-Step (because two packets are required).

6.4.5 End-To-End (E2E) or Peer-To-Peer (P2P) Delay Measurements

In addition to receiving the SYNC/FOLLOWUP messages a PTP slave device needs to be able to measure the network delay, i.e. the time it took the SYNC message to traverse the network path between the master and the slave. This delay is required to correct the received time information accordingly and it is measured by the slave in a configured interval (more about the message intervals later). A delay measurement is performed by sending a so-called DELAY_REQUEST to the master which timestamps it and returns the timestamp in a DELAY_RESPONSE message.

IEEE 1588-2008 offers two different mechanisms for performing the delay measurements. A slave can either measure the delay all the way to the master, this is called End-To-End (or E2E in short) or to its direct network neighbors (which would in almost all cases be a switch – or two in a redundant setup), using the Peer-To-Peer delay measurement mechanism (P2P). The delay measurements of all links between the master and the slave are then added and accumulated while a SYNC packet is traversing the network.

The advantage of this method is that it can dramatically reduce the degradation of accuracy after topology changes. For example: in a redundant network ring topology the network delay will be affected when the ring breaks open and network traffic needs to be redirected and flows into the other direction. A PTP slave in a sync infrastructure using E2E would in this case apply the wrong delay correction calculations until it performs the next delay measurement (and finds out that the network path delay has changed). The same scenario in a P2P setup would see much less time error, because the delay of all changed network links were already available.

The drawback: the P2P approach requires that all involved PTP devices and all switches support this mechanism. A switch/hub without P2P support would in the best case simply pass the so-called PDELAY messages through and as a result degrade the accuracy of the delay measurements. In the worst case it would block/drop the PDELAY messages completely, which effectively would result in no delay measurements at all.

So, E2E is the only available choice if you are running PTP traffic through non-PTP-aware switches. It is a reasonable choice if you are not using redundant network topologies or can accept that the delay measurements are wrong for a certain amount of time.

6.4.6 Mode Recommendations

Meinberg recommends to set up your PTP infrastructure to use Layer 3, Multicast, Two-Step and End-To-End Delay measurements if that is possible. This will provide the largest possible compatibility and reduces interoperability problems.

6.4.7 Message Rate Settings

The decision between the different general mode options is mainly dictated on the network environment in which the PTP infrastructure is installed.
In addition to the mode selection, a number of intervals for certain types of PTP network messages needs to be defined. In most cases, the default values as defined in the standard are a safe bet, but there are applications and scenarios where a custom message rate is required.

A possible example is a situation where the PTP infrastructure is integrated within an environment with high network load. In this case, the PTP packets can be affected by the effect of packet delay variation (PDV). An increase of the PTP message rate(s) can avoid synchronization problems due to packet queuing within non-PTP compliant switches which might cause false measurements. At higher rates, these false measurements can be detected and corrected faster as compared to lower rates at the cost of increased traffic.

The message rates for the following message types can be changed:

1)   ANNOUNCE messages
2)   SYNC/FOLLOWUP messages
3)   (P)DELAY_REQUEST messages

6.4.8 ANNOUNCE Messages

These PTP messages are used to inform the PTP network participants about existing and available master clock devices. They include a number of values that indicate the potential synchronization accuracy.

The procedure used to decide which of the available devices (that could become masters) is selected is called the "best master clock algorithm" (BMCA). The values that are used in this BMCA are read from the ANNOUNCE messages that potential masters send out periodically.

The rate at which these messages are sent out are directly affecting the time that is required by a slave device to select a master and to switch to a different master in case the selected one fails.

Multiple devices can simultaneously transmit ANNOUNCE messages during periods in which no master has been selected (yet). This happens for example when a PTP network is powered up, i.e. all devices are starting to work at the same time. In this case all devices that consider themselves (based on their configuration and status) being capable of providing synchronization to all the other PTP devices will start to send out ANNOUNCE messages. They will receive the other candidates' ANNOUNCE messages as well and perform the BMCA. If they determine that another candidate is more suitable to become the master clock, they stop sending ANNOUNCE messages and either become slave devices or go into "PASSIVE" mode, waiting for the selected master to stop sending ANNOUNCE messages. This is determined to be the case when no ANNOUNCE message is received within 3 ANNOUNCE message intervals.

As an example, if the ANNOUNCE interval has been configured to be 2 seconds (one message every 2 seconds, the default value), the master is considered to have failed when no message has been received for 6 seconds.

In order to choose a master (a backup master clock or the primary one during initialization) the devices require to receive at least two consecutive ANNOUNCE messages. Continuing our example, it would take the 6 seconds to determine that the current master has failed and another 4 seconds to select the new one. That means an ANNOUNCE interval of 2 seconds translates into at least 10 seconds of "switching time" and 4 seconds of "initial master clock selection time". So, choosing a shorter ANNOUNCE message interval will allow a faster switching to a backup master clock, but it can lead to false positives when the chosen interval is too short for the network environment.

6.4.9 SYNC/FOLLOWUP Messages

The selected master clock sends out SYNC (and, in Two-Step environments, the corresponding FOLLOWUP) messages in a configured interval. This interval (default value is one SYNC/FOLLOWUP packet every second) determines how often the slave devices receive synchronization data that allows them to adjust their internal clocks in order to follow the master clock time. Between receiving two SYNC messages, a slave clock runs free with the stability determined by its own internal time base, for example a crystal oscillator. One important factor for deciding on the SYNC interval is the stability of this oscillator. A very good oscillator requires a lower SYNC message rate than a cheaper, low-accuracy model. On the other hand you directly affect the required network bandwidth by changing the SYNC interval.

For Meinberg slave devices, the default one-SYNC-every-second setting is more than enough to achieve the highest possible synchronization accuracy.

6.4.10 (P)DELAY_REQUEST Messages

As explained in the General Mode Options chapter (see the "End-To-End or Peer-to-Peer" section), the delay measurements are an important factor for achieving the required accuracy. Especially in E2E mode, the network path delay measurements play a crucial part in the synchronization process. Per default, the slaves will perform delay measurements every 8 seconds, resulting in sending and receiving one packet. This can be increased in case the network path delay variation in the network is relatively large (i.e. the time it takes for the SYNC message

to reach the slave varies a lot) or the slave devices have to tightly follow the master and adjust their time base (oscillator) very often due to its instability.

Meinberg slave devices will limit the effect of an outdated path delay measurement by using filters and slow PLL algorithms. This avoids that a clock "jumps around" and basically monitors the time difference to the master clock carefully for a certain amount of time before adjusting its own clock. With a low cost time base this is not possible, because the instability (i.e. temperature-dependent drift and overall short term stability/aging effects) and therefore these slaves would require to perform as many delay measurements and receive as many SYNC/FOLLOWUP messages as possible.

For P2P mode the delay request interval is not as critical, simply because the delay variation on a single-hop link (i.e. from your slave device to its switch) is very stable and does not change dramatically in typical environments.

Current firmware versions of Meinberg Grandmaster clocks (V5.32a and older) do not offer changing the Delay message rate in Multicast mode, it is fixed to one delay request every 8 seconds. Since this is actually a value that is transmitted in the ANNOUNCE message as a maximum value, the slave devices are not allowed to perform delay measurements more often.

7 GPS satellite controlled clock with MRS option

Lantime/MRS is a Multi Reference Source time server. The reference time base, integrated into the LANTIME, consists of a high precision oscillator OCXO HQ. This oscillator can be optionally controlled by the integrated GPS receiver, an external Puls Per Second (PPS input), an IRIG time code receiver, by max. 7 other NTP timeservers or by a PTP IEEE1588 Grandmaster. In any case the OCXO HQ is used as a reference for internal NTP, even if no GPS reception is possible or external reference clock is available. All outputs like serial output, PPS output or 10MHz will be driven by the internal oscillator. The priority which reference clock will discipline the internal OCXO can be set up in a user defined list via the display or the HTTP interface.

7.1 MRS functionality

After power up the system the internal clock module will be free running on an internal oscillator. If the GPS receiver or one of the external reference sources are available and synchronized then the internal clock will be set once and the internal OCXO will be adjusted. For the first time adjust with an external NTP server the system will wait until the internal NTP has been synchronized and the time offset is below 1 ms (this will take appr. 5 Min). After that the offset to the external NTP server will be calculated and set the internal clock module. The following reference clocks are possible (depending on the expansions):

- GPS receiver

- IRIG time code receiver with DCLS or modulated

- Pulse Per Second Input (PPS in)

- up to 7 external NTP server

- PTP IEEE1588

- Pulse Per Second plus serial time string (STR)

If more than one reference clock is available and synchronized then the clock with the highest priority will be taken to adjust the internal OCXO. This reference clock will be called master clock. If this master clock is unavailable a different clock with the highest priority will be chosen. If a reference clock with a higher priority than the current master will be available the master clock will be switched to the higher priority.

Each external reference source can be set with a bias (a fix offset), if you know the constant offset (bias) of an external reference source. By default this value is 0 ns. The bias of the internal GPS receiver can not be set up – indirectly this can be done via the antenna cable length.

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

*(precision of next reference) / (precision of current master) * constant [s]*
The parameter „constant" depends on the quality of the internal oscillator.

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

The internal NTP is not requesting the external reference clocks directly. It will see only the internal clock of the GPS/MRS module with its high precision oscillator OCXO. The controlling of the internal OCXO will be done by the GPS/MRS module. All offsets from the internal reference time to the external reference clocks will be send to the GPS/MRS clock. The external NTP server will be configured as "server" at the internal NTP with the option "noselect" only to get the offsets to the external NTP servers.

The status information of the activated reference clocks will be shown in the display. The state of the master will be marked with "*" or written as text. Also the offset from the reference clock to the internal clock will be displayed.

```
  1.GPS *   20ns      2.PPS   30ns
  2.NTP   30.000us
```
M300

```
1.GPS * 20ns
2.PPS   30ns
3.NTP   30.000us
```
M400 / M900

```
         MRS Input Priorities        ⟳
1.GPS            is master    : -10ns
2.PPS in         is available : -20ns
3.IRIG           no signal    : n/a
4.NTP            is available : -30.000us
2.PTP(IEEE1588)is available : -300ns
```
M600

If an external PTP IEEE1588 grandmaster is available the reference source will be taken prior to the external NTP server. The PTP time stamping unit will be scanned every 10 seconds (independently of the broadcast interval of the PTP master). The external NTP server will be scanned every 64 seconds.

After setting the time offset of the internal clock module the NTP will be restarted. Now only small offset values will be send to the internal clock module; the fine synchronization mode will start. While fine synchronization mode all offsets greater than 10 ms will be ignored 5 times in a row – after the 5 times the offset will be set.

IMPORTANT: After power up the Lantime/MRS the maximum time difference between internal clock and external NTP server or PTP grandmaster must be lower than 1000s. Otherwise the internal clock must be set manually via LC display or synchronized by GPS once.

7.2 GPS functionality

A Meinberg GPS170 satellite controlled radio clock is used as a reference time base. The satellite receiver clock GPS170 has been designed to provide extremely precise time to its user. The clock has been developed for applications where conventional radio controlled clocks can not meet the growing requirements in precision. High precision available 24 hours a day around the whole world is the main feature of the new system which receives its information from the satellites of the Global Positioning System.

The Global Positioning System (GPS) is a satellite-based radio-positioning, navigation, and time-transfer system. It was installed by the United States Department of Defence and provides two levels of accuracy: The Standard Positioning Service (SPS) and the Precise Positioning Service (PPS). While PPS is encrypted and only available for authorized (military) users, SPS has been made available to the general public.

GPS is based on accurately measuring the propagation time of signals transmitted from satellites to the user's receiver. A nominal constellation of 21 satellites together with 3 active spares in six orbital planes 20000 km over ground provides a minimum of four satellites to be in view 24 hours a day at every point of the globe. Four satellites need to be received simultaneously if both receiver position (x, y, z) and receiver clock offset from GPS system time must be computed. All the satellites are monitored by control stations which determine the exact orbit parameters as well as the clock offset of the satellites' on-board atomic clocks. These parameters are uploaded to the satellites and become part of a navigation message which is retransmitted by the satellites in order to pass that information to the user's receiver.

The high precision orbit parameters of a satellite are called ephemeris parameters whereas a reduced precision subset of the ephemeris parameters is called a satellite's almanac. While ephemeris parameters must be evaluated to compute the receiver's position and clock offset, almanac parameters are used to check which satellites are in view from a given receiver position at a given time. Each satellite transmits its own set of ephemeris parameters and almanac parameters of all existing satellites.

7.3 GPS170 Features

The GPS170 module is a 100 mm x 160 mm microprocessor board, and is connected to the antenna/converter unit by a 50 ohm coaxial cable (refer to "Mounting the Antenna"). DC power to fed to the antenna/downconverter via the antenna cable. An optional antenna splitter is available to operate up to four receivers from a single antenna.

The navigation message coming in from the satellites is decoded by the GPS170´s microprocessor in order to track the GPS system time with an accuracy of better than 500 ns (or 250 nsec OCXO). Compensation of the RF signal's propagation delay is done by automatic determination of the receiver's position on the globe. A correction value computed from the satellites´ navigation messages increases the accuracy of the board's TCXO or OCXO to 10^{-9} and automatically compensates for the oscillators aging. The last recent value is restored from the battery buffered memory at power-up.

7.4 Time Zone and Daylight Saving

GPS system time differs from the universal time scale (UTC) by the number of leap seconds which have been inserted into the UTC time scale since GPS was initiated in 1980. The current number of leap seconds is part of the navigation message supplied by the satellites, so the internal real time of the GPS170 is based on UTC. Conversion to local time and annual daylight saving time can be done by the receiver's microprocessor if the corresponding parameters are set up by the user.

8 Mounting the GPS Antenna

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

The antenna/converter unit can be mounted on a wall, or on a pole up to 60 mm in diameter. A 45 cm plastic tube, two wall-mount brackets, and clamps for pole mounting are included with every GPS170. A standard RG58 coaxial cable should be used to connect the antenna/downconverter unit to the receiver. The maximum length of cable between antenna and receiver depends on the attenuation factor of the coaxial cable.

Up to four GPS170 receivers can be run with one antenna/downconverter unit by using an optional antenna splitter. The total length of an antenna line from antenna to receiver must not be longer than the max. length shown in the table below. The position of the splitter in the antenna line does not matter.

High voltage protectors must be installed directly after reaching the indoors. The optional delivered protection kit is not for outdoor usage.

8.1 Example:

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

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

8.2 Antenna Short-Circuit Assembly with surge voltage protection

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

GPS Antenna

GPS satellite antenna

free view to the equator!

cable slot

Type N male

As short as possible!

Type N female

Surge Voltage Protector
connect to earth by using the mounting bracket.

Type N female

Meinberg GPS

Type N / BNC male

Ground lead to PE Rail
(Protective Earth)
Cable / 16mm^2 - fastened
with cable shoe
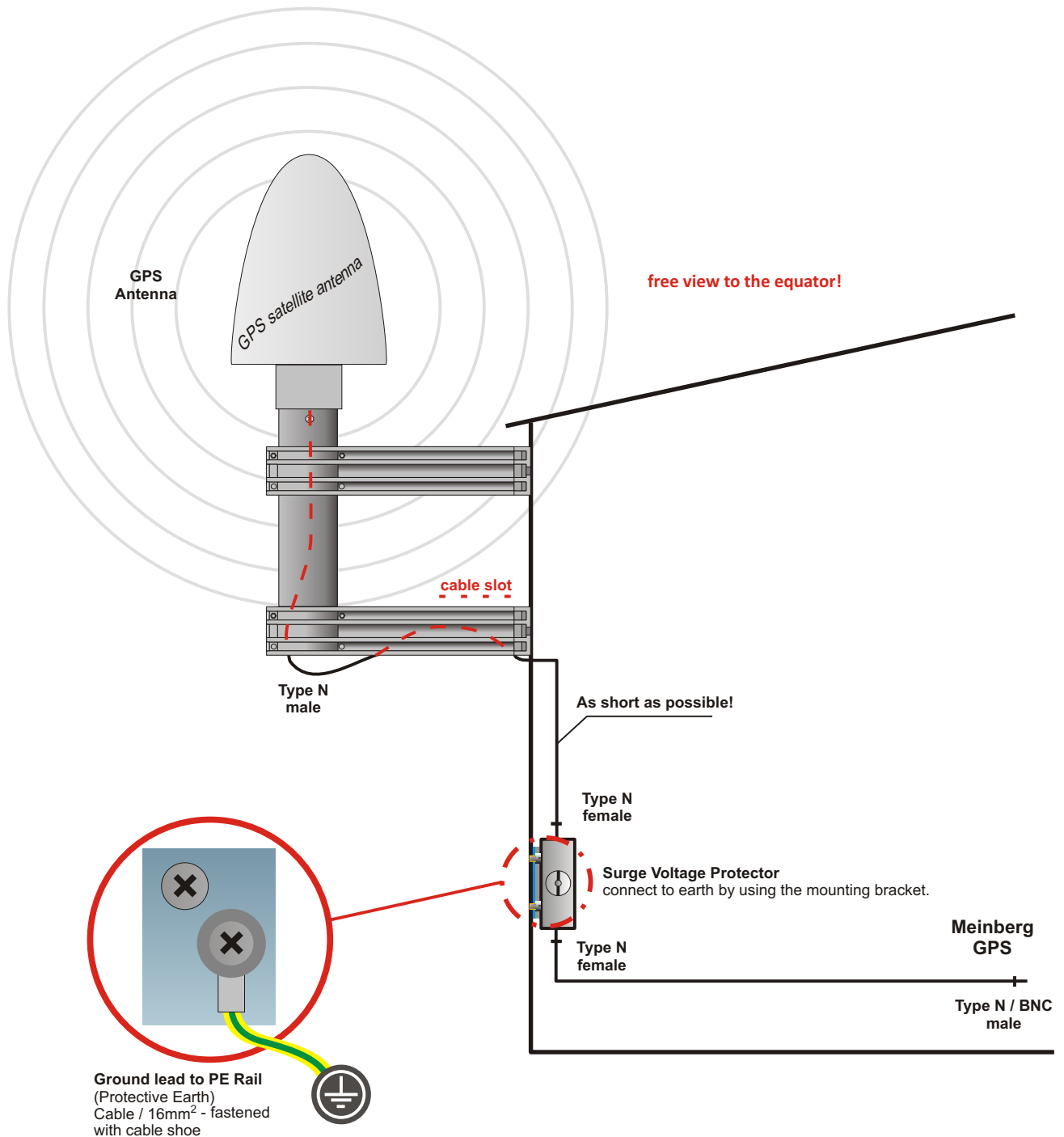
8.3 Antenna Short-Circuit

(optional for displayed systems)
In case of an antenna line short-circuit the following message appears in the display:

```
         ANTENNA
      SHORT-CIRCUIT
   DISCONNECT POWER
           ! ! !
```

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

9 Booting the GPS receiver

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

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

10 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. two minutes. During this time the following message appears on the display:

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

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

```
                              ⏏
         12:00:00

    UTC    Tue, 01.01.2008
```

```
12:00:00  UTC                 ⏏
          Tue, 01.01.2008

NTP: Offs. 1ms        Stratum: 1
GPS: NORMAL OPERATION Satellites:9/10
PTP: ok PTP_MASTER    GM:00:00:00:00:00:00
Press F1 for help or F2 for setup overview
```

For the synchronization of the NTPD with the GPS it is necessary that the GPS receiver is synchronous with the GPS time. In this case the following message is monitored on the display:

```
12:00:00  UTC                 ⏏
          Tue, 01.01.2008

NTP: Offs. 1ms        Stratum: 1
GPS: NORMAL OPERATION Satellites:9/10

Press F1 for help or F2 for setup overview
```

The second line shows the user that the NTPD is synchronized to the GPS with a certain offset. Because of the fact that the NTPD controlled internal system time is adjusted by a software PLL (phase locked loop) it takes a certain time to adjust this offset. The NTPD tries to keep the offset below +-128 ms. If the offset becomes too large the system time is set with the GPS time. Typically values for the offset are +- 5 ms after the NTPD has already synchronized and settled.

11 Configuration User Interface

11.1 Introduction: Configuration LANTIME

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 terminal in front panel
(38400/8N1/VT100)
HTTP Interface
Secure HTTP Interface (HTTPS)
Front panel LCD/VFD Interface
SNMP Management

In order to be able to configure the time server via the web interface or a telnet/SSH connection, an IP address has to be assigned via the front panel keys and LC/VF display (for automatic assignment possibilities please refer to: DHCP IPv4 or AUTOCONF IPv6). LANTIME variants without a display can be configured using the serial terminal interface (labeled "Term" or "Terminal") The termin program should be set to 38400Baud / 8N1 − VT100 emulation. Once the IPv4 address, net mask and IPv4 GATEWAY have been set up or the network interface has been automatically configured with DHCP/Autoconf, further configuration changes can be done via a network connection:

To set up a TELNET connection the following commands are entered:
telnet 198.168.10.10 // LANTIME IP address
user: root
password: timeserver
With "setup" the configuration program is started.

To set up a SSH connection the following commands are entered:
ssh root@198.168.10.10 // LANTIME IP address
password: timeserver
With "setup" the configuration program is started.

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 entered in a web browser:
https://198.168.10.10 // LANTIME IP address
password: timeserver

11.2 The menus in Detail

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

```
                    F1
                                      12:00:00  UTC            F1
                                                Tue, 01.01.2008
       12:00:00
                                      NTP: Offs. 1ms        Stratum: 1
                                      GPS: NORMAL OPERATION Satellites:9/10
       UTC   Tue, 01.01.2008          PTP: ok PTP_MASTER    GM:00:00:00:00:00:00
                                      Press F1 for help or F2 for setup overview
```

```
   F1           ↑            OK       ● Ref. Time
                                      ● Time Service
           ←       →                  ● Network
   F2           ↓           ESC       ● Alarm
```
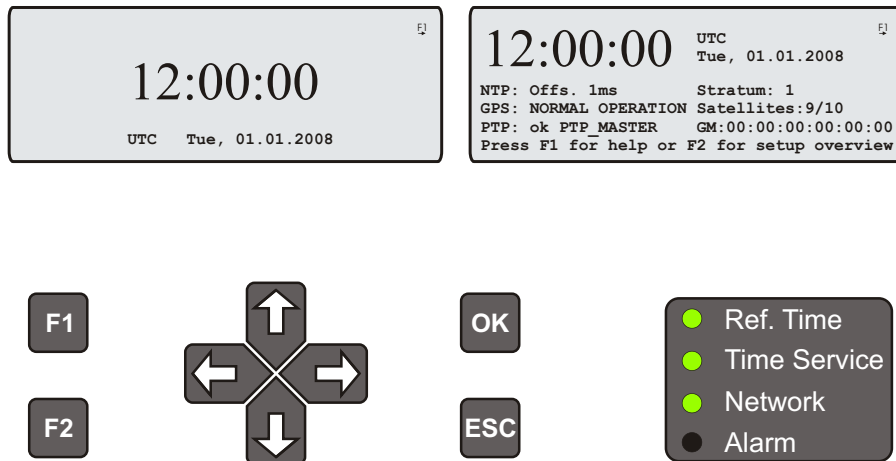
The multicolor LEDs will reflect the current state of the device:

„Ref. Time"
green: the reference clock (e.g. integrated GPS) produce valid time.
red: the reference clock produce no valid time (e.g. not synchronized)

„Time Service"
green: NTP has been synchronized to reference clock.
red: NTP is not synchronous to reference clock or sync to „local clock"

„Network"
green: all watched network ports has been "link up" detected
red: at least one of the watched network ports (look at „Setup Device
Parameter / Check Network Linkup") is not connected

„Alarm"
off: no error at moment
ret: general error – more information will be shown on display.

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

```
   Use ↑ and ↓ to select different
   main menus. Use → and ← to
   enter specific submenus. Press
   F2 for SETUP overview.    [ESC]
```

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

```
TYP: ELX800  GPS170 M6x  V5.26
Serial Num.: 000000000000
NTP: 4.2.0@1.1438-o
Kernel: 2.6.12                  ↵
```

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

```
12:00:00  UTC
          Tue, 01.01.2008
NTP: Offs. 1ms        Stratum: 1
MRS: NORMAL OPERATION Satellites:9/10
PTP: ok  PTP_SLAVE    GM:00:00:00:00:00:00
Press F1 for help or F2 for setup overview
```

```
  ->   Reference Time  <-
       Time Service
       Network
       System
```

```
       Reference Time
  ->   Time Service    <-
       Network
       System
```

```
       Reference Time
       Time Service
  ->   Network         <-
       System
```

```
       Reference Time
       Time Service
       Network
  ->   System          <-
```

```
 -> MRS Management      <-
    Info  GPS Receiver
    Setup GPS Receiver
    Setup Outputs
```

```
 -> NTP Current State       <-
    external NTP servers
    Stratum of local clock
    PTP IEEE1588
```

```
 -> Global Configuration   <-
    Network Interfaces
    Network Services
```

```
 -> Set time zone           <-
    Restart NTP
    Reset to factory defaults
    Reboot time server
```

11.3 Menu: Reference Time

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

```
  ->   Reference Time  <-
       Time Service
       Network
       System
```

```
 -> MRS Management      <-
    Info  GPS Receiver
    Setup GPS Receiver
    Setup Outputs
```

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

11.3.1 Menu Setup MRS

```
-> Reference Time  <-
   Time Service
   Network
   System
```

[OK]

```
-> MRS Management        <-
   Info GPS Receiver
   Setup GPS Receiver
   Setup Outputs
```

[OK]

```
->  MRS Status and Setup  <-
    IRIG Input Management
```
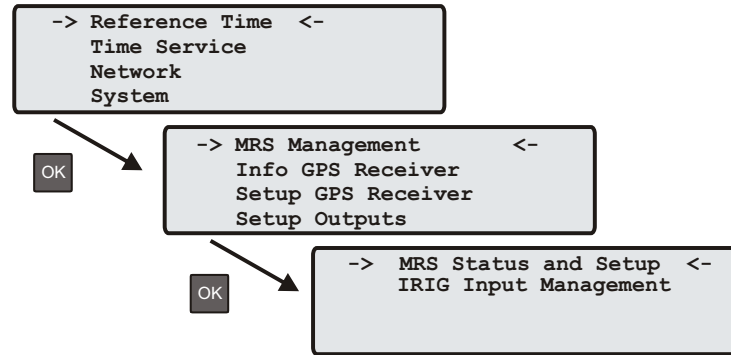
The internal reference clock of the integrated GPS clock module with the high precision oscillator (OCXO HQ) can be disciplined by different time sources. The possible time sources are GPS, external 1-PPS, external 10 MHz, IRIG Time Code (TC-AM or -DCLS), external NTP server or optionally a PTP-IEEE1588 Grandmaster. The priorities for the internal control and administration of the references can be set up in configuration. The priority will define which reference source will be used next if the highest priority reference source is no longer available. For each reference source a bias (fixed offset) and a precision value can be defined.

```
-> MRS Status            <-
   Setup Input Priorities
   Setup Fixed Offsets
   Setup Precisions
```

[OK]

```
->  Numerical Status  <-
    Graphical Status
```

[OK]

```
       MRS Status
1.GPS is available  :  -50.0us
2.PPS is available  :  -50.0ns
3.FRQ no signal     :  n/a
4.NTP is available  :  - 5.0ns
5.PTP is available  :  -50.0ns
```
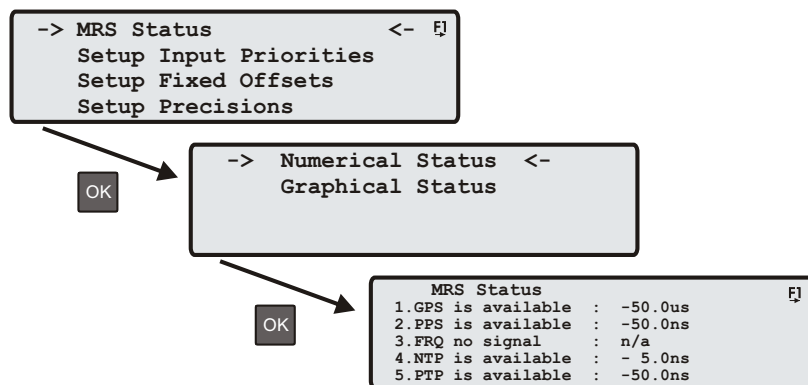
With the OK and arrow buttons you can select an overview of the current status of the MRS. All possible reference clocks will be shown with the number of priority, the name of the reference clock and the current offset to the internal time reference (OCXO). The current master will be marked with a "*" behind the name of the reference clock.

In the next menu ("Setup Input Priorities") the user can define in which order the references will be used to control the internal oscillator. The reference clock with the highest priority will always be used if it is available.

```
    MRS Status
-> Setup Input Priorities <-
   Setup Fixed Offsets
   Setup Precisions
```

[OK]

```
Setup MRS Input Priorities
1.■GPS            2. PPS in
3. TCR in         4. NTP
5. PTP (IEEE158 6. FRQ in
```
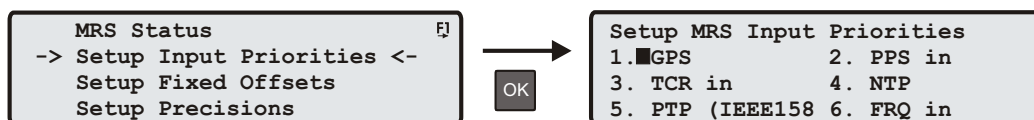
The bias (a fixed offset) can be set up in the next sub menu, if you know the constant offset (bias) of an external reference source. By default this value is 0 ns. The bias of the internal GPS receiver can not be set up – indirectly this can be done via the antenna cable length.

```
    MRS Status
    Setup Input Priorities
-> Setup Fixed Offsets     <-
    Setup Precisions
```

[OK]

```
     Set Fixed Offsets in [ns]
PPS:■              TCR:
NTP:               PTP:
FRQ:
```
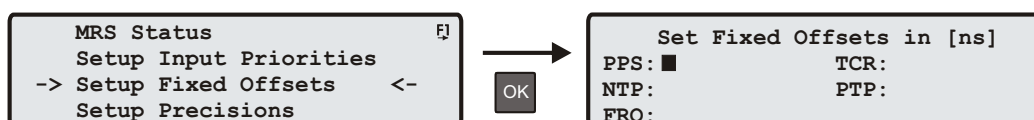
Each reference clock can be assigned a specific precision which will reflect the accuracy of the reference clock. This precision value will determine the hold over time when switching to the next reference clock if the current master is not available anymore. If the precision is 0 the next reference clock will be switched at once. If the precision value is greater then 0 the time for switching to the next reference (hold over time) will be calculated by the following formula: *((precision of next reference) / (precision of current master) * constant [s])*

The parameter „constant" depends on the quality of the internal oscillator.

```
   MRS Status              ⌐                    Set Precision of Refclocks [ns]
   Setup Input Priorities          OK          GPS:■              PPS:
   Setup Fixed Offsets                         TCR:               NTP:
-> Setup Precisions      <-                    PTP:               FRQ:
```

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

```
-> Numerical Status   <-                           MRS Status            ⌐
   Graphical Status                 OK      1.GPS  no signal * : (5m19s/19m00s)
                                            2.PPS  no signal    : n/a
                                            3.TCR  no signal    : +1.349us [+31.50us]
                                            4.NTP  is available : -30.00us
                                            5.PTP  is available :  -50.0ns
```

11.3.2 Menu IRIG Input Management

The first line of the display shows the system state with 8 options described above. Next line will shown the IRIG code and the offset from UTC:

```
   MRS Status and Setup                     -> IRIG Receiver State    <-
-> IRIG Input Management <-        OK           setup IRIG Receiver
```
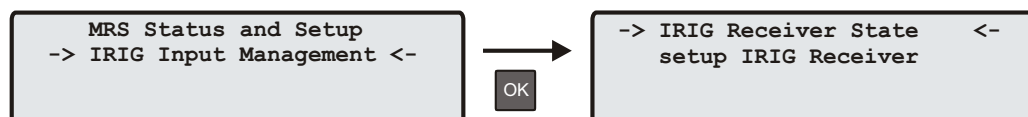
Bit 7:   Invalid UTC parameter
Bit 6:   TCAP exceeded, jitter out of range
Bit 5:   Lock on
Bit 4:   Telegram error
Bit 3:   Data available
Bit 2:   Invalid sysconf
Bit 1:   Pulses enabled
Bit 0:   Warmed up

```
-> IRIG Receiver State    <-                   Time Code Receiver (IRIG)  ⌐
   setup IRIG Receiver              OK      IRIG Code: B002/B003 (DC)
                                            IRIG Offset from UTC: +00.00
                                            TCR State:  --------
```
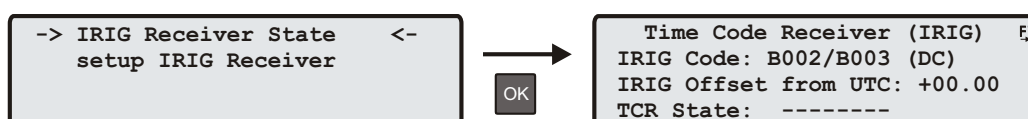
Invalid UTC parameter:
This bit is set to one if the checksum of the 'Offset from UTC' parameter, which must be used if no IEEE1344 extensions are available, is invalid. User must enter new 'Offset from UTC' data to clear this bit. Please note that

the IRIG-receiver never leaves freewheeling mode if IEEE1344 is disabled and the UTC-Parameter are invalid!

TCAP exceeded, jitter out of range:
If the jitter between two consecutive IRIGtelegrams exceeds +/- 100 μs the receiver switches into freewheeling mode and the 'TCAP exceeded' Bit is set. 'TCAP exceeded' is cleared if the measured jitter is below +/- 100 μs.

Lock on:
'Lock On' is set whenever the receiver is in synchronous mode and the internal oscillator correction value has settled.

Telegram error:
This bit is set if the consistency check of two consecutive IRIGtelegrams fails. The IRIG-receiver switches into freewheeling mode if 'telegram error' is set.

Data available:
'data available' is set if the receiver can read the timecode.

Invalid sysconf:
If 'invalid sysconf' is set the checksum of the system configuration data is invalid. In this case the default mode 'IEEE1344 disabled' is selected. User must cycle the system or enter a new system configuration in the IRIG-parameter
menu.

Pulses enabled:
The pulse per second (PPS) signal which increases the NTP's accuracy is turned when 'lock on' is set the first time. The 'pulses enabled' bit is set if the PPS signal is enabled.

Setup IRIG Receiver:

```
       IRIG Receiver State          OK    Set IRIG Receiver Parameters
   -> Setup IRIG Receiver   <-    ----->  IRIG Code: B002/B003 (DC)
                                          IRIG Offset from UTC (+HH:MM)
                                                  ⊞00:00
```
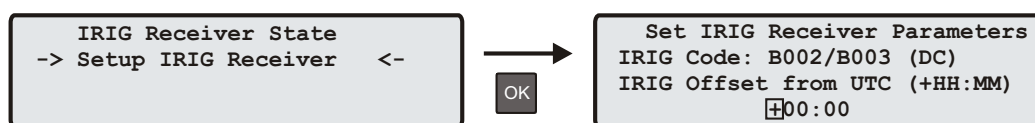
When pressing the OK button the IRIG code can be selected with the Up/Down arrow keys. Only the codes which are supported by the IRIG receiver will be selectable. It must be ensured that a "DC" code is selected if the IRIG signal is connected to the DCLS input. Otherwise the correspondent Non-DC code must be selected if an AM signal is connected to the TC-AM input.
If the connected IRIG signal does not support the Offset to UTC you have to set up this parameter as well.

11.3.3 Info GPS Receiver

```
   -> GPS Receiver Position <-              GPS Receiver Position
      Satellite Constellation         LAT: 51.9828  51°58'58" N
      GPS Status & Version            LON:  9.2258  09°13'32" E
                                      ALT: 176 m


                                            GPS Receiver Position
                                      x: 3885653 m
                                      y: 631134  m
                                      z: 5001764 m


      GPS Receiver Position               SATELLITE CONSTELLATION
   -> Satellite Constellation <-          satellites in view: 8
      GPS Status & Version                good satellites   : 8
                                          selected set: 08 12 21 09


      GPS Receiver Position           Reference Clock Information
      Satellite Constellation         MRS State: SYNC
   -> GPS Status & Version    <-      GPS170 v.1.20      OCXO HQ
                                      S/N: 0290100000680
```

11.3.4 GPS Receiver Position

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

```
-> GPS Receiver Position <-
   Satellite Constellation
   GPS Status & Version
```

```
        GPS Receiver Position
LAT: 51.9828        51°58'58" N
LON:  9.2258        09°13'32" E
ALT: 176 m
```

```
        GPS Receiver Position
 x: 3885653 m
 y: 631134  m
 z: 5001764 m
```
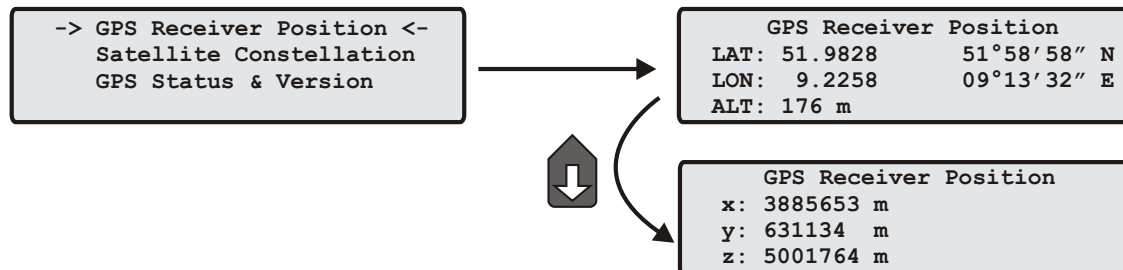
11.3.5 GPS Satellite Constellation

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

```
       GPS Receiver Position
-> Satellite Constellation <-
   GPS Status & Version
```

```
      SATELLITE CONSTELLATION
      satellites in view: 5
       good satellites  : 5
      selected set: 04 09 21 17
```

11.3.6 GPS Status and Version

This page will monitor the current state („SYNC" or „ASYNC!").

```
       GPS Receiver Position
       Satellite Constellation
-> GPS Status & Version    <-
```

```
   Reference Clock Information
   GPS State: SYNC
   GPS170 v1.20    OCXO HQ
   S/N:  029010000680
```

The next line will reflect the version number of the GPS170 and the oscillator type. In the bottom line the serial number of the GPS170 will be shown.

11.3.7 Setup GPS Receiver Parameters

```
->  Init GPS Receiver    <-
    Setup Antenna Length
    Setup Simulation Mode
```

```
-> Init Receiver Position <-
   Init Receiver Time
   Init COLD Boot
   Init WARM Boot
```

```
     Init GPS Receiver
-> Setup Antenna Length    <-
    Setup Simulation Mode
```

```
         Edit and Set
      Antenna Cable Length
        of GPS receiver
        Length: 020 m
```

```
      Init GPS Receiver
      Setup Antenna Length
-> Setup Simulation Mode  <-
```

```
         Edit and Set
   GPS Receiver Simulation Mode

   Simulation Mode: disabled
```

11.3.8 Init GPS Receiver

```
-> Init GPS Receiver  <-              -> Init Receiver Position <-
   Setup Antenna Length                  Init Receiver Time
   Setup Simulation Mode                 Init COLD Boot
                                         Init WARM Boot
```

11.3.9 Init Receiver Position

When the receiver is primarily installed at a new location far away from the last position saved in the receiver's memory the satellites in view and their doppler will differ so much from those expected due to the wrong position that GPS170 has to scan for satellites in Warm Boot mode. Making the new approximately known position available to the receiver can avoid Warm Boot and speed up installation

```
-> Init Receiver Position <-          Init GPS Receiver Position
   Init Receiver Time                    LAT: 51.58'58" N
   Init COLD Boot                        LON: 09.13'32" E
   Init WARM Boot                        ALT: 176 m
```
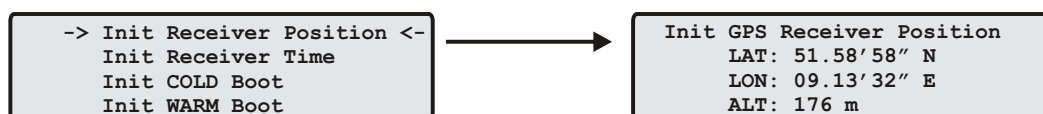
11.3.10 Init Receiver Time

If the receiver's on-board real time clock keeps a wrong time the receiver is unable to compute the satellites´ correct elevation angles and Doppler. This submenu enables the user to change the receiver's system time for initialisation. After the receiver has locked, its real time clock will be adjusted using the information from the satellites.

When the antenna is disconnected it is possible to set the LANTIME with any time. Note that the NTP will not synchronize to a GPS losing its reception or if the deviation to the system time is larger than 1024 seconds. In this case the menu SIMULATION MODE (see below) has to be active. After setting the clock manually the system time will be set and the NTP will be restarted.

```
   Init Receiver Position              Init GPS Receiver Time
-> Init Receiver Time   <-
   Init COLD Boot                         MESZ:  12:48:29
   Init WARM Boot                            01.07.2008
```
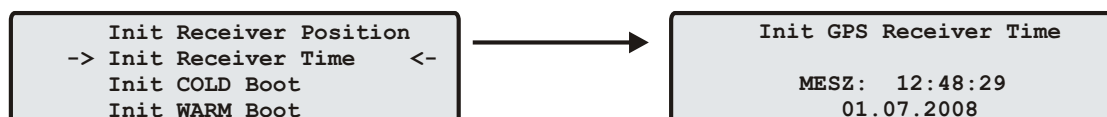
11.3.11 Initiate Cold Boot of GPS Receiver

This menu lets the user initialize all GPS data, i.e. all saved satellite data will be cleared. The user has to acknowledge this menu again before the initialisation starts. The system starts operating in the COLD BOOT mode and seeks for a satellite to read its actual parameters.

```
   Init Receiver Position              Initiate COLD Boot
   Init Receiver Time                    of GPS Receiver
-> Init COLD Boot       <-
   Init WARM Boot                       Press F2 to confirm
```

11.3.12 Initiate Warm Boot of GPS Receiver

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

```
     Init Receiver Position              Initiate WARM Boot
     Init Receiver Time                   of GPS Receiver
     Init COLD Boot
  -> Init WARM Boot         <-          Press F2 to confirm
```

11.3.13 Set Antenna Cable Length

This menu asks the user to enter the length of the antenna cable. The received time frame is delayed by approx. 5 ns per meter antenna cable. The receiver is able to compensate this delay if the exact cable length is given. The default value is 20 m. The maximum value that can be entered is 500 m (only with low loss cable).

```
     Init GPS Receiver                       Edit and Set
  -> Setup Antenna Length  <-            Antenna Cable Length
     Setup Simulation Mode                  of GPS receiver
                                            Length: 020 m
```
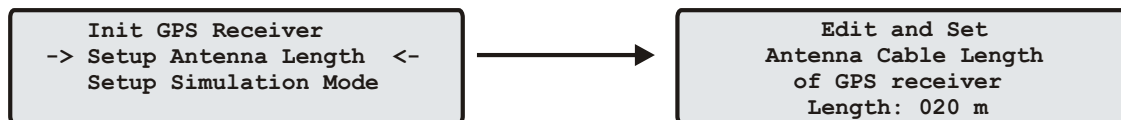
11.3.14 Set GPS Receiver Simulation Mode

Enabling this menu lets the user run the LANTIME without antenna. Normally the NTPD loses synchronisation with the GPS when the antenna is disconnected or the GPS did not receive enough satellites (red FAIL LED is turned on). When IGNORE LOCK is enabled the status information from the GPS is fixed to SYNC. So it is possible to set the NTPD with any other time entered by the SETUP INITIAL TIME menu. Usually this menu should be disabled. If this option is enabled an "*" will be shown behind the time string in the root menu.

```
     Init GPS Receiver                       Edit and Set
     Setup Antenna Length             GPS Receiver Simulation Mode
  -> Setup Simulation Mode <-
                                         Simulation Mode: disabled
```

11.3.15 Setup GPS Outputs

```
  ->  Enable Outputs      <-               Enable Outputs
      Setup Serial Outputs           ->    Synthesizer: always  <-
      Setup IRIG Outputs                       Pulses: always
      Setup Pulse Outputs               Serial Outputs: always


      Enable Outputs                   ->   Setup COM 0        <-
  ->  Setup Serial Outputs <-               Setup COM 1
      Setup IRIG Outputs                    Setup Time Zone
      Setup Pulse Outputs


      Enable Outputs                   Time Code (IRIG, AFNOR, IEEE)
      Setup Serial Outputs                   Output Settings
  ->  Setup IRIG Output     <-         ->   Code: AFNOR NFS-87500 <-
      Setup Pulse Outputs                   TIME: UTC


      Enable Outputs
      Setup Serial Outputs            -> Setup prg. pulse outputs <-
      Setup IRIG Output                  Setup prg. Synthesizer
  ->  Setup Pulse Outputs  <-
```

11.3.16 Enable Outputs

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

```
   -> Enable Outputs      <-                      Enable Outputs
      Setup Serial Outputs              ->    Synthesizer: always  <-
      Setup IRIG Output                             Pulses: always
      Setup Pulse Outputs                   Serial Outputs: always
```

11.3.17 Setup Serial Outputs

```
      Enable Outputs                     ->      Setup COM 0      <-
   -> Setup Serial Outputs <-                    Setup COM 1
      Setup IRIG Output                          Setup Time Zone
      Setup Pulse Outputs
```
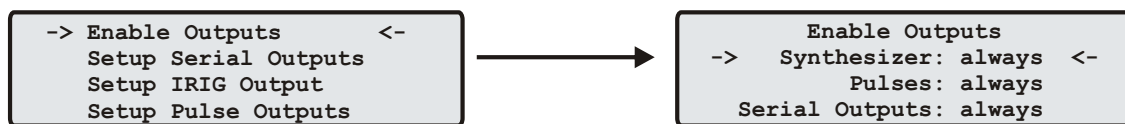
This menu lets the user configure the baud rate and the framing of the serial RS232 port to one of the following values:

Baud Rate: 300 to 19200
Framing: 7E2, 8N1, 8E1, 8O1

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

Default: COM: 19200 baud, 8N1, once per second

This topic is used to select one of several different types of serial time strings or the capture string for each serial port. The following time strings can be selected. All time strings are described in the appendix at the end of this documentation.

- Meinberg Standard String
- GPS167 Capture String
- SAT String
- UNI-Erlangen String
- NMEA String (RMC)
- SPA String
- Computime String
- Sysplex1 String
- RACAL String

Refer to chapter Time Strings for details.

11.3.18 Setup Time Zone

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

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

```
        Setup COM 0
        Setup COM 1
  ->    Setup Time Zone <-
```
→
```
       Time Zone Parameters
            of display
  -> Daylight Saving OFF  <-
     Daylight Saving ON
```

```
              Daylight Saving OFF
   >TZ Name:MEZ <     Offs.:+01:00h
    Day of Week: Sun
    Date:25.10.****   Time:03:00:00
```

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

All changeover rules for the daylight saving like "the first/the second/the second to last/the last Sunday/Monday etc. in the x-th month," can be described by the used format "first specified day-of-week after a defined date". If the number of the year is not displayed as wildcar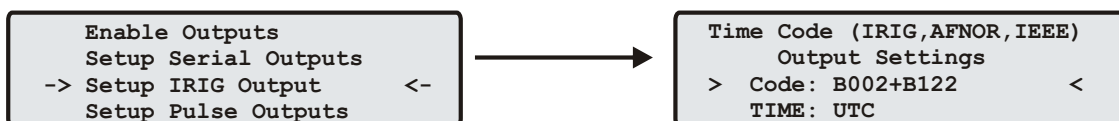ds the complete date exactly determines the day daylight saving has to change (October 26th, 2008 in the figures below), so the day-of-week does not need to be specified and therefore is displayed as wildcards.

```
   Time Zone Daylight Saving OFF
   TZ Name: MEZ    Offs.UTC:+01:00h
   Day of Week: Sun
   Date:25.10.****   Time:03:00:00
```

```
   Time Zone Daylight Saving OFF
   TZ Name: MEZ    Offs.UTC:+01:00h
   Day of Week: ***
   Date:26.10.2008   Time:03:00:00
```

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

11.3.19 TIME CODE (IRIG)

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

```
        Enable Outputs
        Setup Serial Outputs
   ->   Setup IRIG Output      <-
        Setup Pulse Outputs
```
→
```
   Time Code (IRIG,AFNOR,IEEE)
        Output Settings
   >   Code: B002+B122        <
        TIME: UTC
```

Refer to chapter Timecode for details.

11.3.20 Synthesizer Frequency Output

```
           Synthesizer
        Frequency Output
      Frequence: 0 Hz
          Phase: 0 el           →
```
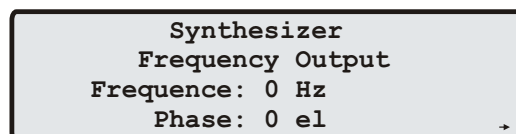
This setup menu lets the user edit the frequency and phase to be generated by the on-board synthesizer. Frequencies from 1/8 Hz up to 10 MHz can be entered using four digits and a range. The range can be selected if the „UP" or „DOWN" key is pressed while the cursor is positioned on the frequency´s units string. If the least significant range has been selected valid fractions of the frequency are .0, .1 (displayed as 1/8), .3 (displayed

as 1/3), .5 and .6 (displayed as 2/3). Selection of 1/3 or 2/3 means real 1/3 or 2/3 Hz, not 0.33 or 0.66. If frequency is set to 0 the synthesizer is disabled.

The last line of the display lets the user enter the phase of the generated frequency from -360° to +360° with a resolution of 0.1°. Increasing the phase lets the signal come out later. Phase affects frequencies less than 10.00 kHz only, if a higher frequency is selected a message "(phase ignored)" informs the user that the phase value is ignored.

11.4 Menu Time Service
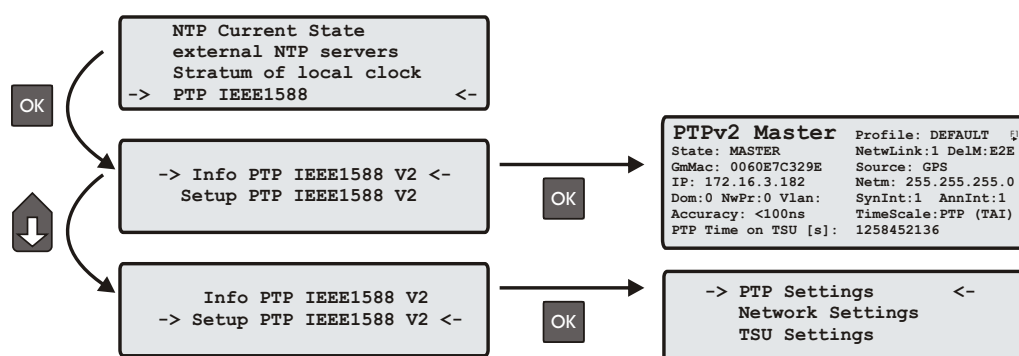
11.4.1 Menu NTP Current State

A table with current information of the reference clocks will be shown in this menu.

11.4.2 Menu: NTP Configuration

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. The local clock can be disabled if the timeserver should not answer anymore when the reference clock is out of order. Four additional external NTP servers can be set up in this menu to provide a high grade of redundancy for the internal reference clock.
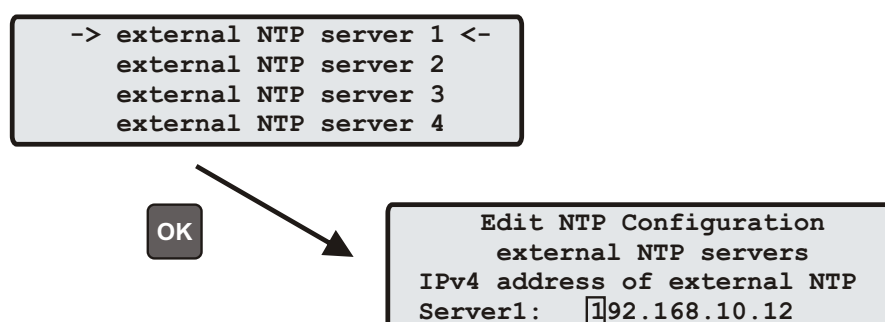
11.4.3 Menu: Stratum of local clock

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

```
          NTP Configuration
        Stratum of local clock
    new stratum value from 0 to 15
             stratum: 12
```

11.4.4 Menu PTP v2: IEEE 1588-2008
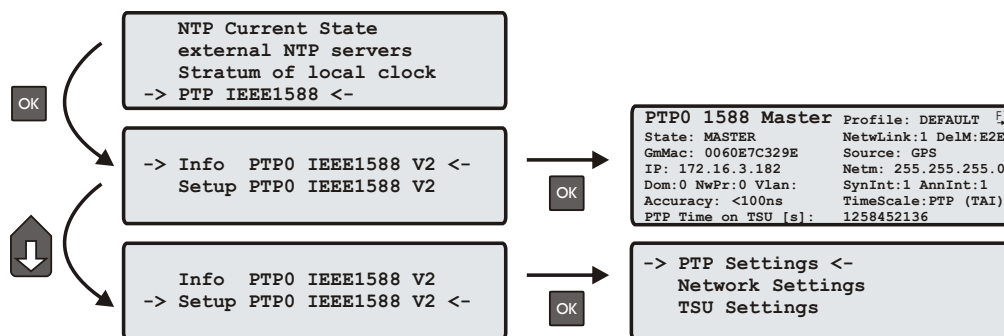
The menu for PTP IEEE 1588 configuration is located under the "Time Service" main menu and is divided into "Info" and "Setup".

Menu Info PTPv2

```
      -> Info PTP IEEE1588 V2 <-
         Setup PTP IEEE1588 V2
```

The page „Info PTP0 IEEE1588 V2" gives an overview of the state of the most important PTP parameters from the time stamp unit which is connected to the PTP0 interface. The appearance of this page is depending on the mode of the PTP engine. If the unit is configured as a PTP grandmaster clock, then this page shows the „PTP0 1588 Mstr." state.

With MRS (Multi Reference Source) devices, the PTP engine can be configured to act as Slave as well. So in this case, this page will show "PTP 1588 Slave".

```
PTP0 1588 Master  Profile: DEFAULT
State: MASTER          NetwLink:1 DelM:E2E
GmMac: 0060E7C329E     Source: GPS
IP: 172.16.3.182       Netm: 255.255.255.0
Dom:0 NwPr:0 Vlan:     SynInt:1  AnnInt:1
Accuracy: <100ns       TimeScale:PTP (TAI)
PTP Time on TSU [s]:   1258452136
```

Menu Setup PTPv2

```
-> PTP Settings      <-
   Network Settings
   TSU Settings
```

OK

```
-> PTP Mode          <-
   PTP Presets
   PTP Parameters
```

OK

```
      Setup PTP Mode:
  PTPv2 Multicast Master
```

```
   PTP Mode
-> PTP Presets       <-
   PTP Parameters
```

OK

```
   Load PTP Preset Defaults:
  (PTP values will be overwritten)
  Delay Req.Resp. Default Profile
```

```
   PTP Mode
   PTP Presets
->    PTP Parameters       <-
```

OK

```
Prio1:128  Prio2:128 Domain:0
DelayMech:E2E   Netw.Prot:UDP
Timescale: 1    Sync Int:  2s
Requ Int:  8s   Ann.Int:   2s
```

With this menu, all PTP parameters can be configured for the selected interface.

Menu PTP Mode

```
-> PTP Mode          <-
   PTP Presets
   PTP Parameter
```

```
      Setup PTP Mode
  PTPv2 Multicast Slave
  PTPv2 Multicast Master
  PTPv2 Unicast Slave
  PTPv2 Unicast Master
```
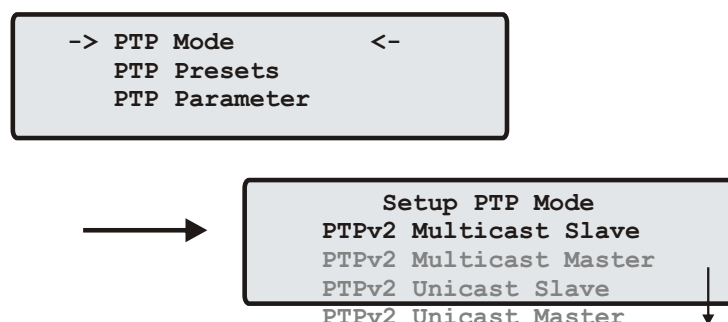
The number of different PTP operation modes depends on the feature set of the purchased unit.

Supported modes on a GPS-only system:

- PTPv2 Multicast Master
- PTPv2 Unicast Master

Supported Modes on a MRS system:
- PTPv2 Multicast Slave
- PTPv2 Multicast Master
- PTPv2 Unicast Slave
- PTPv2 Unicast Master

Load PTP Presets

Each PTP preset respresents a set of PTP configuration parameters that will switch the PTP engine to a dedicated PTP profile. After a preset has been selected, the user still has the opportunity to change all PTP parameters and "fine-tune" them.

```
        PTP Mode
    ->  PTP Presets    <-
        PTP Parameter
```

```
      Load PTP Presets default
   (PTP values will be overwritten)
   Delay Reg.Resp. Default Profile
   Peer to Peer Default Profile
   Power Systems Profile
```
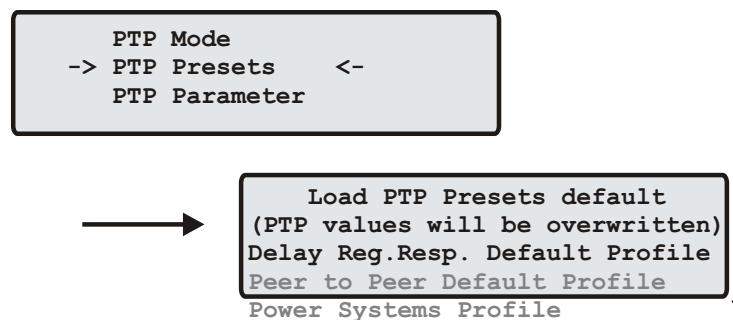
Note: Whenever a PTP preset is selected, all previously saved PTP parameters will be overwritten!

Currently 3 different presets are supported:

Delay Request Response Default Profile
- Sync Msg. Rate: 1/sec
- Ann. Msg. Rate: 2 sec
- Priority 1:   128
- Priority 2:   128
- Delay Mech.:   "E2E"

Peer-to-Peer Default Profile
- Sync Msg. Rate: 1/sec
- Ann. Msg. Rate: 2 sec
- Priority 1:   128
- Priority 2:   128
- Delay Mech.:   "P2P"

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

Global Parameters

Depending on the selected mode, different sub menus will appear for configuring the global PTP parameters.

```
┌─────────────────────────────────┐
│ -> Global PTP Parameters <-     │
│    Unicast Parameters           │
│                                 │
│                                 │
└─────────────────────────────────┘
```

Slave ⟶
```
┌─────────────────────────────────┐
│ Def.Asym.Offs[ns]:+          ↰  │
│ Max.Pathdelay[ns]:              │
│ Domain Number    :   0          │
│ DelayMech:E2E    Netw.Prot:UDP  │
└─────────────────────────────────┘
         P2P                  ETH    ↓
```
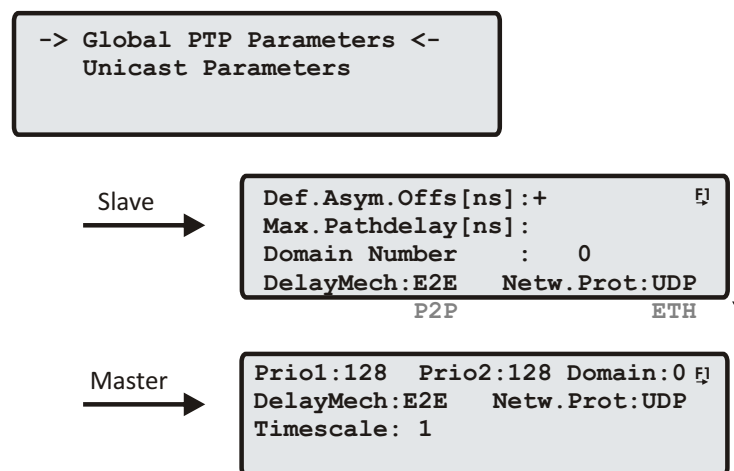
Master ⟶
```
┌─────────────────────────────────┐
│ Prio1:128  Prio2:128 Domain:0 ↰ │
│ DelayMech:E2E    Netw.Prot:UDP  │
│ Timescale: 1                    │
└─────────────────────────────────┘
```

The global parameters that are common with all modes are:

Domain Number:
A PTP domain is a logical group of PTP devices within a physical network that belong to the same domain number.
Slave devices that shall sync to a certain master within a network must have configured a unique domain number which is the same on the master.

Delay Mechanism:
E2E - End-to-End (Delay Request-Response)
P2P - Peer-to-Peer (Pdelay Request-Response)

Network Protocol:
UDP - UDP/IPv4 (Layer 3)
ETH - IEEE 802.3/Ethernet (Layer 2), currently only supported in Multicast mode!

Priority1 (Master only):
The attribute is used in the execution of the best master clock algorithm (BMCA). Lower values take precedence. Configurable range: 0..255.
The operation of the best master clock algorithm selects clocks from a set with a lower value of priority1 over clocks from a set with a greater value of priority1.

Priority2 (Master only):
The attribute is used in the execution of the best master clock algorithm. Lower values take precedence. Configurable range: 0..255.
In the event that the operation of the best master clock algorithm fails to order the clocks based on the values of priority1, clockClass, clockAccuracy, and scaledOffsetLogVariance, the priority2 attribute allows the creation of up
to 256 priorities to be evaluated before the tiebreaker. The tiebreaker is based on the clockIdentity.
The values clockClass, clockAccuracy, and scaledOffsetLogVariance depend on the internal state of the grandmaster and cannot be configured.

Timescale:

- **"1":** PTP(TAI) time scale (TAI time stamp in sync messages). This is the default setting. Slave devices will be able to calculate the UTC time when substracting the UTC offset value of the announce message from the TAI time stamp of the Sync Message. The TAI time scale is the International Atomic Time scale which was started on January 1st, 1970 synchronous to UTC time. No leap seconds have been inserted

since then to create a monotonic time scale. That's why the TAI time scale was 34 seconds ahead of UTC in 2010.

- **"0":** ARB (arbitrary time scale): User defined time scale where the UTC offset in the Announce message will be set to 0. This setting shall be used for test purposes only. Slaves will not be able to calculate the correct UTC time!

MRS only
The global parameters that are common in all Slave modes are:

Default Asymmetry Offset:
If a network path has a constant asymmetry offset which is known and has been measured separately, then this offset can be entered to compensate the time offset.

Maximum Path Delay:
Path Delay measurements above this value will be ignored

Unicast Master

If unicast mode is selected then an additional sub menu will appear to configure or display unicast specific parameters.

```
-> Global PTP Parameters <-
   Unicast Parameters
```

```
Prio1:128   Prio2:128 Domain:0 ↵
DelayMech:E2E    Netw.Prot:UDP
Timescale: 1
```

```
   Global PTP Parameters
-> Unicast Parameters <-
```

```
    Unicast Settings
-> Clock ID <-
```

```
PTPv2 Unicast Clock Identity
 of this Unicast Master is:
   00:50:C2:FF:FE:C2:DB:94
```
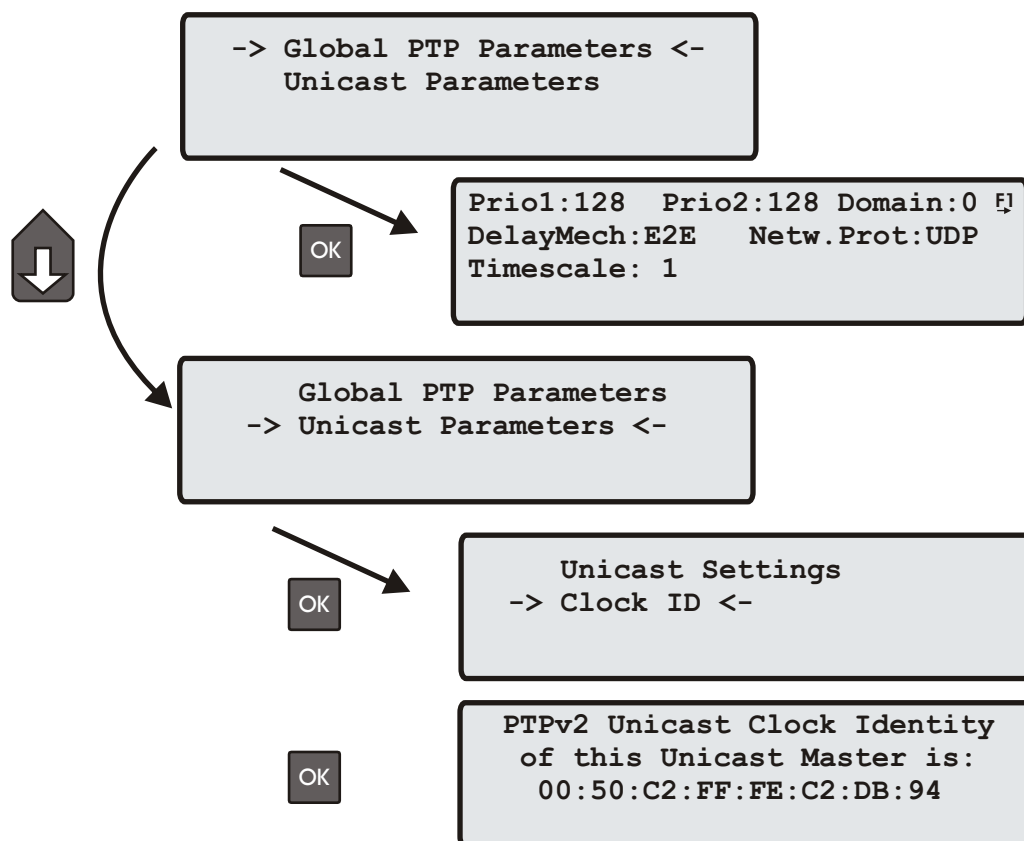
In "Unicast Master" mode, only the "Clock ID" will be displayed for informational purpose. This is the Clock Identity of the grandmaster and represents the MAC ID of the PTP port. The "Unicast Negotiation" feature is supported when operating as grandmaster, therefore all Unicast specific message parameters have to be configured on the Slave.

Unicast Slave (MRS only)

```
          -> Global PTP Parameters <-
             Unicast Parameters
```

```
    OK        Def.Asym.Offs[ns]:-              ↲
              Max.Pathdelay[ns]: 0
              Domain Number    : 0
              DelayMech:E"E    Netw.Prot:UDP
```

```
             Global PTP Parameters
          -> Unicast Parameters <-
```

```
    OK            Unicast Settings
              -> Clock ID <-    Delay. resp.
                 Sync Msg       Announce
```

```
    OK        PTPv2 Unicast Clock Identity  ↲
                   of Unicast Master
              ClockID:00:50:C2:FF:FE:C2:DB:94
              Protocol Addr: 172.016.003.180
```

```
           -> Sync Msg <-
           Set Unicast Sync messages:     ↲
           Sync Msg. requested:☐enabled
           Sync Interval[2^x]:    2s
           Sync Duration[s]: 100000
```

```
           -> Delay. resp. <-
           Set Unicast Delay Resp. mess.:↲
           Delay Resp. requested:☐enabled
           Delay Resp. Interval[2^x]:  2s
           Delay Resp. Duration[s]:100000
```

```
           -> Announce <-
           Set Unicast Announce messages:↲
           Announce requested:☐enabled
           Announce Interval[2^x]:    2s
           Announce Duration[s]: 100000
```

Clock ID:
The correct Clock ID of the selected Master must be entered here. Alternatively "FF:FF:FF:FF:FF:FF:FF:FF"
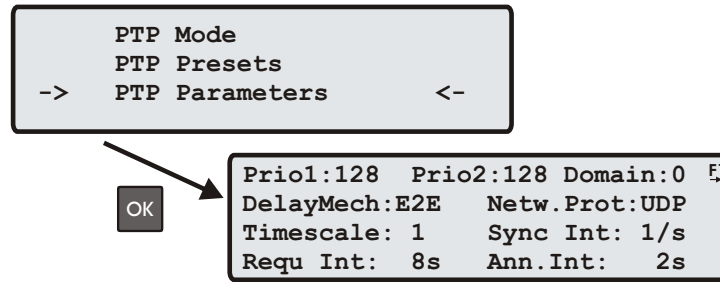can be configured to accept every clock ID which is present behind a certain Master IP address.

The correct IP address of the Master's PTP port must be entered under **"Protocol Address"** .

Message Rates and duration for Sync, Announce and Delay Response Messages:
These sub menus allow the configuration of the different PTP messages that shall be sent from the Grandmaster
to the slave. It can be configured which message at which rates and for how long they are requested from a
grandmaster clock within the "unicast message negotiation" mechanism.

For requesting a certain message, the **"Message requested"** parameter must be set to "enabled". The **"Inter-
val"** parameter represents the message rate that is requested from the grandmaster. The **"Duration"** parameter
is used to set a timeout for the grandmaster that sends out the requested message unit the timeout expires. A
slave sends a new signaling message to refresh the request before the end of this timeout to receive the requested
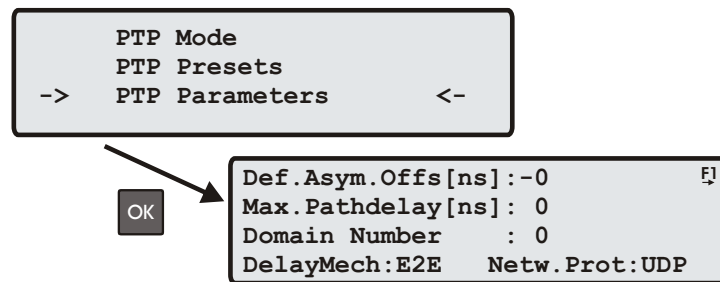message continuously.

Multicast Master

```
          PTP Mode
          PTP Presets
->        PTP Parameters          <-
```

```
  Prio1:128   Prio2:128 Domain:0  ↵
  DelayMech:E2E    Netw.Prot:UDP
  Timescale: 1     Sync Int: 1/s
  Requ Int:  8s    Ann.Int:   2s
```

OK

In addition to the already described parameters which are described in the chapter Global Parameters, the following settings can be done in Multicast Master Mode.

- Sync Int: Packet rate of the Sync Messages (64/sec...64 sec).

- Requ Int: Minimum allowed interval between two Delay Measurements which are executed by the Slaves (64/sec...64 sec).

- Ann. Int: Packet rate of the Announce Messages (64/sec...64 sec).

Multicast Slave (only on MRS devices)

```
          PTP Mode
          PTP Presets
->        PTP Parameters          <-
```

```
  Def.Asym.Offs[ns]:-0            ↵
  Max.Pathdelay[ns]: 0
  Domain Number     : 0
  DelayMech:E2E    Netw.Prot:UDP
```
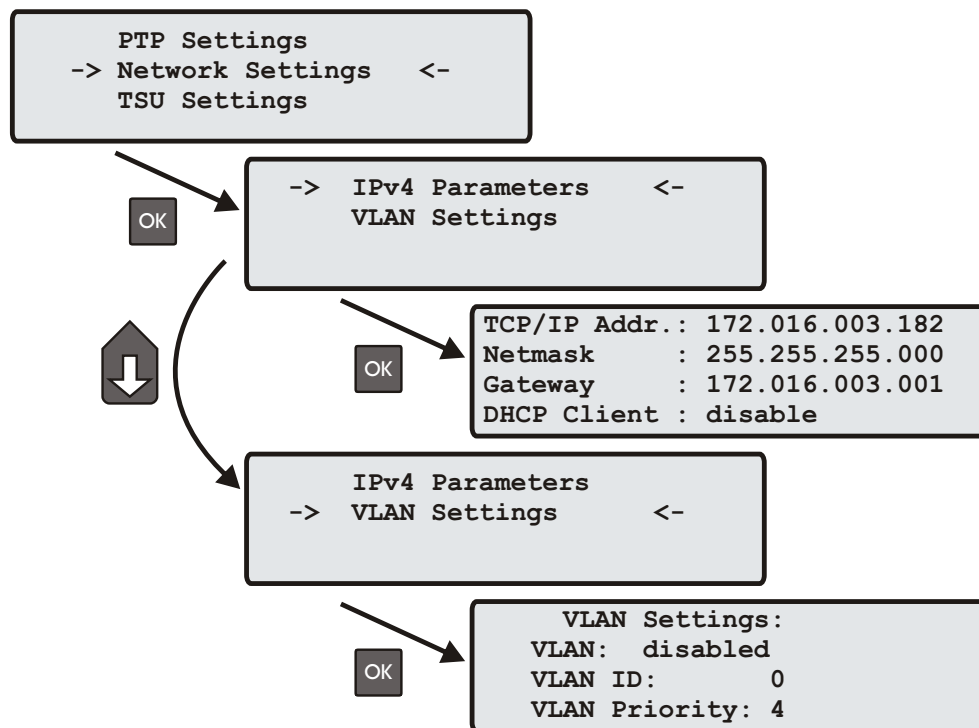
OK

In addition to the already described common parameters which can be found in the chapter "Global Parameters", the following settings can be done in Multicast Slave Mode.

- Def.Asym.Offs: An initial calibration value (in ns) can be entered here if a certain asymmetry offset of the network path is known when the PTP unit starts. This occurs in SDH networks for example.

- Max. Path Delay: If a measured path delay exceeds the value of this parameter (in ns), then the PTP unit is able to detect a change in the asymmetry offset and can take this into account for its delay measurements.

Note: Changes to the default settings (0 ns for both parameters) should be done only if problems with the client synchronization accuracy are observed and only if the asymmetry offset can be measured.

Menu Network Settings

Configuration for the PTP network port

```
        PTP Settings
     -> Network Settings   <-
        TSU Settings
```

OK

```
     ->  IPv4 Parameters     <-
         VLAN Settings
```

OK

```
TCP/IP Addr.: 172.016.003.182
Netmask      : 255.255.255.000
Gateway      : 172.016.003.001
DHCP Client : disable
```

```
         IPv4 Parameters
     ->  VLAN Settings        <-
```

OK

```
        VLAN Settings:
        VLAN:  disabled
        VLAN ID:        0
        VLAN Priority: 4
```

IPv4 parameters:

```
TCP/IP Addr.: 172.016.003.182
Netmask      : 255.255.255.000
Gateway      : 172.016.003.001
DHCP Client : disable
```

IP configuration for the PTPx interface. It can be selected if either a static IP address shall be used or if a dynamic IP address via DHCP should be assigned.

VLAN settings

Configuration of Virtual LAN (IEEE 802.1Q) settings for the PTPx interface:

```
        VLAN Settings:
        VLAN:  disabled
        VLAN ID:        0
        VLAN Priority: 4
```

- VLAN ID: A 12-bit value (0..4096) specifying the VLAN to which the network port belongs.
- VLAN Priority: The priority indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data,...)

11.5 Programmable pulse (Option)

At the male connector type VG64 there are optionally three programmable TTL outputs (Prog Pulse 1-3), which are arbitrarily programmable.

11.5.1 SETUP POUT X

This menu is used for configuration of the pulse outputs.
There are three pulse outputs available (POUT 1-3).

```
Programmable Pulses Output
    Output 1: TIMER
    Output 2: CYCLIC
    Output 3: PASSIV
```

With the arrow key right or OK Button the parameters of each programmable pulse output can be set:

```
Programmable Pulses Output
--->      Output 1      <---
          Output 2
          Output 3
```

Each programmable pulse output has its own Mode to be set. With the arrow keys up and down the mode can be selected:

```
---> POUT1 Mode PASSIV <---
     POUT1 Mode TIMER
     POUT1 Mode SINGLE
     POUT1 Mode CYCLIC
     POUT1 Mode PPS
     POUT1 Mode PPM
     POUT1 Mode PPH
```

11.5.2 Mode

This field selects the mode of operation of an output. Possible modes are PASSIV, TIMER, SINGLE, CYCLIC, PPS, PPM and PPH.

11.5.3 Timer Mode

```
              POUT1 TIMER1
         output activ: low
              Time ON: 10:50:00
              Time OFF: 11:00:00
```

```
              POUT1 TIMER2
         output activ: low
              Time ON: 13:00:00
              Time OFF: 14:00:00
```

```
              POUT1 TIMER3
         output activ: low
              Time ON: 23:45:00
              Time OFF: 09:30:00
```

If Timer mode is selected, a window as shown above is displayed. The switching plan is assigned per day. Three turn-on and turn-off times are programmable for each output. If a switching time has to be configured, only the turn-on and turn-off time must be programmed. Thus the example shows switching times from 10:50 to 11:00, 13:00 to 14:00 and 23:45 to 09:30. A turn-off time earlier than the turn-off time would cause the output to be enabled over midnight. For example a program 'ON Time' 10:45:00, 'OFF Time' 9:30:00 would cause an active ouput from 10:45 to 9:30 (the next day!). If one or more of the three switching times are unused just enter the same time into the fields 'ON Time' and 'OFF Time'. In this case the switch time does not affect the output.

11.5.4 Single Pulse

Selecting Single Pulse generates a single pulse of defined length once per day.

```
              POUT1 SINGLE:
         output activ: low
              Time: 12:00:00
              Length: 00.10 sec
```

You can enter the time when the pulse is generated in the field 'Time'. The value in field 'Length' determines the pulse duration. A pulse duration from 10 msec to 10 sec in steps of 10 msec can be selected.
The example shows a single pulse at 12:00 every day with a duration of 100 ms.

11.5.5 Cyclic mode

Cyclic mode is used for generating periodically repeated pulses.

```
              POUT1 CYCLIC:
         output activ: low
              Time: 00:00:02
              Length: 00.10 sec
```

The value in field 'Time' determines the time between two consecutive pulses (2 sec in example above). This cycle time must be entered as hours, minutes and seconds. The pulse train is synchronized at 0:00 o'clock local time, so the first pulse of a day always occurs at midnight. A cycle time of 2 seconds for example, would cause pulses at 0:00:00, 0:00:02, 0:00:04 etc. Basically it is possible to enter any cycle time between 0 and 24 hours, however only a cycle times that causes a constant distance between all consecutive pulses make sense. For example a cycle time of 1 hour 45 minutes would generate a pulse every 6300 seconds (starting from 0 o'clock). The duration between the last pulse of a day and the first pulse of the next day (0:00:00 o'clock) would only be 4500 sec.

11.5.6 PPS, PPM, PPH Modes

```
  POUT1 Pulse Per Sec (PPS):


     output activ: low
     Length: 00.10 sec
```

```
  POUT1 Pulse Per Min (PPM):


     output activ: low
     Length: 00.10 sec
```
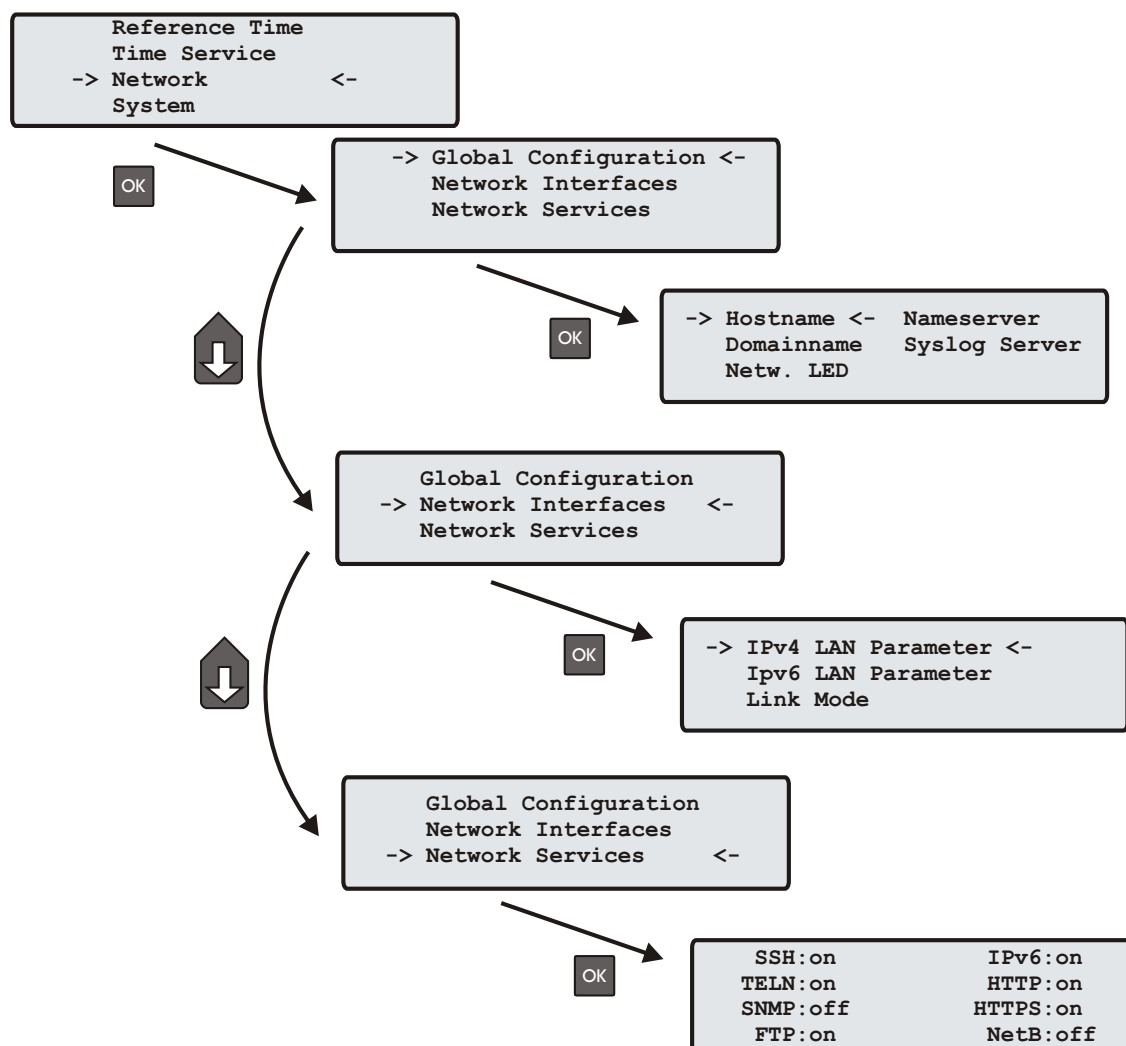
```
  POUT1 Pulse Per Hour (PPH):


     output activ: low
     Length: 00.10 sec
```

These modes generate pulses of defined length once per second, once per minute or one per hour. 'Time' determines the pulse duration (10 msec...10 sec). The respective output remains in active state, when selecting a pulse duration longer than 990ms in pulse per sec mode.
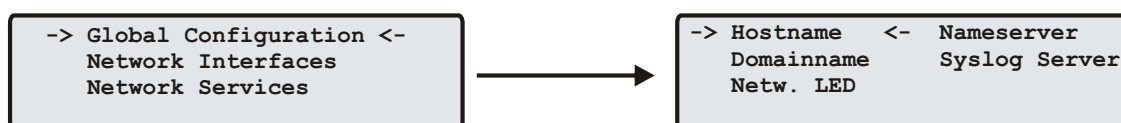
11.6 Menu: Network

```
        Reference Time
        Time Service
     -> Network          <-
        System
```

`OK`

```
     -> Global Configuration <-
        Network Interfaces
        Network Services
```

`OK`

```
     -> Hostname <-   Nameserver
        Domainname    Syslog Server
        Netw. LED
```

```
        Global Configuration
     -> Network Interfaces   <-
        Network Services
```

`OK`

```
     -> IPv4 LAN Parameter <-
        Ipv6 LAN Parameter
        Link Mode
```

```
        Global Configuration
        Network Interfaces
     -> Network Services     <-
```

`OK`

```
        SSH:on          IPv6:on
        TELN:on         HTTP:on
        SNMP:off        HTTPS:on
         FTP:on          NetB:off
```

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

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

11.6.1 Menu: Global Configuration

```
     -> Global Configuration <-
        Network Interfaces
        Network Services
```

```
     -> Hostname    <-   Nameserver
        Domainname        Syslog Server
        Netw. LED
```
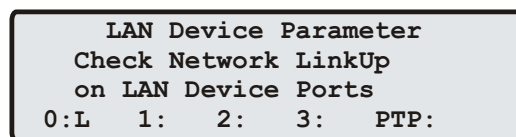
In this sub menu you can change the global network settings like host and domain name, nameserver and syslog server. Further name- or syslog servers can be set up via HTTP interface or CLI Setup. In the nameserver and

syslog server fields you have to enter an Ipv4 address.

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

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

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

```
           LAN Device Parameter
        Check Network LinkUp
        on LAN Device Ports
      0:L   1:   2:   3:   PTP:
```

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

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

11.6.2 Menu: Setup Network Interfaces

```
        Global Configuration          -> IPv4 LAN Parameter  <-
     -> Network Interfaces   <-          IPv6 LAN Parameter
        Network Services                 Link Mode
```
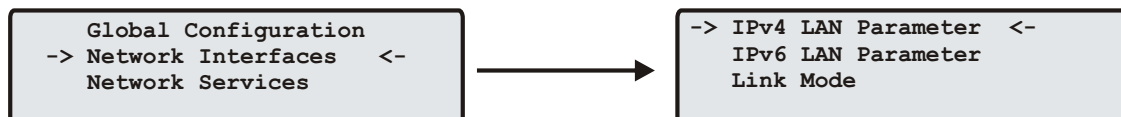
11.6.3 Menu: Setup IPv4 LAN Parameter

```
        IPv4 LAN Parameter            ETH0: -> DHCP:   enabled  <-
     -> ETH0 <-    ETH1                      ADDRESS:  172.16.3.64
        ETH2      ETH3                       NETMASK:  255.255.255.0
              PTP0                      DEF.GATEWAY:
```

There is a separate configuration submenu for every physical network interface. If there is no DHCP client mode
activated a static IP address for each interface can be entered. IPv4 addresses are built of 32 bits which are
grouped in four octets, each containing 8 bits. You can specify an IP address in this mask by entering four
decimal numbers, separated by a point "." .
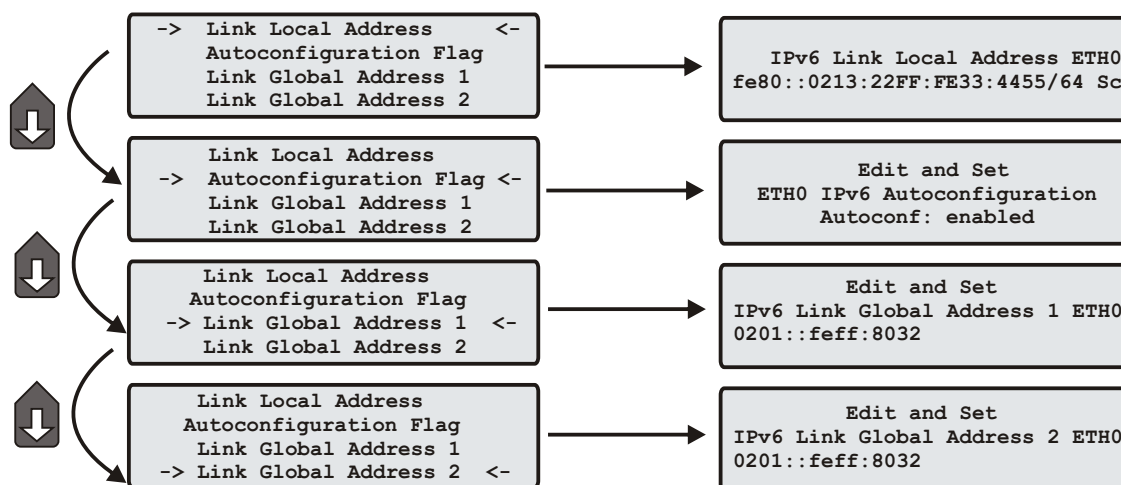
Example: 192.168.10.2

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

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

If there is a DHCP (Dynamic Host Configuration Protocol) server available in your network, the 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". Using DHCP is the default factory setting.

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

11.6.4 Menu: Setup IPv6 Parameter

```
-> Link Local Address    <-          IPv6 Link Local Address ETH0
   Autoconfiguration Flag            fe80::0213:22FF:FE33:4455/64 Sc
   Link Global Address 1
   Link Global Address 2
```

```
   Link Local Address                       Edit and Set
-> Autoconfiguration Flag <-          ETH0 IPv6 Autoconfiguration
   Link Global Address 1                  Autoconf: enabled
   Link Global Address 2
```

```
   Link Local Address                       Edit and Set
   Autoconfiguration Flag            IPv6 Link Global Address 1 ETH0
-> Link Global Address 1  <-          0201::feff:8032
   Link Global Address 2
```

```
   Link Local Address                       Edit and Set
   Autoconfiguration Flag            IPv6 Link Global Address 2 ETH0
   Link Global Address 1             0201::feff:8032
-> Link Global Address 2  <-
```

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

If you enabled the IPv6 protocol, the 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.

11.6.5 Menu: Link Mode

```
   Global Configuration                 IPv4 LAN Parameter
-> Network Interfaces   <-              IPv6 LAN Parameter
   Network Services                  -> Link Mode            <-
```

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

11.6.6 Menu: Network Services

```
 SSH:on            IPv6:on
TELN:on            HTTP:on
SNMP:off          HTTPS:on
 FTP:on            NetB:off
```
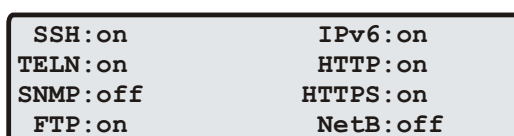
The possible network protocols and access methods can be configured. After pressing the OK button you can enable/disable SSH, TELNET, SNMP, FTP, IPV6, HTTP, HTTPS and NETBIOS by using the UP/DOWN Keys and navigate through the list with the LEFT/RIGHT keys. After you saved your settings with the "OK" button, all these subsystems are stopped and eventually restarted (only if they are enabled, of course).

11.7 Menu: System

```
        Reference Time                    -> Set time zone              <-
        Time Service                         Restart NTP
        Network                              Reset to factory defaults
     -> System          <-                   Reboot time server
```

In this submenu system specific parameters can be configured.

With **Set time zone** the time zone displayed on the front panel display can be configured (see below).

With **Restart NTP** you can stop the currently running NTP daemon and restart it afterwards.

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

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

11.7.1 Menu: Set time zone

```
  -> Set time zone            <-            Time Zone parameters
     Restart NTP                                 of display
     Reset to factory defaults           -> Daylight Saving OFF <-
     Reboot time server                      Daylight Saving ON
```

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

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

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

All changeover rules for the daylight saving like "the first/the second/the second to last/the last Sunday/Monday etc. in the x-th month," can be described by the used format "first specified day-of-week after a defined date".
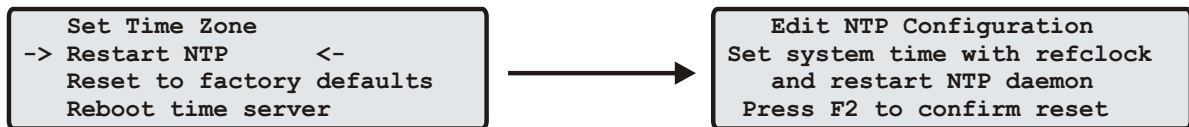
If the number of the year is not displayed as wildcards the complete date exactly determines the day daylight saving has to change (October 26th, 2008 in the figures below), so the day-of-week does not need to be specified and therefore is displayed as wildcards.

```
 Time Zone Daylight Saving OFF          Time Zone Daylight Saving OFF
 TZ Name: MEZ   Offs.UTC:+01:00h        TZ Name: MEZ   Offs.UTC:+01:00h
 Day of Week: Sun                       Day of Week: ***
 Date:25.10.****  Time:03:00:00         Date:26.10.2008  Time:03:00:00
```

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

11.7.2 Menu: Restart NTP

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

```
    Set Time Zone
-> Restart NTP       <-
   Reset to factory defaults
   Reboot time server
```

```
    Edit NTP Configuration
Set system time with refclock
   and restart NTP daemon
 Press F2 to confirm reset
```

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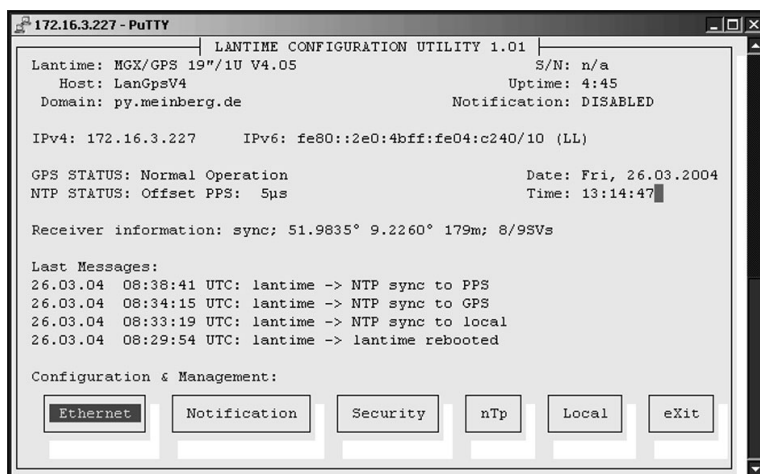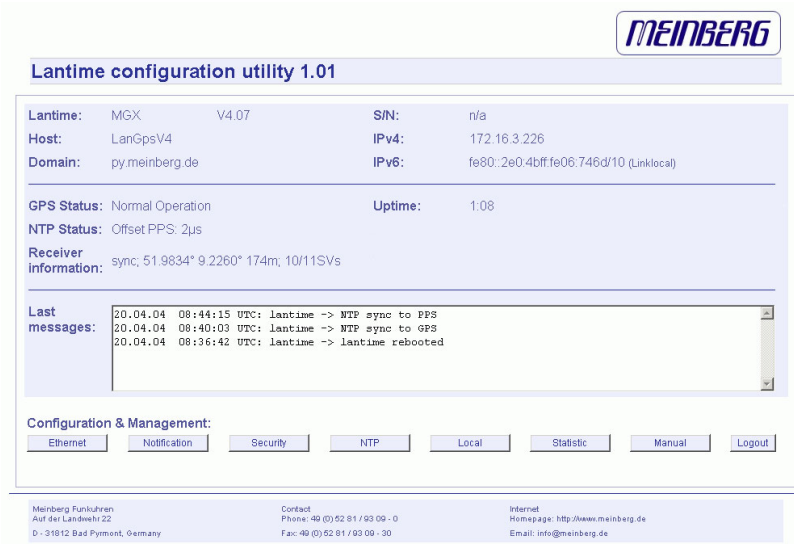
In addition to the SNMP and web interface, you can also manage your LANTIME configuration via a command line interface (CLI), which can be used via a TELNET or SSH connection. A setup tool can be started after login, just type "setup" and press ENTER at the prompt.

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 screen shots show the web interface and the Command Line Interface setup tool. The CLI setup tool cannot 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.

13 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 receiver.

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 day of the week. 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 with the receiver, this can also appear if the receiver looses synchronisation and the NTP switches back to its "LOCAL CLOCK" time source.

The receiver is connected to the LANTIME system internally by using a serial connection and additionally by using the second pulse. There are therefore 2 references used by NTPD, the receiver (GPS, 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 GPS [PZF,MSF,WWV,TCR]: x" or "NTP: Offset PPS: x" where "x" is the actual offset to the receiver or PPS time source.

This page will be reloaded every 30 seconds in order to reflect the current status of the unit. Please bear 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 user and password field is cleared and you have to start over again.

13.1 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 GPS reference clock and the NTP subsystem is shown, additional information about the GPS receiver are also found here. This includes the number of satellites in view and the number of good satellites in view.

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.

13.2 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 domain name. 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).

13.2.1 SYSLOG Server

All information written to the LANTIME SYSLOG (/var/log/messages) can be forwarded to one or two remote SYSLOG servers. The SYSLOG daemon of this remote SYSLOG needs to be configured to allow remote systems

to create entries. A Linux 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 cannot be used over IPv6 in this version. It is no problem to use IPv4 and IPv6 in a mixed mode environment on your LANTIME.

13.3 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.

13.3.1 IPv4 addresses and DHCP

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

Example: 192.168.10.2

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

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

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

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

13.3.2 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.

13.3.3 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.

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

13.3.4 Additional Network Configuration

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

Also the Samba Configuration from "/etc/samba/smb.conf" can be edited:

13.4 Configuration: Notification

13.4.1 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 different ways of informing the administrator or a responsible person about

nine different events: EMAIL sends an e-mail message to a specified e-mail account, SNMP-TRAP sends a SNMP trap to one or two SNMP trap receivers, WINDOWS POPUP MESSAGE sends a winpopup message to one or two different computers. DISPLAY shows the alarm message on a wall mount display model VP100/NET, which is an optional accessory you can obtain for your LANTIME. You also can use user defined scripts and the error relay out (see appendix).

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

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

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

- mbgLtTrapConfigChanged
- mbgLtTrapLeapSecondAnnounced
- mbgLtTrapServerBoot

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

13.4.2 E-mail messages

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

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

- The host name and domain name should be known to the SMTP smarthost

- A valid nameserver entry is needed

- The domain part of the "From:" address has to be valid

13.4.3 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:
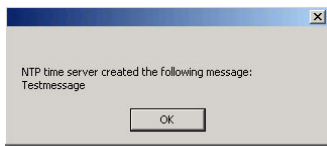
13.4.4 SNMP-TRAP messages

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).

13.4.5 VP100/NET wall mount display

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

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

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

13.4.6 User defined Alarm scripts

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

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

13.4.7 NTP Client Monitoring

You can monitor a group of NTP clients and supervise the time offset, the NTP stratum value and if the client is reachable or not. With the button „edit client list" you can edit the list of clients to monitor. You can add the TCP/IP address or the hostname of the client:

You can monitor the current states of the configured clients:

13.4.8 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.

13.5 Configuration: Security

Security management

Login:

Config HTTP access control

Front Panel:

Lock Front Panel: Deactivated

SSH key generation:

Generate SSH key   Show SSH key

HTTPS certificate generation:

Generate SSL certificate for HTTP   Show SSL certificate for HTTP

[   ] Durchsuchen…
Upload HTTPS certificate   Download HTTPS certificate

NTP autokey generation:

Generate new NTP public key   Generate groupkey

[   ] Durchsuchen…
Upload groupkey

NTP autokey password: ●●●●●●●●●

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
Please edit these values on the local page

User name: root

Authentication passphrase: [   ]

Re-enter passphrase: [   ] Change SNMP v3 authentication

Save settings   Reset changes   Back

13.5.1 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.

13.5.2 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:

13.5.3 SSH Secure Shell Login

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

ssh root @ 192.168.16.111

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

Default Password: **timeserver**

If you generate a new SSH key, you can copy and paste it into your SSH client configuration afterwards in

order to allow you to login without being prompted for a password. We strongly recommend to use SSH for shell access, TELNET is a very insecure protocol (transmitting passwords in plain text over your network).

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

13.5.4 Generate SSL Certificate for HTTPS

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

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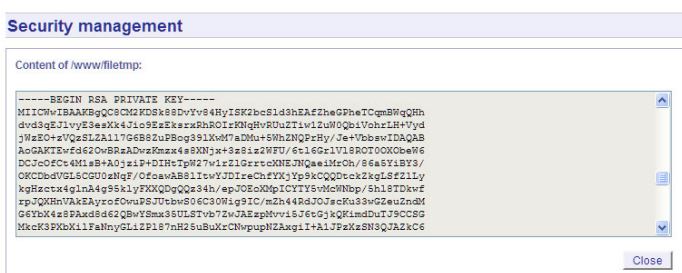
It is also possible to upload your own HTTPS certification. If you upload a non valid certification HTTPS will not work.

13.5.5 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).

Security management

Content of /mnt/flash/config/ntp/ntp.key:

```
6 M key1
```

Save file   Close

13.5.6 SNMP Parameter

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

13.6 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 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. The local clock can be disabled if the timeserver should not answer any more when the reference clock is out of order.

Because the reference clock is internally connected to the LANTIME system by using a serial connection, the accuracy using this way of synchronisation is around 1 ms. The high accuracy of the LANTIME timeserver (around 10 microseconds) is available by using the 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 GPS167 with UNI ERLANGEN

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

server 127.127.8.0 mode 135 prefer    # GPS167 UNI Erlangen PPS
fudge 127.127.8.0 time1 0.0042        # relative to PPS
server 127.127.22.0                   # ATOM (PPS)
fudge 127.127.22.0 flag3 1            # enable PPS API
enable stats
statsdir /var/log/
```

statistics loopstats
driftfile /etc/ntp.drift

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

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 five 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 "Prefer" flag can be set for each external server. The internal refclock has set this flag by default. The "Prefer" flag is usefull if one of the refclocks are not available or out of sync.

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 or space 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
keys /etc/ntp/keys
trustedkey 6 15
requestkey 15
controlkey 15
```


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

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

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


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

NTP management

Content of /mnt/flash/config/ntp/ntpconf.add:

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

Save file   Close

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.
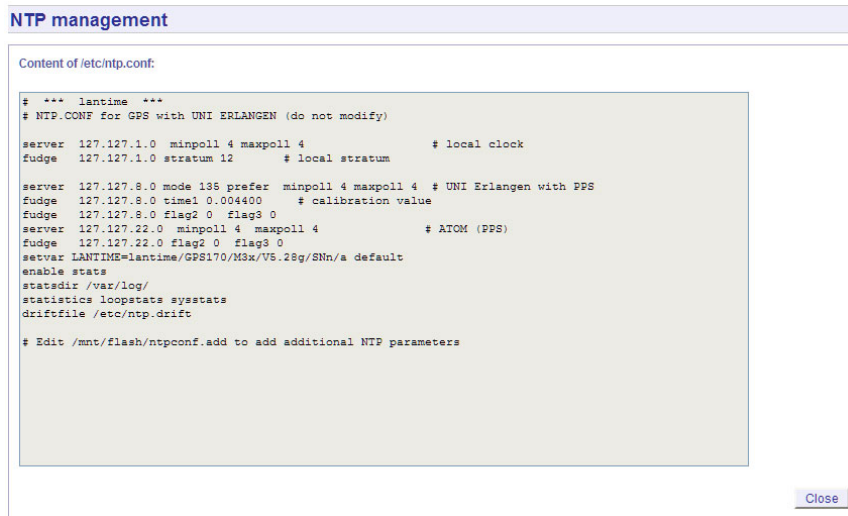
13.6.1 NTP Authentication

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.

- The LANTIME supports MD5 authentication only.

- Please be aware of the following restrictions: No **"#", "t" (tab), "n" (newline) and "0"** (null) are allowed in a DES or MD5 ASCII key. The key ID 0 is reserved for special purposes and should not appear in the keys file.

13.6.2 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, if they are already included):

    crypto pw cryptosecret
    keysdir /etc/ntp/

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

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

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

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

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

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

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

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

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

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

Example:
This autokey group is formed by one Stratum-1-server (B), two Stratum-2-servers (D and E) and a number of clients (in the diagram there are 4 clients shown, c1 − c4). B is the trusted host, he holds the group key and a self-signed certificate marked as "trusted".
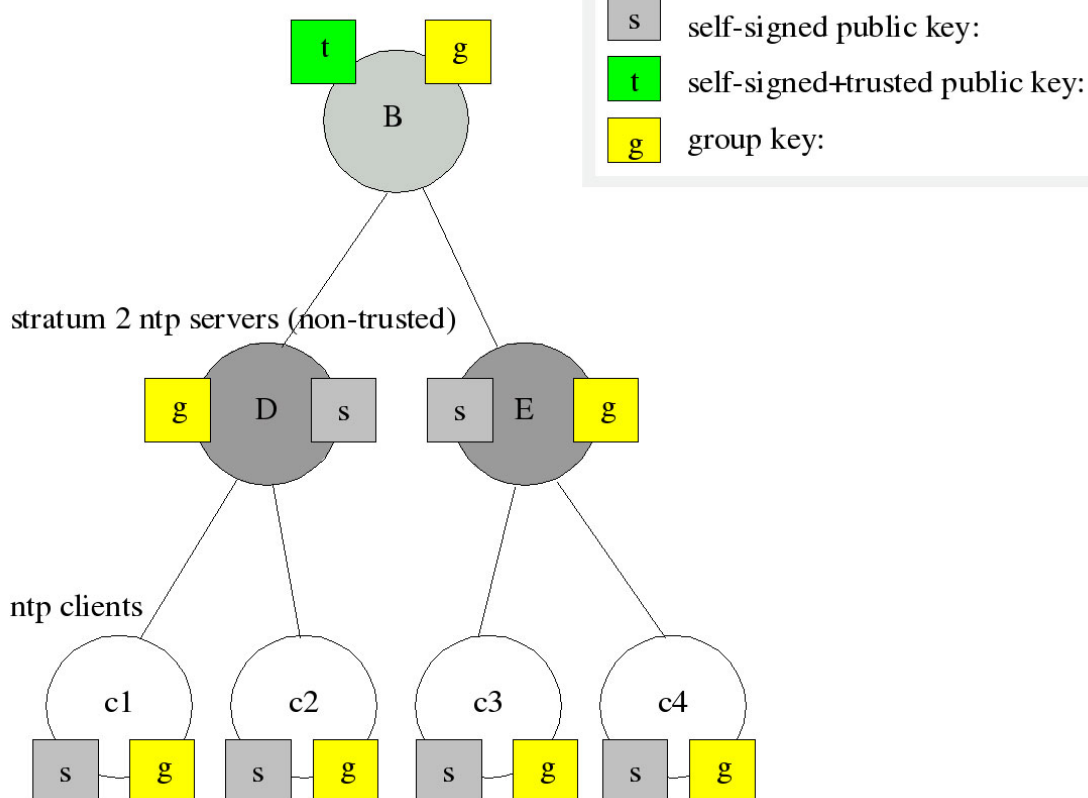
D and E are NTP servers, which are "non-trusted" hosts of the group, they hold the group key and a self-signed certificate which lacks the "trusted" mark. The clients also hold the group key and a self-signed certificate. In order to distribute new public keys to the whole group, the administrator only has to generate a new "t" key, which will be distributed automatically to the two hosts D and E. Because these two servers can now present a unbroken chain of certificates to a trusted host, they can be considered "trusted" by the clients as well.

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

13.7 Configuration: Local

13.7.1 Administrative functions

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

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

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

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

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

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

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

13.7.2 User Management

For administration different users can be set up. 3 group memberships can be assigned to each user: the Super-User has all properties for administration. The group membership Administrator can change all parameters via the command line interface (CLI) configuartion tool and the WEB interface. The group Administrator cannot use any Linux command in a Telnet, SSH or Terminal session. If the Administrator will login, the setup program will be started directly. After termination of the Setup program this user will be logout automatically. The group membership "Info" has the same properties like the Administrator but cannot change any parameter.

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

13.7.3 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 (upper case) kernel. The SYSLOG file /var/log/messages is only stored in
the system's ram disk, therefore it is lost after a power off or restart. If you configured an external SYSLOG
server, all LANTIME syslog entries will be duplicated on this remote system and can be saved permanently this way.

    Mar 15 13:35:17 LanGpsV4 ntpd[12948]:   ntpd 4.2.0@1.1161-r Fri Mar 5 15:58:48 CET 2004 (3)
    Mar 15 13:35:17 LanGpsV4 ntpd[12948]:   signal_no_reset: signal 13 had flags 4000000
    Mar 15 13:35:17 LanGpsV4 ntpd[12948]:   precision = 3.000 usec
    Mar 15 13:35:17 LanGpsV4 ntpd[12948]:   kernel time sync status 2040
    Mar 15 13:35:17 LanGpsV4 ntpd[12948]:   frequency initialized 45.212 PPM from /etc/ntp.drift
    Mar 15 13:38:36 LanGpsV4 lantime[417]:   NTP sync to GPS
    Mar 15 13:38:36 LanGpsV4 lantime[417]:   NTP restart
    Mar 15 13:45:36 LanGpsV4 proftpd[14061]:   connect from 172.16.3.2 (172.16.3.2)
    Mar 15 14:01:11 LanGpsV4 login[15711]:   invalid password for 'root' on 'ttyp1' from '172.16.3.45'
    Mar 15 14:01:17 LanGpsV4 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 GPS information" gives you the possibility to check detailed GPS status information. The first parameter indicates the time and date of the last update of the shown parameters. Next you find the GPS receiver status and the NTP status, followed by the GPS position data. The position uses the Latitude / Longitude / Altitude format. Latitude and Longitude are shown in degrees, minutes and seconds, Altitude is shown in meters above WGS84 ellipsoid.

The satellite section shows the numbers of satellites in view and the number of usable satellites ("good SV"). Additionally, the selected set of the four used satellites can be read.

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

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

13.7.4 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.

13.7.5 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 reachabilitytests, the whole check process may take a while.

13.7.6 Get Diagnostics Information

The diagnostics information is a set of configuration parameters and files stored in a packed text file. With the help of these informations the technical support from Meinberg can reproduce the current state of your LANTIME. It takes some time to collect all information from the LANTIME. Do not press the button again while this process is running - some web browsers will cancel the job if you press the button twice. After that you can download the packed file "config.zip" to your local computer. If you have any questions or problems with your LANTIME please send this file "config.zip" as an attachment of an e-mail to Meinberg support and describe your problem.

13.7.7 Web interface language

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

13.8 Configuration: Statistics
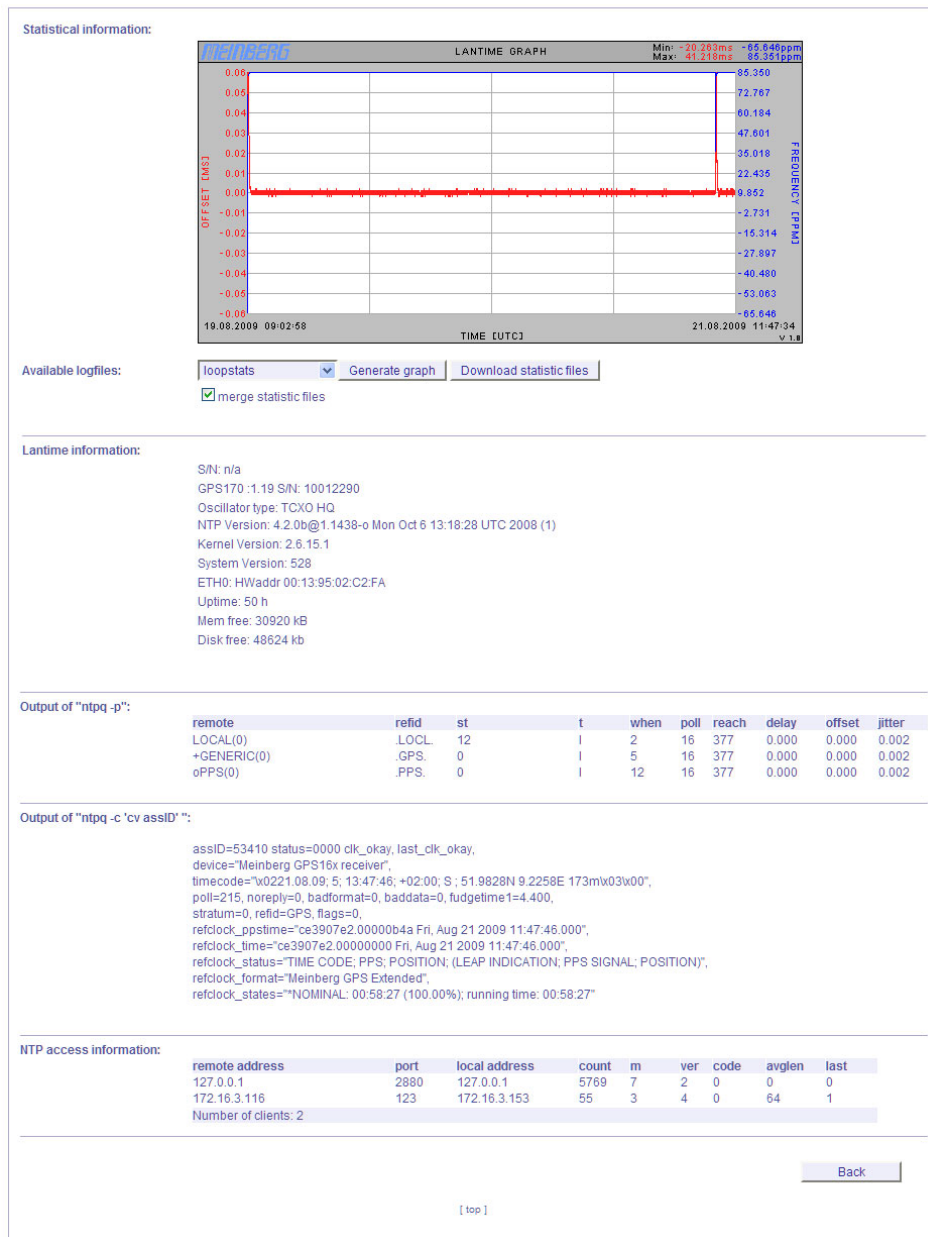
13.8.1 Statistical Information

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

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

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

After that a list of all actually refclocks of the internal NTP server will be shown.

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

with the following meaning:

———

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

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

13.9 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.

14 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.

```
172.16.3.227 - PuTTY                                              _ □ ×
          ┤ LANTIME CONFIGURATION UTILITY 1.01 ├
  Lantime: MGX/GPS 19"/1U V4.05                      S/N: n/a
     Host: LanGpsV4                              Uptime: 4:45
   Domain: py.meinberg.de                  Notification: DISABLED

  IPv4: 172.16.3.227     IPv6: fe80::2e0:4bff:fe04:c240/10 (LL)

  GPS STATUS: Normal Operation                   Date: Fri, 26.03.2004
  NTP STATUS: Offset PPS:  5µs                   Time: 13:14:47

  Receiver information: sync; 51.9835° 9.2260° 179m; 8/9SVs

  Last Messages:
  26.03.04  08:38:41 UTC: lantime -> NTP sync to PPS
  26.03.04  08:34:15 UTC: lantime -> NTP sync to GPS
  26.03.04  08:33:19 UTC: lantime -> NTP sync to local
  26.03.04  08:29:54 UTC: lantime -> lantime rebooted


  Configuration & Management:

   ┌──────────┐  ┌──────────────┐  ┌──────────┐  ┌─────┐  ┌───────┐  ┌──────┐
   │ Ethernet │  │ Notification │  │ Security │  │ nTp │  │ Local │  │ eXit │
   └──────────┘  └──────────────┘  └──────────┘  └─────┘  └───────┘  └──────┘
```

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 GPS reference clock and the NTP subsystem is shown, additional information about the GPS receiver can also be found here. This includes the number of satellites in view and the number of good satellites in view.

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, that are described below.

14.1 CLI Ethernet

```
                    ┤ ETHERNET CONFIGURATION ├

 <Hostname>       LantimeV4
 <Domainname>     py.meinberg.de

 <Nameserver 1>   172.16.3.1
 <Nameserver 2>

 <Syslogserver 1>
 <Syslogserver 2>

 <IPv4 Default Gateway> 172.16.3.1
 <IPv6 Default Gateway>

 <Telnet>         ENABLED      <SSH>           ENABLED
 <FTP>            ENABLED      <HTTPS>         ENABLED
 <HTTP>           ENABLED      <SAMBA>         DISABLED
                               <SNMP>          ENABLED
 <IPv6 protocol:> ENABLED

   Ethernet 0                         SAVE      CLOSE
```

In the network configuration all parameters related to the network interfaces can be changed. In the first section you can change the hostname and domain name. 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 server's 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 cannot 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.

```
┌──────────────┤ ETHERNET CONFIGURATION LINE 0 ├──────────────┐

  IPv4:  <TCP/IP address>      172.16.3.226
         <Netmask>             255.255.255.0
         <Gateway>             172.16.3.1
         <DHCP Client>         DISABLED

  IPv6:  <IP 1>
         <IP 2>
         <IP 3>
         <Autoconf>            ENABLED

               <Net Link Mode>  Auto
  <High availability bonding>  single connection

  IPv6: IP Router Advert.:
              Link local: fe80::2e0:4bff:fe04:c240/10


                                             ┌──────┐
                                             │ BACK │
                                             └──────┘
```

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

   Example: 192.168.10.2

 Additionally you can specify the IPv4 Netmask and your default gateway address.
Please contact your network administrator, who 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 "EN-ABLED". 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 16 bit 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.

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

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 provides the IP Address and the net mask of this new virtual device.

14.2 CLI Notification

```
                        ┌──────── NOTIFICATION CONFIGURATION ────────┐
  Email:        <To address>       gregoire.diehl@meinberg.de
                <From address>     LantimeGregoire
                <Smarthost>        gateway
                <CC recipients>    info@meinberg.de

  Windows Mail: <Mail address 1>
                <Mail address 2>

  SNMP:         <SNMP manager 1>
                <Community>
                <SNMP manager 2>
                <Community>

  Display       <Display 1 address>
                <Serial number 1>
                <Display 2 address>
                <Serial number 2>

      <Show user defined script>          <Edit user defined script>

  <Notification conditions>                    <SAVE>    <CLOSE>
```
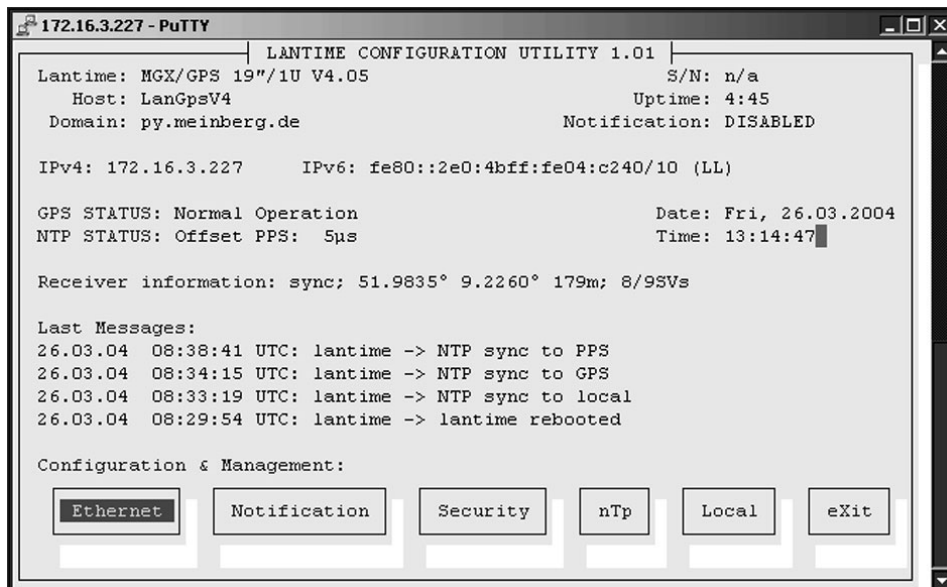
Alarm events

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 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, that is an optional accessory you can obtain from us.

"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 GPS receiver
"Receiver not sync"	Internal GPS clock is not synchronised to GPS time
"Antenna faulty"	GPS antenna disconnected
"Antenna reconnect"	GPS antenna reconnected
"Config changed"	Configuration was changed by a user
„Leap second announced"	A leap second has been announced

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.

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 who is forwarding your mail to the receiver. If your LANTIME system is connected to the internet, it can deliver those e-mails itself. Additional e-mail recipients can be configured with the button "CC recipients". These settings cannot 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

```
                    ┤ NOTIFICATION CONDITIONS ├

    Sending notification under following conditions:

    Condition:            EMail   SNMP   WinMail  Display

    NTP not sync          [█]     [ ]    [ ]      [ ]
    NTP stopped           [ ]     [ ]    [ ]      [ ]
    Server boot           [ ]     [ ]    [ ]      [ ]
    Receiver not responding [ ]   [ ]    [ ]      [ ]
    Receiver not sync     [ ]     [ ]    [ ]      [ ]
    Antenna faulty        [ ]     [ ]    [ ]      [ ]
    Antenna reconnect     [ ]     [ ]    [ ]      [ ]
    Config changed        [ ]     [ ]    [ ]      [ ]
    Leap Second announced [ ]     [ ]    [ ]      [ ]




                                              BACK
```

Windows Popup Messages

Most Microsoft Windows operating systems provide you with a local notification tool.

```
┌─────────────────────────────────┐
│                              [x] │
│                                  │
│  NTP time server created the following message: │
│  Testmessage                     │
│                                  │
│         ┌──────────┐             │
│         │    OK    │             │
│         └──────────┘             │
└─────────────────────────────────┘
```

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 (10/100 Mbit) 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 its 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.

NTP Client Monitoring
You can monitor a group of NTP clients and supervise the time offset, the NTP stratum value and if the client is reachable or not. With the button „edit client list" you can edit the list of clients to monitor. You can add the TCP/IP address or the hostname of the client:

```
                    ┤ NTP Client Monitoring ├

        <NTP client offset limit(ms)> 10
        <NTP client stratum limit>    10

        <Show client list>                  <Edit client list>

        <Show client status>








                                                     ┌──────┐
                                                     │ BACK │
                                                     └──────┘
```

You can monitor the current states of the configured clients:

```
                        ┤ NTP client status ├

  NTP Client Management updated at 18.10.05  08:49:46 UTC

  172.16.3.227 : not reachable        *** Error Condition ! ***
  server 172.16.3.228, stratum 16, offset 1.639886, delay 0.02640   ***
  Error: Offset > 10ms ! ***
  server 192.53.103.103, stratum 1, offset 0.298621, delay 0.67401   ***
  Error: Offset > 10ms ! ***






                                                          <CLOSE>
```

14.3 CLI Security

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.

```
                    ┤ CONFIG SECURITY PARAMTERS ├

    Security management:

    <Lantime password>                    <Config HTTP access control>

    <Generate SSH key>
    <Show SSH key>

    <Generate SSL certificate for HTTP>   <Show SSL certificate for HTTP>

    <Show NTP MD5 keys>                   <Edit NTP MD5 keys>
    <Generate new NTP public key>         <Generate groupkey>
    <NTP autokey password> timeserver

    <Change SNMP user>    root
    <Read community>      public
    <Write community>

    SNMP contact         Meinberg       ┌──────┐  ┌───────┐
    SNMP location        Germany        │ SAVE │  │ CLOSE │
    Please edit Contact & Location on the LOCAL page └──────┘  └───────┘
```

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 authenticate itself to the client (web browser). The first time a web browser connects to the HTTPS web server of your LANTIME, you are asked to accept the certificate of the web server. To make sure that you are talking to your known timeserver, check the certificate and accept it, if it matches the one stored on the LANTIME. All further connections are comparing the certificate with this one, which is saved in your web browser configuration. Afterwards you are prompted to verify the certificate only when it changed.

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 recreate 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).

14.4 CLI NTP Parameter

```
                         ┤ CONFIG NTP PARAMETERS ├

    <Config External NTP Server>

         <NTP Broadcast address>  0
      <NTP Broadcast intervall>
                     <Autokey>  DISABLED   <Key>

         <Stratum of local clock> 12
                  <Local Clock> ENABLED

                        <PPS>   ENABLED
                    <Autokey>  DISABLED

                  <Trusted key>

             <NTP trust time> 0     hour(s)

    <Edit additional NTP Parameter>     <Show current NTP configuration>
                                          SAVE      CLOSE
```

The NTP configuration page is used to set up the additional NTP parameters needed for a more specific config-
uration 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. The local clock
can be disabled.

Because the GPS reference clock is internally connected to the LANTIME system by using a serial connec-
tion, 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 di-
rectly interpreting the PPS (pulse per second) of the GPS reference clock. The default configuration looks like this:

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

        server        127.127.1.0                        # local clock
        fudge         127.127.1.0 stratum 12             # local stratum
        server        127.127.8.0 mode 135 prefer        # GPS167 UNI Erlangen PPS
        fudge         127.127.8.0 time1 0.0042           # relative to PPS
        server        127.127.22.0                       # ATOM (PPS)
        fudge         127.127.22.0 flag3 1               # enable PPS API

        enable stats
        statsdir /var/log/
        statistics loopstats
        driftfile /etc/ntp.drift
```

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

14.4.1 CLI NTP Authentication

Please see the corresponding chapter in the web interface description.

14.5 CLI Local

```
                        ┤ LOCAL CONFIGURATION ├
 <General Information>

 <Reboot Lantime>
 <Manual configuration>

 <Start firmware update>
 <Send test notification>

 <List all messages>
 <List detailed version information>
 <List Lantime options>
 <List detailed GPS info>

 <Save NTP drift file>

 <Reset to factory defaults>

 <Check configuration>

                                      SAVE      CLOSE
```
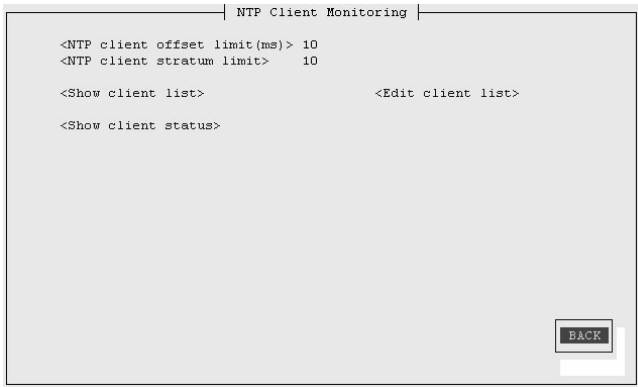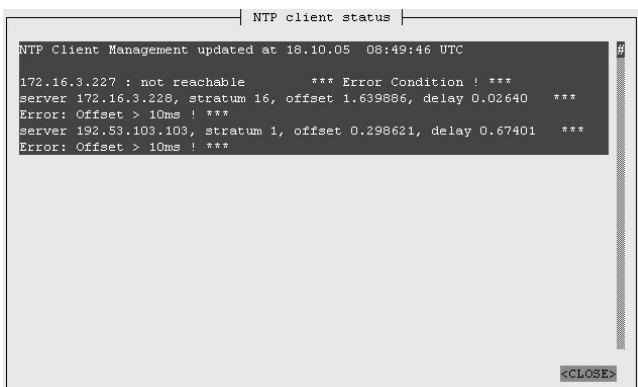
Administrative functions
In the first section there are several functions which may be used by the administrator. The button "Reboot LAN-TIME" is restarting the system, the built-in reference clock is not affected by this, only the included computer system is rebooted, which may take up to 30 seconds.

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

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

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

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

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

User Management
For administration different users can be set up. 3 group memberships can be assigned to each user: the Super-User has all properties for administration. The group membership Administrator can change all parameters via the command line interface (CLI) configuartion tool and the WEB interface. The group Administrator cannot use any Linux command in a Telnet, SSH or Terminal session. If the Administrator will login, the setup program

will be started directly. After termination of the Setup program this user will be logout automatically. The group membership "Info" has the same properties like the Administrator but cannot change any parameter.
The menu "User Management" allows you to set up different users with a password and the group membership. To change the properties of an user you have to delete the old user and set up a new one. The user "root" cannot be deleted and has always the membership of Super-User. The password of the user "root" can be set on the security page.

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 LanGpsV4 ntpd[12948]:    ntpd 4.2.0@1.1161-r Fri Mar 5 15:58:48 CET 2004 (3)
Mar 15 13:35:17 LanGpsV4 ntpd[12948]:    signal_no_reset: signal 13 had flags 4000000
Mar 15 13:35:17 LanGpsV4 ntpd[12948]:    precision = 3.000 usec
Mar 15 13:35:17 LanGpsV4 ntpd[12948]:    kernel time sync status 2040
Mar 15 13:35:17 LanGpsV4 ntpd[12948]:    frequency initialized 45.212 PPM from /etc/ntp.drift
Mar 15 13:38:36 LanGpsV4 lantime[417]:   NTP sync to GPS
Mar 15 13:38:36 LanGpsV4 lantime[417]:   NTP restart
Mar 15 13:45:36 LanGpsV4 proftpd[14061]: connect from 172.16.3.2 (172.16.3.2)
Mar 15 14:01:11 LanGpsV4 login[15711]:   invalid password for 'root' on 'ttyp1' from '172.16.3.45'
Mar 15 14:01:17 LanGpsV4 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 GPS information" gives you the possibility to check detailed GPS status information. The first parameter indicates the time and date of the last update of the shown parameters. Next you find the GPS receiver status and the NTP status, followed by the GPS position data. The position uses the Latitude / Longitude / Altitude format. Latitude and Longitude are shown in degrees, minutes and seconds, Altitude is shown in meters above WGS84 ellipsoid.

The satellite section shows the numbers of satellites in view and the number of usable satellites ("good SV"). Additionally, the selected set of the four used satellites can be read.

The accuracy of the calculated receiver position and time deviation is dependent on the constellation of the four selected satellites. Using the position of the receiver and the satellites, a number of values can be calculated, which allow a rating of the selected constellation. These values are called "Dilutions of Precision (DOP)".

PDOP is the abbreviation for "Position Dilution of Precision", TDOP means "Time Dilution of Precision" and GDOP stands for "General Dilution of Precision". Lower values are indicating better accuracy.

The next section "Satellite Info" shows information about all the satellites, which are in view momentarily. The satellite ID, elevation, Azimuth and distance to the receiver reveal the position of the satellite in the sky. The

Doppler shows whether the satellite is ascending (positive values) or descending (negative value).

Software Update
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.

15 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 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 Satellites: 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).

15.1 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 located at /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.

15.1.1 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 -v 2c -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 -v 2c -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 -v 2c -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.

15.1.2 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.

15.1.3 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, win-popup, 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.

15.1.4 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?

SNMP branch	Variable	Data type	Description
	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?
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
	mbgLtCfgStratumLocal Clock	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)
	mbgLtCfgNTPBroadcast Key	integer	Link to the key which should be used for outgoing NTP-broadcasts
	mbgLtCfgNTPBroadcast Autokey	integer (0 = disabled, 1 = enabled)	Use autokey for NTP broadcasts?
	mbgLtCfgAutokeyFeature	integer (0 = disabled, 1 = enabled)	Use autokey feature of the NTP server?

SNMP branch	Variable	Data type	Description
	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
	mbgLtCfgSNMPRO Community	string	The SNMP community, which has read-only access and therefore can be used to only monitor status variables or configuration values (SNMP V2c)
	mbgLtCfgSNMPRW Community	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
mbgLtCfgWinpopup	mbgLtCfgWMailAddress1	string	First receiver of notifications sent as windows popup messages
	mbgLtCfgWMailAddress2	string	Second receiver of notifications sent as windows popup messages

SNMP branch	Variable	Data type	Description
mbgLtCfgWalldisplay	mbgLtCfgVP100Display1IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the first wall-mount display used for showing notifications
	mbgLtCfgVP100Display 1SN	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)
	mbgLtCfgVP100Display 2IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the second wall mount display used for showing notifications
	mbgLtCfgVP100Display 2SN	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	mbgLtCfgNotifyNTPNot Sync	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"
	mbgLtCfgNotifyNTP Stopped	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „NTP Daemon stopped"
	mbgLtCfgNotifyServer Boot	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Timeserver reboot"
	mbgLtCfgNotifyRefclock NotResponding	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not ready"
	mbgLtCfgNotifyRefclock NotSync	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not synchron"
	mbgLtCfgNotifyAntenna Faulty	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna not connected or dammaged"
	mbgLtCfgNotifyAntenna Reconnect	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna reconnected"
	mbgLtCfgNotifyConfig Changed	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Configuration changed"
	mbgLtCfgNotifyLeapSecond Announced	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Leap second announced"

SNMP branch	Variable	Data type	Description
mbgLtCfgEthernet	mbgLtCfgEthernetIf0IPv4 IP	string (IPv4 IP-address)	IPv4-address of first network interface of the timeserver
	mbgLtCfgEthernetIf0IPv4 Netmask	string (IPv4 Netz-maske)	IPv4-netmask of first network interface of the timeserver
	mbgLtCfgEthernetIf0IPv4 Gateway	string (IPv4 IP-address)	IPv4-address of the default gateway of the timeservers first network interface
	mbgLtCfgEthernetIf0DHCP Client	integer (0 = dis-abled, 1 = en-abled)	Configure the first network interface of the timeserver with DHCP?
	mbgLtCfgEthernetIf0IPv6 IP1	string (IPv6 IP-address)	First IPv6-IP-address of the timeservers first network interface
	mbgLtCfgEthernetIf0IPv6 IP2	string (IPv6 IP-address)	Second IPv6-IP-address of the time-servers first network interface
	mbgLtCfgEthernetIf0IPv6 IP3	string (IPv6 IP-address)	Third IPv6-IP-address of the timeservers first network interface
	mbgLtCfgEthernetIf0IPv6 Autoconf	integer (0 = dis-abled, 1 = en-abled)	Activate autoconf for the IPv6 - config-uration of the timeservers first network interface?
	mbgLtCfgEthernetIf0 NetlinkMode	integer (0..4)	Configuration of the network-speed and duplex settings of the timeservers first network interface 0 = autosensing, 1 = 10 Mbit/s half duplex, 2= 10 Mbit/s full duplex, 3=100 Mbit/s half duplex, 4=100 Mbit/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!

15.2 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. . . ." . These 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 GPS

"Receiver not sync"   GPS receiver not synchronised

"Antenna faulty"   GPS antenna not connected

"Antenna reconnect"   GPS antenna reconnected

"Config changed"   System parameter changed by user

„Leap second announced"   Leap second announced

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

15.2.1 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.

16 Attachment: Technical Information

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

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

ATTENTION!

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

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

16.2 Technical Specifications M600/300 Multipac

HOUSING: Metal desktop case, Schroff 282T
                    Front panel: 1U/84HP (43 mm high / 442 mm wide)

POWER
SUPPLY: 100-240 VAC/VDC

PROTECTION
RATING: IP20

POWER
CONSUMPTION: 28W

PHYSICAL
DIMENSIONS: 442 mm wide x 43 mm high x 288 mm deep
                    (498 mm wide with mounting bracket)

16.3 Safety instructions for building-in equipment

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

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

- The building-in equipment is a class 1 - equipment and must be connected to an earthed outlet (TN Power System).

- The building-in equipment has been evaluated for use in office environment (pollution degree 2) and may be only used in this environment. For use in rooms with a higher pollution degree more stringent requirements are applicable.

- The building-in equipment may not be opened.

- Protection against fire must be assured in the end application.

- The ventilation opening may not be covered.

- The equipment/building-in equipment was evaluated for use in a maximum ambient temperature of 40°C.

- For safe operation the building-in equipment must be protected by max 16 A fuse in the power installation system.

- Disconnection of the equipment from mains is done by pulling the mains plug.

16.4 Rear Panel Connectors

Name	Type	Signal	Cabel
Network	RJ-45	Ethernet	shielded data line
IEEE1588 PTP	RJ-45	Ethernet	shielded data line
PPS	BNC	TTL	shielded coaxial line
10 MHz	BNC	TTL	shielded coaxial line
Error Relais	DFK	Relay, make contact	screwterminal
COM 0	9pin. D-SUB	RS232	shielded data line
COM 1	9pin. D-SUB	RS232	shielded data line
PPS in	BNC	TTL	shielded coaxial line
Freq. in	BNC	TTL	shielded coaxial line
PPM out	BNC	TTL into 50 Ohm	shielded coaxial line
F.Synth. out	BNC	TTL into 50 Ohm	shielded coaxial line
Time Code			
AM in	BNC		shielded coaxial line
DCLS in	BNC		shielded coaxial line
AM out	BNC	3Vpp into 50 Ohm	shielded coaxial line
DCLS out	BNC	2.5Vpp into 50 Ohm	shielded coaxial line
Antenna	BNC		shielded data line
Netz	power cord receptable		power supply cord

16.5 Connector Assignments

```
TxD0 –                     TxD1 –
RxD0 –                     RxD1 –

GND  –                     GND  –

        COM0                       COM1
```
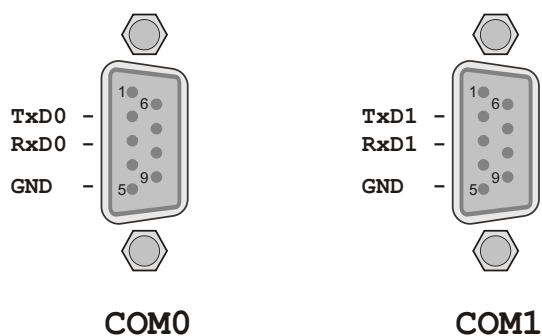
16.6 RS232 TERMINAL

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

```
DSR_IN -          -DCD_IN
RTS_OUT-          -RXD_IN
CTS_IN-           -TXD_OUT
RI_IN-            -DTR_OUT
                  -GND

        TERM
```
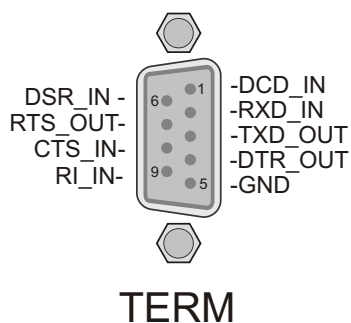
16.7 Error Relay

On the back panel of the device you can find a DFK connector labeled „Error". This relay output is connected to the TTL TIME_SYNC output of the reference clock (GPS, PZF, TCR, ...). If the internal reference clock has been synchronized by its source (GPS, DCF77 or IRIG) the relay will switch to mode „NO" . In case of bad antenna signal or the device has been switched off the relay falls back to mode „NC".

Additionally the relay can be switched by one of the notification conditions. In the notification condition table via WEB or CLI interface you can select the relay out. The priority is on the "TIME SYNC ERROR" signal of the receiver ("refclock not sync"). Relay state which will be set via notification conditions will be reseted by any access via the WEB or CLI interface (if no "TIME SYNC ERROR" is active).

16.7.1 Technical Specification

SWITCHING VOLTAGE max.:		125 VDC
		150 VAC
SWITCHING CURRENT max.:		1A
SWITCHING LOAD max.:	DC	30 W
	AC	60 VA
SWITCHING-CURRENT		
UL/CSA:	0.46A	150V AC
	0.46A	65V DC
	1A	30V DC
RESPONSE TIME:	ca.2ms	

Error

CO NO NC

Normal Operation: CO - NO connected

Error: CO - NC connected

.... Error

.... VCC
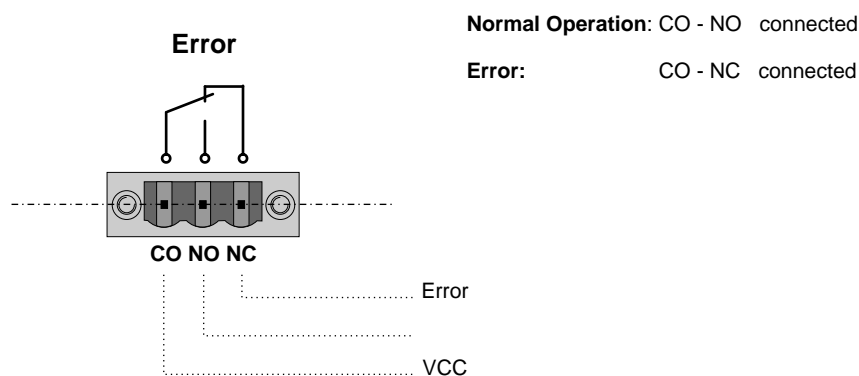
16.8 Technical Specifications GPS receiver

RECEIVER:	6 channel C/A code receiver with external antenna/converter unit
ANTENNA:	Antenna/converter unit with remote power supply refer to chapter "Technical Specifications GPS Antenna"
ANTENNA INPUT:	Antenna circuit dc-insulated; dielectric strength: 1000 V Length of cable: refer to chapter "Mounting the Antenna"
LC DISPLAY:	1HE: 2 x 40 character, menu selectable by push buttons and light BGT: 4 x 16 Zeichen, menu selectable by push buttons
TIME TO SYNCHRONIZATION:	One minute with known receiver position and valid almanac 12 minutes if invalid battery buffered memory
PULSE OUTPUTS:	Change of second (P_SEC, TTL level) Change of minute (P_MIN, TTL level)
ACCURACY OF PULSES:	Better than +-250 nsec after synchronization and 20 minutes of operation Better than +-2 μsec during the first 20 minutes of operation
FREQUENCY OUTPUTS:	10 MHz (TTL level)
SERIAL PORTS:	3 asynchronous serial ports (RS-232)

	COM0:	fixed, internal used
	COM1:	fixed, internal used
	COM2+3:	configurable, sending Standard Meinberg Time String (once per second or per minute)

POWER REQUIREMENTS:	5 V +- 5 %, @ 700 mA
PHYSICAL DIMENSION:	Eurocard, 100 mm x 160 mm
REAR EDGE CONNECTOR:	According to DIN 41612, type C 64, rows a+c (male)
RF CONNECTOR:	Coaxial SMB connector (male)
AMBIENT TEMPERATURE:	0 ... 50 °C
HUMIDITY:	85 % max.

16.8.1 Oscillator specifications

Oscillators available for Meinberg GPS Receivers/Time Servers: OCXO, TCXO, Rubidium

	TCXO	OCXO LQ	OCXO MQ	OCXO HQ	OCXO DHQ	Rubidium (only available for 3U models)
short term stability (= 1 sec)	$2 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$2 \cdot 10^{-10}$	$5 \cdot 10^{-12}$	$2 \cdot 10^{-12}$	$2 \cdot 10^{-11}$
accuracy of PPS (pulse per sec)	< ±250 ns	< ±250 ns	< ±100 ns	< ±100 ns	< ±100 ns	< ±100 ns
phase noise	1Hz -60dBc/Hz 10Hz -90dBc/Hz 100Hz -120dBc/Hz 1kHz -130dBc/Hz	1Hz -60dBc/Hz 10Hz -90dBc/Hz 100Hz -120dBc/Hz 1kHz -130dBc/Hz	1Hz -75dBc/Hz 10Hz -110dBc/Hz 100Hz -130dBc/Hz 1kHz -140dBc/Hz	1Hz < -85dBc/Hz 10Hz < -115dBc/Hz 100Hz < -130dBc/Hz 1kHz < -140dBc/Hz	1Hz < -80dBc/Hz 10Hz < -110dBc/Hz 100Hz < -125dBc/Hz 1kHz < -135dBc/Hz	1Hz -75dBc/Hz 10Hz -89dBc/Hz 100Hz -128dBc/Hz 1kHz -140dBc/Hz
accuracy free run, one day	$\pm 1 \cdot 10^{-7}$ ±1Hz (Note1)	$\pm 2 \cdot 10^{-8}$ ±0.2Hz (Note1)	$\pm 1.5 \cdot 10^{-9}$ ±15mHz (Note1)	$\pm 5 \cdot 10^{-10}$ ±5mHz (Note1)	$\pm 1 \cdot 10^{-10}$ ±1mHz (Note1)	$\pm 2 \cdot 10^{-11}$ ±0.2mHz (Note1)
accuracy, free run, 1 year	$\pm 1 \cdot 10^{-6}$ ±10Hz (Note1)	$\pm 4 \cdot 10^{-7}$ ±4Hz (Note1)	$\pm 1 \cdot 10^{-7}$ ±1Hz (Note1)	$\pm 5 \cdot 10^{-8}$ ±0.5Hz (Note1)	$\pm 1 \cdot 10^{-8}$ ±0.1Hz (Note1)	$\pm 5 \cdot 10^{-10}$ ±5mHz (Note1)
accuracy GPS-synchronous, average 24h	$\pm 1 \cdot 10^{-11}$	$\pm 1 \cdot 10^{-11}$	$\pm 5 \cdot 10^{-12}$	$\pm 1 \cdot 10^{-12}$	$\pm 1 \cdot 10^{-12}$	$\pm 1 \cdot 10^{-12}$
accuracy of time free run, 1 day	± 4.3 ms	± 865 µs	± 65 µs	± 22 µs	± 4.5 µs	± 1.1 µs
accuracy of time free run, 1 year	± 16 s	± 6.3 s	± 1.6 s	± 788 ms	± 158 ms	± 8 ms
temperature dependant drift free run	$\pm 1 \cdot 10^{-6}$ (-20...70°C)	$\pm 2 \cdot 10^{-7}$ (0...60°C)	$\pm 5 \cdot 10^{-8}$ (-20...70°C)	$\pm 1 \cdot 10^{-8}$ (5...70°C)	$\pm 2 \cdot 10^{-10}$ (5...70°C)	$\pm 6 \cdot 10^{-10}$ (-25...70°C)

Note 1: The accuracy in Hertz is based on the standard frequency of 10 MHz.

For example: Accuracy of TCXO (free run one day) is $\pm 1 \cdot 10^{-7} \cdot 10\text{MHz} = \pm 1$ HZ

The given values for the accuracy of frequency and time (not short term accuracy) are only valid for a constant ambient temperature! A minimum time of 24 hours of GPS-syncronicity is required before free run starts.

16.8.2 Technical Specifications GPS Antenna

ANTENNA:	dielectrical patch antenna,	25 x 25 mm
	receive frequency:	1575.42 MHz
BANDWITH:	9 MHz	
CONVERTER:	local oscillator to	
	converter frequency:	10 MHz
	first IF frequency:	35.4 MHz
POWER REQUIREMENTS:	12V ... 18V, @ 100mA (provided via antenna cable)	
CONNECTOR:	N-Type, female	
AMBIENT TEMPERATURE:	-40 ... +65°C	
HOUSING:	ABS plastic case for outdoor installation (IP66)	

Physical Dimension:
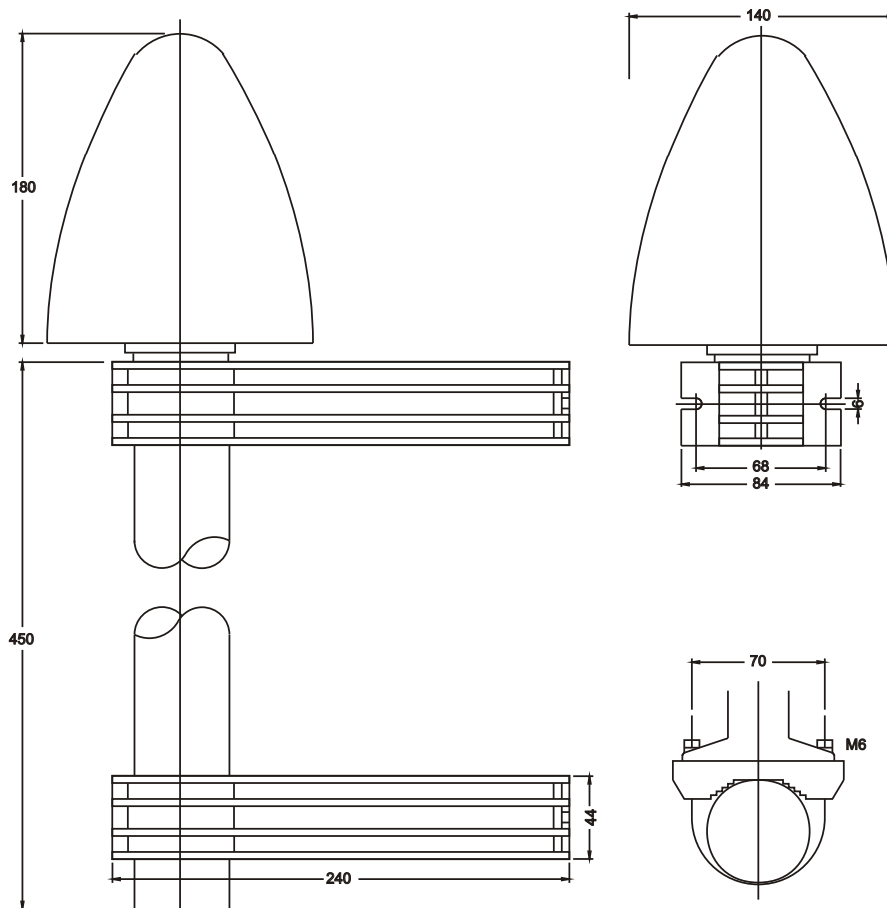
16.8.3 Signal Description GPS170

Name	Pin	Function
GND	32a+c	Ground
VCC in (+5V)	1a+c	+5V supply
VCC in (+12V)	2a+c	+12V supply
VCC in (+5V)	3a+c	+5 V supply (TCXO / OCXO)
P_SEC out	6c	Pulse when second changes, TTL level, active high, length 200 msec
P_MIN out	8c	Pulse when minute changes, TTL level, active high, length 200 msec
/RESET in/out	9c	RESET signal, Open Drain pulled up to +5V
Prog. Pulse out	10c-12c	programmable pulse, TTLlevel
100 kHz out	10a	100 kHz frequency output, TTL level
1 MHz out	11a	1 MHz frequency output, TTL level
10 MHz out	12a	10 MHz frequency output, TTL level
TIME CODE DC	13a	Time code unmod. out
TIME CODE AM	14a	Time code mod. out 3Vpp
DCF_MARK out	17c	DCF77 compatible second marks, TTL level, active high, length 100/200 msec
TIME_SYN	19c	TTL output, HIGH level if synchronization has been achieved, LOW level after reset or in case of serious errors (e.g. antenna faulty)
F_SYNTH	21c	Synthesizer output, TTL-Pegel
F_SYNTH_OD	22c	Synthesizer output, Open Drain, max sink current to GND: 150mA
F_SYNTH_SIN	23c	Synthesizer output, sine-wave 1.5 V eff.
CAPx	27c, 28c	Time capture inputs (TTL), capture on falling slope
COMx TxD out		COMx RS-232 transmit data output
COMx RxD in		COMx RS-232 receive data input
SDA, SCL, SCL_EN (reserved)		internal serial control bus, for extension boards, reserved, do not connect

16.8.4 Rear Connector Pin Assignments GPS170

PIN	a	c
1	VCC in (+5V)	VCC in (+5V)
2	VCC in (+12V)	VCC in (+12V)
3	VDD in (TCXO/OCXO)	VDD in (TCXO/
4	(reserved, FreqAdjust out)	
5		
6		P_SEC out
7		
8	(reserved, 10 MHz in) P_MIN out	
9		/RESET in/out
10	100 kHz out	ProgPulse0 out
11	1 MHz out	ProgPulse1 out
12	10 MHz out	ProgPulse2 out
13		SCL
14		SCL_EN
15	COM2 RxD in	SDA
16	COM2 TxD out	(reserved, P3.2)
17	COM3 RxD in	DCF_MARK out
18	COM3 TxD out	(reserved, Vref/TxD2
19	GND	TIME_SYN out
20	GND	(reserved, P2.3)
21	GND	F_SYNTH out
22	GND	F_SYNTH_OD out
23	GND	F_SYNTH_SIN out
24	GND	COM1 TxD out
25	GND	
26	GND	COM0 TxD out
27	GND	CAP1 in
28	GND	CAP0 in
29	GND	COM1 RxD in
30	GND	COM0 RxD in
31	GND	GND
32	GND	GND

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

16.9 Technical Specifications LAN CPU

PROCESSOR:	Geode^{TM} LX800 with 500 MHz
MAIN MEMORY:	128 MB
CACHE-MEMORY:	16 KB 2nd Level Cache
FLASHDISK:	512 MB
NETWORK CONNECTOR:	10/100 MBIT with RJ45-Jack
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
VGA-CONNECTION:	10-pol pin contact strip
KEYBOARD CONNECTION:	10-pol pin contact strip
STATE LEDs:	- power supply - 'Connect', 'Activity' and 'Speed' of the network connection
POWER REQUIREMENTS:	5 V +- 5 %, @ 1 A
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, USB Port
AMBIENT TEMPERATURE:	0 ... 50 °C
HUMIDITY:	85 % max.

16.9.1 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	
5	/ERR in	/SLIN out	/INIT out
6			
7			
8	/ACK in		
9	/SLCT in		
10	GND	GND	GND
11	GND	GND	GND
12			
13			
14			
15			
16	- USB1 in/out	+ USB1 in/out	
17	+ USB3 in/out		
18	- USB3 in/out		
19			
20	- USB2 in/out	+ USB2 in/out	
21	10MHz in		
22	GND	GND	GND
23	Rx+ in	Tx- out	Tx+ out
24	Rx- in	- USB4 in/out	
25	+ USB4 in/out	LED SPEED 100M out	LED 10M out
26	GND	GND	GND
27	RxD4 in	TxD4 out	DCD4 in
28	RxD3 in	TxD3 out	DCD3 in
29	RxD2 in	TxD2 out	PPS2 in
30	RxD1 in	TxD1 out	DCD1 in
31	GND	GND	GND
32	GND	GND	GND

16.9.2 VGA, Keyboard Connector Pin Assignments
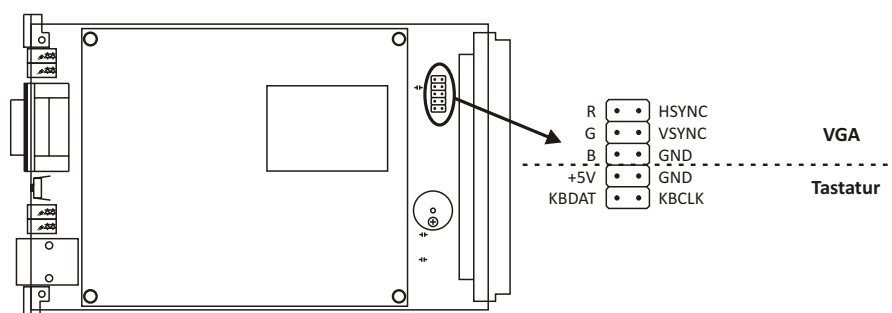
16.10 Technical Specifications Power Supply

INPUT: 85 ... 264 V AC, 47 ... 63 Hz, 1 A/230 V, 2 A/115 V

FUSE: Electronic

16.11 Time Code

16.11.1 Abstract of Time Code

The transmission of coded timing signals began to take on widespread importance in the early 1950´s. Especially the US missile and space programs were the forces behind the development of these time codes, which were used for the correlation of data. The definition of time code formats was completely arbitrary and left to the individual ideas of each design engineer. Hundreds of different time codes were formed, some of which were standardized by the "Inter Range Instrumentation Group" (IRIG) in the early 60´s.

Except these "IRIG Time Codes", other formats like NASA36, XR3 or 2137 are still in use. The board TCR however generates the IRIG-B, AFNOR NFS 87-500 code as well as IEEE1344 code which is an IRIG coded extended by information for time zone, leap second and date. Other formats may be available on request.

16.11.2 Principle of Operation

The Board TCG has been designed for the generation of IRIG, AFNOR and IEEE1344 standard time codes. Apart from the digitally generated amplitude-modulated code, the TCG also provides the unmodulated DC-Level shift code. The modulated sine wave carrier and the board´s internal time pattern are derived from the radio clock´s disciplined oscillator.

16.11.3 Block Diagram Time Code

16.11.4 IRIG Standard Format
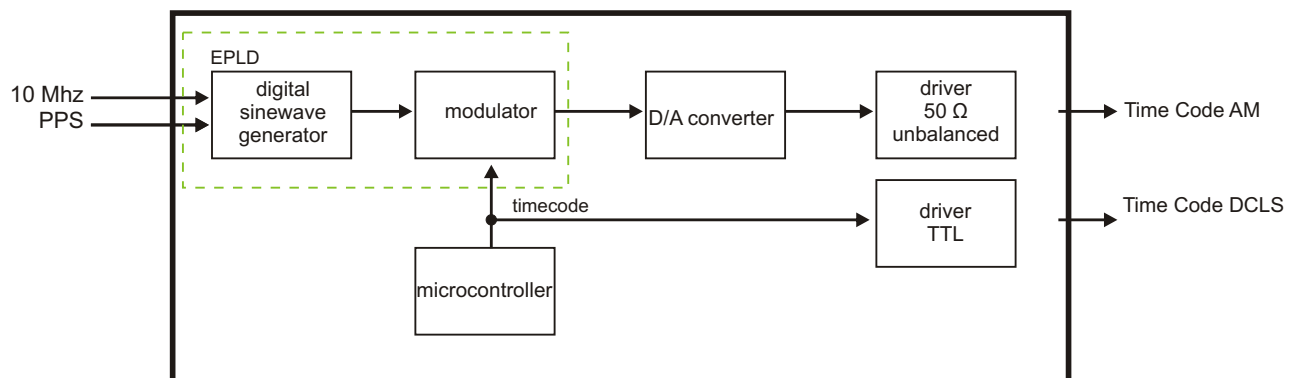
16.11.5 AFNOR Standard Format
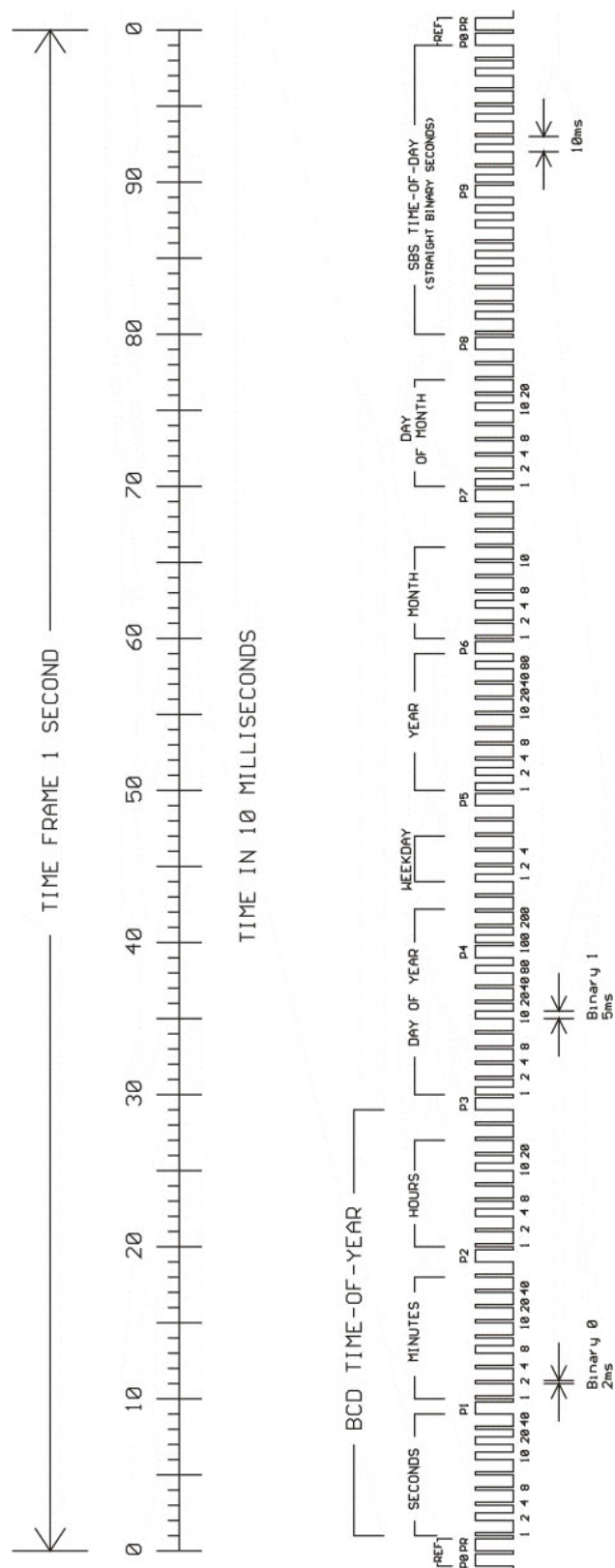
16.11.6 Assignment of CF Segment in IEEE1344 Code

Bit No.	Designation	Description
49	Position Identifier P5	
50	Year BCD encoded 1	
51	Year BCD encoded 2	low nibble of BCD encoded year
52	Year BCD encoded 4	
53	Year BCD encoded 8	
54	empty, always zero	
55	Year BCD encoded 10	
56	Year BCD encoded 20	high nibble of BCD encoded year
57	Year BCD encoded 40	
58	Year BCD encoded 80	
59	Position Identifier P6	
60	LSP - Leap Second Pending	set up to 59s before LS insertion
61	LS - Leap Second	0 = add leap second, 1 = delete leap second 1.)
62	DSP - Daylight Saving Pending	set up to 59s before daylight saving changeover
63	DST - Daylight Saving Time	set during daylight saving time
64	Timezone Offset Sign	sign of TZ offset 0 = '+', 1 = '-'
65	TZ Offset binary encoded 1	
66	TZ Offset binary encoded 2	Offset from IRIG time to UTC time.
67	TZ Offset binary encoded 4	Encoded IRIG time plus TZ Offset equals UTC at all times!
68	TZ Offset binary encoded 8	
69	Position Identifier P7	
70	TZ Offset 0.5 hour	set if additional half hour offset
71	TFOM Time figure of merit	
72	TFOM Time figure of merit	time figure of merit represents approximated clock error. 2.)
73	TFOM Time figure of merit	0x00 = clock locked, 0x0F = clock failed
74	TFOM Time figure of merit	
75	PARITY	parity on all preceding bits incl. IRIG-B time

1.) current firmware does not support leap deletion of leap seconds
2.) TFOM is cleared, when clock is synchronized first after power up. see chapter Selection of generated timecode

16.11.7 Generated Time Codes

Besides the amplitude modulated sine wave signal, the board also provides unmodulated
DC-Level Shift TTL output in parallel. Thus six time codes are available.

a) B002:   100 pps, DCLS signal, no carrier
                             BCD time-of-year

b) B122:   100 pps, AM sine wave signal, 1 kHz carrier frequency
                             BCD time-of-year

c) B003:   100 pps, DCLS signal, no carrier
                             BCD time-of-year, SBS time-of-day

d) B123:   100 pps, AM sine wave signal, 1 kHz carrier frequency
                             BCD time-of-year, SBS time-of-day

e) AFNOR: Code according to NFS-87500, 100 pps, wave signal,
                             1kHz carrier frequency, BCD time-of-year, complete date,
                             SBS time-of-day, Signal level according to NFS-87500

f) IEEE1344:   Code according to IEEE1344-1995, 100 pps, AM sine wave signal,
                             1kHz carrier frequency, BCD time-of-year, SBS time-of-day,
                             IEEE1344 extensions for date, timezone, daylight saving and
                             leap second in control functions (CF) segment.
                             (also see table 'Assignment of CF segment in IEEE1344 mode')

16.11.8 Selection of Generated Time Code

The time code to be generated can be selected by Menu Setup IRIG-settings or the GPS Monitorprogram. DC-Level Shift Codes (PWM-signal) B00x and modulated sine wave carrier B12x are always generated simultaneously. Both signals are provided at the VG64-Connector, i.e. if code B132 is selected also code B002 is available. This applies for the codes AFNOR NFS 87-500 and IEEE1344 as well.

The TFOM field in IEEE1344 code is set dependent on the 'already sync'ed' character ('#') which is sent in the serial time telegram. This character is set, whenever the preconnected clock was not able to synchronize after power up reset. The 'time figure of merit' (TFOM) field is set as follows.

Clock synchronized once after power up: TFOM = 0000
Clock not synchronized after power up: TFOM = 1111

For testing purposes the output of TFOM in IEEE1344 mode can be disabled. The segment is set to all zeros then.

16.11.9 Outputs

The module M600 provides modulated (AM) and unmodulated (DCLS) outputs. The format of the timecodes is illustrated in the diagramms "IRIG-" and "AFNOR standard-format".

AM - Sine Wave Output

The amplitude-modulated carrier is available at the VG-connector pin 14a. The carrier frequency depends on the code and has a value of 1 kHz (IRIG-B). The signal amplitude is 3 Vpp (MARK) and 1 Vpp (SPACE) into 50 Ohm. The encoding is made by the number of MARK-amplitudes during ten carrier waves. The following agreements are valid:

a) binary "0":   2 MARK-amplitudes, 8 SPACE-amplitudes
b) binary "1":   5 MARK-amplitudes, 5 SPACE-amplitudes

c)   position-identifier: 8 MARK-amplitudes, 2 SPACE-amplitudes

DCLS Output

The pulse width DCLS signals shown in the diagramms "IRIG" and "AFNOR standard format" are coexistent to the modulated output and is available at the VG connector pin 13a with TTL level.

16.11.10 Technical Data

OUTPUTS: Unbalanced AM-sine wave-signal:
                  3 VPP (MARK) / 1 VPP (SPACE) into 50 Ohm

                  DCLS signal: TTL, high and low active

16.12 Time Strings

16.12.1 Format of the Meinberg Standard Time String

The Meinberg Standard Time String is a sequence of 32 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. The format is:

<STX>D:*dd.mm.yy;T:w;U:hh.mm.ss;uvxy*<ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<STX>	Start-Of-Text, ASCII Code 02h		
	sending with one bit occuracy at change of second		
dd.mm.yy	the current date:		
	dd	day of month	(01..31)
	mm	month	(01..12)
	yy	year of	
	the century	(00..99)	
w	the day of		
	the week		(1..7, 1 = Monday)
hh.mm.ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)

uv   clock status characters (depending on clock type):

u:	'#'	GPS: clock is running free (without exact synchr.)	
		PZF: time frame not synchronized	
		DCF77: clock has not synchronized after reset	
	' '	(space, 20h)	
		GPS: clock is synchronous (base accuracy is reached)	
		PZF: time frame is synchronized	
		DCF77: clock has synchronized after reset	
v:	'*'	GPS: receiver has not checked its position	
		PZF/DCF77: clock currently runs on XTAL	
	' '	(space, 20h)	
		GPS: receiver has determined its position	
		PZF/DCF77: clock is syncronized with transmitter	

x   time zone indicator:

	'U'	UTC	Universal Time Coordinated, formerly GMT
	' '	MEZ	European Standard Time, daylight saving disabled
	'S'	MESZ	European Summertime, daylight saving enabled

y   anouncement of discontinuity of time, enabled during last hour before discontinuity comes in effect:

	'!'	announcement of start or end of daylight saving time
	'A'	announcement of leap second insertion
	' '	(space, 20h) nothing announced

<ETX> End-Of-Text, ASCII Code 03h

16.12.2 Format of the Meinberg Capture String

The Meinberg Capture String is a sequence of 31 ASCII characters terminated by a CR/LF (Carriage Return/Line Feed) combination. The format is:

CH*x*_ *tt.mm.jj*_ *hh:mm:ss.fffffff* \<CR\>\<LF\>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

x	0 or 1 corresponding on the number of the capture input
_	ASCII space 20h

dd.mm.yy the capture date:

dd	day of month	(01..31)
mm	month	(01..12)
yy	year of the century	(00..99)

hh:mm:ss.fffffff the capture time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)
fffffff	fractions of second, 7 digits	

\<CR\>   Carriage Return, ASCII Code 0Dh

\<LF\>   Line Feed, ASCII Code 0Ah

16.12.3 Format of the SAT Time String

The SAT Time String is a sequence of 29 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. The format is:

<STX>*dd.mm.yy/w/hh:mm:ssxxxxuv*<ETX>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<STX>   Start-Of-Text, ASCII Code 02h
           sending with one bit occuracy at change of second
dd.mm.yy   the current date:
           dd   day of month   (01..31)
           mm   month   (01..12)
           yy   year of the century   (00..99)
           w   the day of the week   (1..7, 1 = Monday)

hh:mm:ss   the current time:
           hh   hours   (00..23)
           mm   minutes   (00..59)
           ss   seconds   (00..59, or 60 while leap second)

xxxx   time zone indicator:
           'UTC'   Universal Time Coordinated, formerly GMT
           'MEZ'   European Standard Time, daylight saving disabled
           'MESZ'   European Summertime, daylight saving enabled

u   clock status characters:
           '#'   clock has not synchronized after reset
           ' '   (space, 20h) clock has synchronized after reset

v   anouncement of discontinuity of time, enabled during last hour
           before discontinuity comes in effect:
           '!'   announcement of start or end of daylight saving time
           ' '   (space, 20h) nothing announced

<CR>   Carriage Return, ASCII Code 0Dh

<LF>   Line Feed, ASCII Code 0Ah

<ETX>   End-Of-Text, ASCII Code 03h

16.12.4 Format of the Uni Erlangen String (NTP)

The time string Uni Erlangen (NTP) of a GPS clock is a sequence of 66 ASCII characters starting with the STX (start-of-text) character and ending with the ETX (end-of-text) character. The format is:

<p align="center">**<STX>*tt.mm.jj; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn lll.lllle hhhhm*<ETX>**</p>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<STX>	Start-Of-Text, ASCII Code 02h sending with one bit occuracy at change of second

dd.mm.yy	the current date:		
	dd	day of month	(01..31)
	mm	month	(01..12)
	yy	year of the century	(00..99)
	w	the day of the week	(1..7, 1 = Monday)

hh.mm.ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)

v	sign of the offset of local timezone related to UTC

oo:oo	offset of local timezone related to UTC in hours and minutes

ac	clock status characters:		
	a:	'#'	clock has not synchronized after reset
	' '	(space, 20h) clock has synchronized after reset	
	c:	'*'	GPS receiver has not checked its position
	' '	(space, 20h) GPS receiver has determined its position	

d	time zone indicator:		
	'S'	MESZ	European Summertime, daylight saving enabled
	' '	MEZ	European Standard Time, daylight saving disabled

f	anouncement of discontinuity of time, enabled during last hour before discontinuity comes in effect:	
	'!'	announcement of start or end of daylight saving time
	' '	(space, 20h) nothing announced

g	anouncement of discontinuity of time, enabled during last hour before discontinuity comes in effect:	
	'A'	announcement of leap second insertion
	' '	(space, 20h) nothing announced

i	leap second insertion	
	'L'	leap second is actually inserted (active only in 60th sec.)
	' '	(space, 20h) no leap second is inserted

bbb.bbbb	latitude of receiver position in degrees leading signs are replaced by a space character (20h)

n	latitude, the following characters are possible:	
	'N'	north of equator

     'S'   south d. equator

lll.llll   longitude of receiver position in degrees
       leading signs are replaced by a space character (20h)

e   longitude, the following characters are possible:
       'E'   east of Greenwich
       'W' west of Greenwich

hhhh   altitude above WGS84 ellipsoid in meters
       leading signs are replaced by a space character (20h)

<ETX>   End-Of-Text, ASCII Code 03h

16.12.5 Format of the NMEA 0183 String (RMC)

The NMEA String is a sequence of 65 ASCII characters starting with the '$GPRMC' character and ending with the characters CR (carriage return) and LF (line-feed). The format is:

$GPRMC,*hhmmss.ss*,A,*bbbb.bb,n,lllll.ll,e*,0.0,0.0,*ddmmyy*,0.0,*a**hh<CR><LF>

The letters printed in italics are replaced by ASCII numbers or letters where as the other characters are part of the time string. The groups of characters as defined below:

$	Start character, ASCII Code 24h	
	sending with one bit occuracy at change of second	

hhmmss.ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)
	ss	fractions	
		of seconds	(1/10 ; 1/100)

A	Status	(A = time data valid)
		(V = time data not valid)

bbbb.bb	latitude of receiver position in degrees
	leading signs are replaced by a space character (20h)

n	latitude, the following characters are possible:	
	'N'	north of equator
	'S'	south d. equator

lllll.ll	longitude of receiver position in degrees
	leading signs are replaced by a space character (20h)

e	longitude, the following characters are possible:	
	'E'	east of Greenwich
	'W'	west of Greenwich

ddmmyy	the current date:		
	dd	day of month	(01..31)
	mm	month	(01..12)
	yy	year of	
		the century	(00..99)

a	magnetic variation

hh	checksum (EXOR over all characters except '$' and '*')

<CR>	Carriage Return, ASCII Code 0Dh

<LF>	Line Feed, ASCII Code 0Ah

16.12.6 Format of the NMEA 0183 String (GGA)

The NMEA (GGA) String is a sequence of characters starting with the '$GPRMC' character and ending with the characters CR (carriage return) and LF (line-feed). The format is:

$GPGGA,*hhmmss.ss,bbbb.bbbbb,n,lllll.ll,e,A,vv,hhh.h,aaa.a,M,ggg.g,M,,0*cs*<CR><LF>

The letters printed in italics are replaced by ASCII numbers or letters where as the other characters are part of the time string. The groups of characters as defined below:

$ Start character, ASCII Code 24h
sending with one bit occuracy at change of second

hhmmss.ss the current time:

hh	hours	(00..23)
mm	minutes	(00..59)
ss	seconds	(00..59, or 60 while leap second)
ss	fractions	
	of seconds	(1/10 ; 1/100)

A Status (A = time data valid)
(V = time data not valid)

bbbb.bbbbb latitude of receiver position in degrees
leading signs are replaced by a space character (20h)

n latitude, the following characters are possible:
'N' north of equator
'S' south d. equator

lllll.lllll longitude of receiver position in degrees
leading signs are replaced by a space character (20h)

e longitude, the following characters are possible:
'E' east of Greenwich
'W' west of Greenwich

A Position fix (1 = yes, 0 = no)

vv Satellites used (0..12)

hhh.h HDOP (Horizontal Dilution of Precision)

aaa.h Mean Sea Level altitude (MSL = altitude of WGS84 - Geoid Separation)

M Units, meters (fixed value)

ggg.g Geoid Separation (altitude of WGS84 - MSL)

M Units, meters (fixed value)

cs checksum (EXOR over all characters except '$' and '*')

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

16.12.7 Format of the ABB SPA Time String

The ABB SPA Time String is a sequence of 32 ASCII characters starting with the characters **">900WD"** and ending with the **<CR>** (Carriage Return) character. The format is:

> **>900WD:***yy-mm-tt*_ *hh.mm;ss.fff:cc***<CR>**

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

yy-mm-tt   the current date:
            yy   year of the century   (00..99)
            mm   month   (01..12)
            dd   day of month   (01..31)

            _   Space (ASCII code 20h)

hh.mm;ss.fff the current time:
            hh   hours   (00..23)
            mm   minutes   (00..59)
            ss   seconds   (00..59, or 60 while leap second)
            fff   milliseconds   (000..999)

cc   Check sum. EXCLUSIVE-OR result of the previous characters,
            displayed as a HEX byte (2 ASCII characters 0..9 or A..F)

<CR>   Carriage Return, ASCII Code 0Dh

16.12.8 Format of the Computime Time String

The Computime time string is a sequence of 24 ASCII characters starting with the T character and ending with the LF (line feed, ASCII Code 0Ah) character. The format is:

T:*yy:mm:dd:ww:hh:mm:ss*<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other
characters are part of the time string. The groups of characters as defined below:

T   Start character
               sending with one bit occuracy at change of second

yy:mm:dd   the current date:
               yy   year of the century   (00..99)
               mm   month   (01..12)
               dd   day of month   (01..31)
               ww   the day of the week   (01..07, 01 = monday)

hh:mm:ss   the current time:
               hh   hours   (00..23)
               mm   minutes   (00..59)
               ss   seconds   (00..59, or 60 while leap second)

<CR>   Carriage Return, ASCII Code 0Dh

<LF>   Line Feed, ASCII Code 0Ah

16.12.9 Format of the RACAL standard Time String

The RACAL standard Time String is a sequence of 16 ASCII characters terminated by a X (58h) character and ending with the CR (Carriage Return, ASCII Code 0Dh) character. The format is:

<div align="center">

<X><G><U>*yymmddhhmmss*<CR>

</div>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<X>	Control character sending with one bit accuracy at change of second	code 58h
<G>	Control character	code 47h
<U>	Control character	code 55h

yymmdd	the current date:		
	yy	year of the century	(00..99)
	mm	month	(01..12)
	dd	day of month	(01..31)

hh:mm:ss	the current time:		
	hh	hours	(00..23)
	mm	minutes	(00..59)
	ss	seconds	(00..59, or 60 while leap second)

<CR>	Carriage Return, ASCII code 0Dh

Interface parameters:	7 Databits, 1 Stopbit, odd. Parity, 9600 Bd

16.12.10 Format of the SYSPLEX-1 Time String

The SYSPLEX1 time string is a sequence of 16 ASCII characters starting with the SOH (Start of Header) ASCII controll character character and ending with the LF (line feed, ASCII Code 0Ah) character. The format is:

<div align="center">

<SOH>ddd:hh:mm:ssq <CR><LF>

</div>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<SOH>   Start of Header (ASCII control character)
              sending with one bit accuracy at change of second

ddd   day of year   (001..366)

hh:mm:ss   the current time:
              hh   hours   (00..23)
              mm   minutes   (00..59)
              ss   seconds   (00..59, or 60 while leap second)
              q   Quality
                      indicator   (space) Time Sync (GPS lock)
                                     (?) no Time Sync (GPS fail)

<CR>   Carriage-return (ASCII code 0Dh)

<LF>   Line-Feed (ASCII code 0Ah)

16.13 Manual VP100/NET 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

16.14 Global Configuration File

This file contains all global parameters 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:          4.17
Configuration File Last Change:

# Network Parameter Section
Hostname                              [ASCII,50]   :   LanGpsV4
Domainname                            [ASCII,50]   :   py.meinberg.de
Default IPv4 Gateway                  [IP]         :
Default IPv6 Gateway                  [IP]         :
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]       :
NTP Trust Time                        [NUM]        :   0

# 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 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]    :
```

16.15 Global Option File

This file contains 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            : server
SYSTEM DESIGN               : 0
```

16.16 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 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 e-mail 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.

16.16.1 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 information about GNU/Linux can be found on the GNU website
www.gnu.org

and on the website of GNU/Linux
www.linux.org

16.16.2 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

16.16.3 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 information 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.                                                              *
*                                                                        *
**************************************************************************
```

16.16.4 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 as long as 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 MER-CHANTABILITY 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 INTERRUP-TION) 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

16.16.5 GNU General Public License (GPL)

Version 2, June 1991 - Copyright (C) 1989, 1991
Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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 de- rived 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 ex- ecutable 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 cor- responding 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

16.17 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

Konformitätserklärung

Declaration of Conformity

Hersteller Manufacturer	**Meinberg Funkuhren GmbH & Co. KG** **Lange Wand 9** **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 M600/MRS**

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

EN55022:1998, Class B (+A1:2000 +A2:2003)	Grenzwerte und Meßverfahren für Funkstörungen von informationstechnischen Einrichtungen Limits and methods of measurement of radio interference characteristics of information technology equipment
EN55024:1998 (+A1:2001 +A2:2003)	Grenzwerte und Meßverfahren für Störfestigkeit von informationstechnischen Einrichtungen Limits and methods of measurement of Immunity characteristics of information technology equipment
EN 60950-1:2001 (+A11:2004)	Sicherheit von Einrichtungen der Informationstechnik Safety of information technology equipment

gemäß den Richtlinien 2004/108/EG (Elektromagnetische Verträglichkeit), 2006/95/EG (Nieder-spannungsrichtlinie) und 93/68/EWG (CE Kennzeichnung) sowie deren Ergänzungen.
following the provisions of the directives 2004/108/EC (electromagnetic compatibility), 2006/95/EC (low voltage directive) and 93/68/EEC (CE marking) and its amendments.

Bad Pyrmont, den 03.07.2009

Günter Meinberg
Managing Director