

Technische Daten

Inbetriebnahme

**LANTIME / RDT**

ETX 1HE

## **Impressum**

Meinberg Funkuhren GmbH & Co. KG  
Auf der Landwehr 22  
D-31812 Bad Pyrmont

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

Internet: <http://www.meinberg.de>  
E-Mail: [info@meinberg.de](mailto:info@meinberg.de)

Bad Pyrmont, den 8. August 2006

# Inhaltsverzeichnis

|   |    |
|---|----|
| Kurzanleitung zur Erstinbetriebnahme.....                     | 7  |
| Netzwerk Zeitserver extern synchronisierter Zeitreferenz..... | 8  |
| Komplettsystem LANTIME.....                                   | 9  |
| Unterstützte Netzwerk Dienste.....                            | 10 |
| Zusatzfunktionen und Optionen.....                            | 11 |
| Benutzerinterface.....  | 11 |
| Optionen.....   | 11 |
| Gründe für einen Network Timeserver.....                      | 12 |
| Network Time Protocol (NTP).....                              | 13 |
| NTP Client Zielsysteme.....                                   | 14 |
| NTP-Client Installation.....                                  | 14 |
| Anschluss der Referenzuhren.....                              | 17 |
| Bootphase des Linux Rechners.....                             | 18 |
| Benutzerschnittstellen zur Konfiguration.....                 | 19 |
| Bedienelemente der Frontplatte.....                           | 20 |
| LC Display.....   | 20 |
| Taste MENU.....   | 20 |
| Taste CLR/ACK.....  | 20 |
| Taste NEXT.....   | 20 |
| Taste INC.....  | 20 |
| Konfiguration über LC-Display.....                            | 21 |
| Das LCD Menü im Einzelnen.....                                | 22 |
| Hauptmenü.....  | 22 |
| DCT Statusmenü.....   | 22 |
| Menü Referenzuhr Status.....                                  | 23 |
| Menü SETUP.....   | 23 |
| SETUP LAN PARAMETERS.....                                     | 24 |
| Die grafischen Konfigurations-Schnittstellen.....             | 25 |
| Das HTTP Interface.....                                       | 26 |
| Konfiguration: Hauptmenü.....                                 | 27 |
| Konfiguration: Ethernet.....                                  | 28 |

|  |    |
|--|----|
| SYSLOG Server.....                       | 29 |
| Netzwerkdienste.....                     | 30 |
| DHCP IPv4.....                           | 30 |
| IPv6 Adressen und Autoconf.....          | 31 |
| High availability bonding.....           | 31 |
| Zusätzliche Netzwerkkonfiguration.....   | 32 |
| Konfiguration: Notification.....         | 33 |
| Alarm Ereignisse.....                    | 34 |
| Alarm EMAIL.....                         | 34 |
| Windows Popup Message.....               | 35 |
| Alarm SNMP-TRAP.....                     | 35 |
| VP100/NET Display.....                   | 35 |
| Benutzerdefinierte Benachrichtigung..... | 35 |
| Alarm Texte.....                         | 36 |
| Konfiguration: Sicherheit.....           | 37 |
| Passwort.....                            | 38 |
| HTTP Zugangsberechtigung.....            | 38 |
| SSH Secure Shell Login.....              | 39 |
| SSL Zertifikat für HTTPS erstellen.....  | 40 |
| NTP Schlüssel und Zertifikate.....       | 41 |
| SNMP Parameter.....                      | 41 |
| Konfiguration: NTP.....                  | 42 |
| NTP Authentication.....                  | 46 |
| NTP Autokey.....                         | 48 |
| Konfiguration: Lokal.....                | 51 |
| Administrative Funktionen.....           | 52 |
| Benutzerverwaltung.....                  | 53 |
| Administrative Informationen.....        | 53 |
| Software Update.....                     | 55 |
| Automatische Konfigurationsprüfung.....  | 56 |
| Diagnose Informationen speichern.....    | 57 |
| Sprache des WEB-Interface.....           | 57 |
| Konfiguration: Statistik.....            | 58 |
| Statistik Informationen.....             | 59 |
| Konfiguration: Handbuch.....             | 61 |
| Das Kommandozeilen Interface.....        | 62 |
| CLI Ethernet.....                        | 63 |
| CLI Notification.....                    | 66 |
| CLI Security.....                        | 69 |
| CLI NTP Parameter.....                   | 71 |
| NTP Authentication.....                  | 73 |

|  |     |
|--|-----|
| CLI Local.....   | 75  |
| SNMP Server.....   | 78  |
| Konfiguration über SNMP.....                                   | 80  |
| Beispiele SNMP Konfiguration.....                              | 81  |
| Weitere Konfigurationsmöglichkeiten.....                       | 82  |
| Senden von Befehlen an den Zeitserver per SNMP.....            | 82  |
| Konfiguration des Zeitservers via SNMP: Referenz.....          | 84  |
| SNMP Traps.....  | 88  |
| SNMP TRAP Referenz.....  | 89  |
| Anhang: Technische Daten.....                                  | 90  |
| Nur Service-/Fachpersonal: Austausch der Lithium-Batterie..... | 90  |
| Technische Daten Lantime Multipack.....                        | 90  |
| Sicherheitshinweise für Geräte.....                            | 91  |
| CE-Kennzeichnung.....  | 91  |
| Rückwandanschlüsse.....  | 92  |
| Rückansicht LANTIME.....                                       | 93  |
| SUB-D Steckerbelegung.....                                     | 94  |
| Technische Daten LAN CPU.....                                  | 95  |
| Steckerbelegung.....   | 96  |
| Belegung der Stiftleiste (VGA, Tastatur).....                  | 96  |
| Zeitlegramme.....  | 97  |
| Format des Meinberg Standard-Zeitlegramms.....                 | 97  |
| Format des GPS167 Capture-Telegramms.....                      | 98  |
| Format des SAT-Zeitlegramms.....                               | 99  |
| Format des Telegramms Uni Erlangen (NTP).....                  | 100 |
| Format des NMEA Telegramms (RMC).....                          | 102 |
| Format des ABB-SPA-Zeitlegramms.....                           | 103 |
| Format des Computime-Zeitlegramms.....                         | 104 |
| Kurzübersicht LANTIME Bedienung.....                           | 105 |
| Konformitätserklärung.....                                     | 106 |
| Manuelle Displayansteuerung VP100/NET.....                     | 107 |
| Konfigurationsdatei.....                                       | 109 |
| Globale Optionen Datei.....                                    | 110 |
| Eingesetzte Software von Drittherstellern.....                 | 111 |
| Betriebssystem GNU/Linux.....                                  | 111 |

|   |     |
|---|-----|
| Samba.....  | 111 |
| Network Time Protocol Version 4 (NTP).....        | 112 |
| mini_httpd.....                                   | 112 |
| GNU General Public License (GPL).....             | 113 |
| Timecode (optional).....                          | 117 |
| Allgemeines.....                                  | 117 |
| Funktionsweise.....                               | 117 |
| Blockschaltbild Generierung des Timecodes.....    | 117 |
| IRIG - Standardformat.....                        | 118 |
| AFNOR - Standardformat.....                       | 119 |
| Belegung des CF Segmentes beim IEEE1344 Code..... | 120 |
| Generierte Zeitcodes.....                         | 121 |
| Auswahl des generierten Zeitcodes.....            | 121 |
| Ausgänge.....                                     | 122 |
| AM - Ausgang.....                                 | 122 |
| PWM - Ausgänge.....                               | 122 |
| Technische Daten.....                             | 122 |
| USB Stick (optional).....                         | 123 |
| Menü Verzeichnisstruktur.....                     | 123 |
| Menü Konfigurationsdateien.....                   | 124 |
| Menü Script Dateien.....                          | 125 |
| Tastatursperre.....                               | 125 |
| Literaturverzeichnis.....                         | 126 |

## Kurzanleitung zur Erstinbetriebnahme

- Nach dem Einschalten des Gerätes muss nach ca. einer halben Minute die Anzeige in der zweiten Zeile von "NTP: not ready" zu "NTP: not sync" wechseln.

|                  |                 |
|------------------|-----------------|
| SERVER NOT READY | Wed, 18.11.1998 |
| NTP: Not Ready   | UTC 10:03:30    |

 ==> 

|                  |                 |
|------------------|-----------------|
| NORMAL OPERATION | Wed, 18.11.1998 |
| NTP: not sync    | UTC 10:04:10    |

- Eingeben der TCP/IP Adresse, Netzmaske und Default Gateway:
  - Drücken Sie 4 mal die MENU Taste um in das Setup Menü für die Lan-Parameter zu gelangen
  - mit der CLR/ACK Taste wird als erstes die aktuelle TCP/IP Adresse angezeigt

|                 |                  |
|-----------------|------------------|
| SETUP:          | LAN PARAMETERS   |
| TCP/IP ADDRESS: | DHCP 172.16.3.40 |

- nochmaliges Drücken der CLR/ACK Taste ermöglicht das Eingeben der IPv4 Netzwerkadresse
- mit der NEXT Taste kann die Ziffer ausgewählt und mit der INC Taste eingestellt werden
- um den eingegeben Wert zu übernehmen, muss wieder die CLR/ACK Taste gedrückt werden
- rechts oben im Display erscheint ein '\*', welches anzeigt, dass eine Änderung vorgenommen wurde
- mit der NEXT Taste kann dann die Netzmaske, der Default Gateway und der externe NTP Server auf die gleiche Weise eingestellt werden.
- Durch Drücken der MENU Taste und Bestätigung mit der INC Taste werden die Änderungen aller eingestellten Netzwerkparameter durchgeführt.

|                |            |
|----------------|------------|
| Are you sure ? | Press ...  |
| INC -> YES     | MENU -> NO |

- Wenn der NDT nicht synchronisiert hat (FAIL LED leuchtet nach 12 Minuten immer noch), prüfen Sie die Einstellungen des externen NTP Servers durch einmaliges Drücken der MENU Taste, dann CLR/ACK und dann drei mal die NEXT Taste:

|             |                |
|-------------|----------------|
| SETUP:      | LAN PARAMETERS |
| NTP SERVER: | 172.16.3.40    |

**WICHTIG:** Die maximale Zeit-Differenz zwischen dem NDT und dem externen NTP Server darf nicht größer als 3600s sein. Ist dies der Fall, muss die Zeit manuell gesetzt werden.

Danach können alle weiteren Einstellungen über das Netzwerkinterface, entweder über einen WEB Browser oder eine Telnet Session, konfiguriert werden.

Default Benutzer: **root**

Default Passwort: **timeserver**

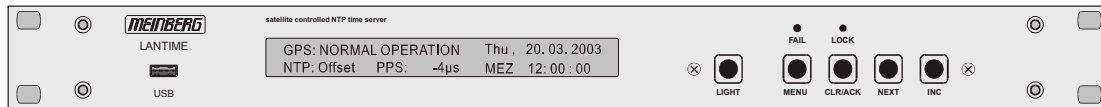
## **Netzwerk Zeitserver extern synchronisierter Zeitreferenz**

LANTIME steht für Local Area Network Timeserver. Das LANTIME stellt eine absolute und hochgenaue Zeitreferenz in einem TCP/IP Netzwerk zur Verfügung (Stratum-1-Server). Die Zeit wird mittels des NTP Protokolls (Network Time Protocol) allen NTP Clients zur Verfügung gestellt. Es soll ein möglichst einfaches Integrieren einer absoluten Zeitreferenz in ein bestehendes Netzwerk ermöglichen. Die einzelnen LANTIME-Varianten unterscheiden sich im Wesentlichen durch die verwendete Referenzzeit: Als Referenzzeitquelle kann eine externe Funkuhr, ein eingebauter DCF77-, GPS-, IRIG-Empfänger oder externer NTP-Server oder auch eine DCF77/GPS-Kombination als Hybridempfänger eingesetzt werden. Das LANTIME/RDT (Remote Disciplined Timeserver) besteht aus einem Einplatinenrechner mit integrierter Netzwerkkarte und einem Netzteil. Diese Bestandteile sind in einem 19 Zoll Gehäuse mit 1 HE integriert. Als Betriebssystem ist ein vereinfachtes LINUX auf dem Einplatinen Rechner implementiert, welches in der Boot-Phase aus einer Flash-Disk geladen wird. Alle Einstellungen können über vier Taster und das 2-zeilige LC - Display vorgenommen werden. Ebenso besteht die Möglichkeit einer Fernkonfiguration über das Netzwerk mittels FTP oder TELNET. Ein integrierter HTML Server ermöglicht den Zugriff auf das LANTIME mit einem beliebigen WEB Browser.



## Komplettsystem LANTIME

Das System LANTIME besteht aus einem Einplatinen Computer ETX-MGX 266MHz mit integrierter Netzwerkkarte und einem Netzteil betriebsbereit in einem Baugruppenträger montiert. Die Ein-/Ausgangssignale der Baugruppe LANTIME sind an der Front- und Rückwand des Systems über Steckverbinder herausgeführt. Die einzelnen Baugruppen werden nachfolgend beschrieben.



Frontansicht LAN TIME RDT

Auf dem LINUX Rechner ist ein NTPD implementiert, welcher zyklisch die Referenzzeit entweder von einem seriellen Telegramm einliest oder einem externen NTP Server über das Netzwerk abholt. Der Status des NTPD wird auf dem Display angezeigt und kann über das Netzwerk abgefragt werden.

Die Installation des LANTIME ist für den System- oder Netzwerkadministrator denkbar einfach. Es müssen die Netzwerkadresse, die Netzmaske und das Default Gateway über das Frontpanel eingestellt werden. Allen NTP Clients im TCP/IP Netzwerk werden dann nur noch die Netzwerkadresse oder der entsprechende Name des LANTIME bekannt gegeben.

Das Linux System unterstützt neben NTP auch weitere Netzwerkprotokolle wie HTTP(S), FTP, SSH und Telnet. Dadurch besteht die Möglichkeit einer Fernkonfiguration bzw. Statusabfrage über das Netzwerk, z.B. mit einem beliebigen WEB Browser. Der Zugang über das Netzwerk kann wahlweise auch deaktiviert werden. Statusänderungen der Funkuhren, Fehler und andere wichtige Ereignisse werden entweder auf dem lokalen Linux System oder auf einem externen SYSLOG Server protokolliert. Zusätzlich können Meldungen über SNMP Traps oder automatisch generierte E-Mails an einer zentralen Verwaltungsstelle gemeldet und dort mitprotokolliert werden. Außerdem besteht die Möglichkeit, alle Alarmnachrichten auf einem Großdisplay VP100/NET anzeigen zu lassen. Wenn eine Redundanz für den Fall eines Ausfalls der Hardware benötigt wird, können mehrere LANTIME NTP Server im gleichen Netzwerk installiert werden.

## **Unterstützte Netzwerk Dienste**

Die folgenden Netzwerkdienste werden über RJ45 10/100Base-T Ethernet (Autosensing) zur Verfügung gestellt:

- NTP v2, v3, v4
  - NTP broadcast mode
  - NTP multicast
  - NTP symmetric keys
  - NTP Autokey
- Simple Network Time Protocol (SNTP)
- TIME
- SNMP v1,2,3 mit erweitertem SNMP-Agent und SNMP-TRAPs für den NTP- und Referenzuhrstatus
- DHCP Client
- NFS
- TELNET
- FTP
- HTTP
- HTTPS mit Openssl2
- SSH2 Secure Shell Login
- Alarmmeldungen per E-Mail
- IPv6
  - 3 globale IPv6 Adressen einstellbar
  - Autoconf Feature abschaltbar
  - unterstützte Netzwerkdienste: NTP, HTTP, HTTPS, SNMP, SSH
- Windows „net time“ über NETBIOS
- Winpopup (Window Mail)

## **Zusatzfunktionen und Optionen**

- Externer NTP Zeitserver
- Freie Konfiguration des NTP: Dadurch MD5-Authentikation und Zugriffskontrolle über Address & Mask Restriction
- Erweiterte Menüführung für Konfiguration und Monitoring über Telnet, SSH oder serielle Terminal-Schnittstelle
- Optional bis zu 3 RJ45/10/100 MBit Ethernet Schnittstellen - erweiterter HTTP Statistik Support mit Langzeit-Grafik und Zugriffsstatistik auf NTP
- Alarmmeldungen auch über externes Großdisplay VP100/20/NET mit Laufschrift
- USB Memory Stick Slot für erweiterte Funktionalität: Softwareupdate, Übertragungen von Sicherheits-Zertifikaten, Log-Dateien und Konfigurationen, Tastatursperre

## **Benutzerinterface**

- Terminal Anschluss über serielle Schnittstelle, LED Status Anzeige
- Web-Browser Interface mit grafischer Statistik der Offset-Werte über einen Tag oder eine Periode
- Telnet oder Secure Shell Login zur vollen Passwort-geschützten Bedienung des Linux Betriebssystems
- FTP Zugang für Update der Betriebssoftware und zum Downloaden von Logg-Dateien
- Simple Network Management Protokoll zur automatischen Versendung von SNMP Traps im Alarmfall
- SYSLOG Meldungen können auf einen anderen Rechner umgeleitet werden
- E-Mail-Benachrichtigung bei konfigurierbaren Ereignissen
- Simulation einer synchronen Funkuhr einstellbar, damit auch ohne Antenne einsetzbar

## **Optionen**

- Bis zu zwei weitere Ethernet RJ45 Anschlüsse (bis zu acht weitere im 3HE Gehäuse)
- Frequenz-/Pulsausgänge über BNC Buchsen (z.B. 10 MHz, 2.048 MHz, PPS)
- Höhere Freilaufgenauigkeit durch bessere Oszillatoren (OCXO)
- IRIG B Ausgänge
- ANZ14LAN oder VP100/20NET als Nebenuhr über Netzwerk anzuschließen

## Gründe für einen Network Timeserver

Wenn die genaue Zeit im eigenen Netzwerk eine wesentliche Rolle für einen reibungslosen Betrieb spielt, sollte ein eigener Timeserver eingesetzt werden. Prinzipiell kann man natürlich seine Rechner im Netzwerk mit Timeservern im Internet synchronisieren. Aus den folgenden Sicherheitsaspekten und/oder Wartbarkeit sollte auf einen eigenen Timeserver im eigenen Netzwerk Wert gelegt werden:

- Bei dem LANTIME besteht die Möglichkeit der Benachrichtigung eines Verantwortlichen per E-Mail oder SNMP-Trap, falls eine Störung auftritt.
- Die Rechner im eigenen Netzwerk sind nicht auf eine funktionierende Internetverbindung angewiesen.
- Die Rechner im eigenen Netzwerk sind nicht auf die Verfügbarkeit des externen Timeservers angewiesen. Selbst die PTB (Physikalisch technisches Bundesamt) stellt auf der von ihnen angegebenen Webseite klar, dass eine dauernde Verfügbarkeit mindestens eines der PTB-Timeserver zwar angestrebt wird, aber nicht garantiert werden kann.
- Bei einem Test von anderen frei verfügbaren Timeservern (nicht PTB!) wurde festgestellt, dass viele eine signifikant falsche Zeit verteilen, obwohl sie sich als Stratum-1-Server ausgaben. Hier liegt das Problem normalerweise bei den zuständigen Administratoren.
- Bei einer "normal" funktionierenden Internet-Verbindung kann NTP die Laufzeit der Netzwerk-Pakete recht gut ermitteln und kompensieren. Wenn allerdings durch unvorhersehbare Vorgänge die Internet-Übertragung bis zur Kapazitätsgrenze ausgereizt wird, kann durch stark schwankende Paket-Laufzeiten die Zeitsynchronisierung signifikant gestört werden. Als Grund sind z.B. großflächige Hacker-Aktivitäten denkbar (die nicht mal das eigene Netzwerk betreffen müssen), oder neue Viren, die sich durch eine Flut von E-Mails verbreiten, wie es in der Vergangenheit bereits vorgekommen ist.
- Ein eigener Timeserver kann nicht so leicht aus dem Internet heraus kompromittiert werden. Dazu als Beispiel ein Fall, der in der NTP-Community einiges Aufsehen erregt hat: Ein Hersteller von Low-Cost-Routern hatte in seinen Produkten die IP-Adresse eines öffentlich zugänglichen NTP-Servers fest codiert, damit diese sich die Zeit holen könnten. Dabei war die Implementierung sogar noch fehlerhaft. Als Folge wurde der NTP-Server mit riesigen Mengen von Anfragen bombardiert, durch die nicht nur die Funktion des NTP-Servers selbst gestört wurde, sondern wodurch auch riesige Mengen von Netzwerk-Verkehr und damit hohe Kosten für den Betreiber des NTP-Servers erzeugt wurden. In diesem Fall half nicht mal das Abschalten des NTP-Servers, da ja auch weiterhin Anfragen gesendet wurden.

Das U.S. Naval Observatory (USNO) hat in den USA eine ähnliche Funktion zur Bereitstellung der gesetzlichen Zeit wie in Deutschland die PTB, und stellt ebenfalls

seit langem öffentliche NTP-Timeserver zur Verfügung. Diese haben immer mehr mit "bösen" Clients zu kämpfen, durch die die Verfügbarkeit des Dienstes in Frage gestellt wird. Es wurden bereits besondere Vorkehrungen getroffen, um die Gefahr einzudämmen. Dave Mills, der "Erfinder" von NTP, arbeitet mit der USNO zusammen und hat in der NTP-Newsgruppe auf diese Tatsache hingewiesen.

## **Network Time Protocol (NTP)**

NTP ist ein allgemeines Verfahren zur Synchronisation von Rechneruhren in lokalen und globalen Netzwerken. Das Grundprinzip, Version 1 [Mills88], wurde bereits 1988 als RFC (Request For Comments) veröffentlicht. Erfahrungen aus der praktischen Anwendung im Internet wurden in Version 2 [Mills89] eingebracht. Das Programmpaket NTP ist eine Implementierung der aktuellen Version 4 [Mills90], basierend auf der Spezifikation RFC-1305 von 1990 (im Verzeichnis doc/NOTES). Das Paket ist frei kopierbar und unterliegt den Copyright Bedingungen.

Die Arbeitsweise von NTP unterscheidet sich grundsätzlich von den meisten anderen Protokollen. NTP synchronisiert nicht einfach alle beliebigen Uhren untereinander, sondern bildet eine Hierarchie von Zeitservern und Clients. Eine Hierarchieebene wird als *stratum* bezeichnet, wobei Stratum-1 die höchste Ebene darstellt (das LANTIME ist ein Stratum-1-Server). Zeitserver dieser Ebene synchronisieren sich auf eine Referenzzeitquelle, das können z. B. Funkuhren, GPS-Empfänger oder Modem-Zeitdienste sein. Stratum-1-Server stellen ihre Zeit mehreren Clients im Netz zur Verfügung, die als Stratum-2 bezeichnet werden.

Ausgehend von einer oder mehreren Referenzzeiten kann durch NTP eine hohe Synchronisationsgenauigkeit realisiert werden. Jeder Rechner synchronisiert sich mit bis zu 3 gewichteten Zeitquellen, wobei ausgefeilte Mechanismen den Abgleich der Systemzeit mit anderen Rechnern im Netz sowie ein Nachregeln der eigenen Systemuhr ermöglichen. Abhängig von der Jitter-Charakteristik der Zeitquellen und der Lokalisierung des einzelnen Rechners im Netzwerk wird eine Zeitgenauigkeit von 128 ms, häufig besser als 50 ms, erreicht.

## **NTP Client Zielsysteme**

Das Programmpaket NTP wurde auf verschiedenen UNIX Systemen getestet (siehe Liste). Bei vielen UNIX Installationen ist bereits ein NTP Client vorinstalliert. Es müssen nur die Konfigurationsdateien (/etc/ntp.conf - siehe NTP Client Installation) angepasst werden. Auch für die meisten anderen Betriebssysteme wie Windows NT/2000/XP/95/98/3x, OS2 oder MAC existieren NTP Clients als Freeware oder Shareware. Als Bezugsquelle für die neuesten Versionen wird die NTP Homepage empfohlen: "<http://www.eecis.udel.edu/~ntp/>" oder "<http://www.ntp.org>". Auf unserer Homepage können aktuelle Informationen zur Installation und Funktion von NTP gefunden werden: "<http://www.meinberg.de/german/sw/ntp.htm>".

## **NTP-Client Installation**

Im Folgenden wird die Installation und Konfiguration eines NTP Clients unter einem UNIX Betriebssystem gezeigt. Prüfen Sie als erstes, ob nicht die NTP Software schon auf Ihrem System vorhanden ist, denn bei vielen UNIX Systemen ist NTP Bestandteil des Auslieferungszustandes.

Der NTP Daemon wird als Source geliefert und muss auf dem Zielsystem übersetzt werden. Über das mitgelieferte Scriptfile wird automatisch eine Konfiguration zum Übersetzen des NTP Daemons und allen Tools erzeugt.

### **configure**

Es werden nun alle notwendigen Informationen aus Ihrem System gesammelt und daraus die entsprechenden Make-Dateien in den einzelnen Unterverzeichnissen erzeugt.

Anschließend wird der NTP-Daemon und alle notwendigen Utilitys erzeugt. Rufen Sie hierzu "make" auf:

### **make**

Beim Übersetzen des NTP-Daemons können diverse Warnungen ausgegeben werden, die aber meist ohne Bedeutung sind. Sollten Sie Probleme mit der Übersetzung haben, beachten Sie die systemabhängigen Hinweise in den Unterverzeichnissen 'html'.

Anschließend müssen noch die Programme und Tools in die entsprechenden Verzeichnisse kopiert werden. Dies geschieht mit dem Befehl:

### **make install**

Der Zeitabgleich des Client-Systems kann nun auf unterschiedliche Art und Weise erfolgen. Entweder kann die Systemzeit mit dem NTP Tool "ntptime" einmalig oder mittels CRON gesetzt werden (dies wird empfohlen direkt einmal automatisch nach dem Booten des Rechners) oder es wird der NTPD Daemon gestartet. Das Letztere wird im Folgenden beschrieben.

Als nächstes muss die Datei /etc/ntp.conf mit einem Editor angelegt werden. Die Datei sollte für das Meinberg LANTIME folgendes Aussehen haben:

```

# Beispiel für /etc/ntp.conf für Meinberg LANTIME
server 127.127.1.0      # local clock
server 172.16.3.35    # TCPIP Adresse des LANTIME
# Optional: Driftfile
# driftfile /etc/ntp.drift
# Optional: alle Meldungen im Syslogfile aktivieren
# logconfig=all

```

Der NTP Daemon wird mit dem Befehl 'ntpd' gestartet. Dieses kann auch aus 'rc.local' beim Systemstart geschehen. Statusmeldungen während des Betriebes können aus den Dateien /var/log/messages (entsprechend der syslog-Einstellungen) entnommen werden.

**z.B.: tail /var/log/messages**  
zeigt die letzten Zeilen aus der Datei "messages" an.

Die Statusmeldungen können auch mit der folgenden Option in eine Loggdatei umgeleitet werden (siehe Beispiel im Anhang):

**ntpd -llogfile**

Mit dem Befehl 'ntpq' aus dem Verzeichnis 'ntpq' kann der aktuelle Status des NTP Daemon abgefragt werden (siehe auch doc/ntpq.8).

**z.B.: ntpq/ntpq**

Es erscheint ein Komandointerpreter; mit "?" wird die Liste der möglichen Befehle angezeigt werden. Hier werden nur die wichtigsten Befehle kurz skizziert:

Mit dem Befehl "peer" werden in einer Tabelle die aktiven Referenzuhren zeilenweise angezeigt:

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

Folgende Informationen werden angezeigt:

---

- remote: Auflistung aller verfügbaren Zeit-Server (ntp.conf)
- refid: Referenznummer
- st: aktueller Stratum-Wert (Hierarchieebene)
- when: wann die letzte Abfrage stattgefunden hat (in Sekunden)
- poll: in welchem Intervall der Zeitserver abgefragt wird
- reach: oktale Darstellung eines 8 Bit Speichers, in welchem die erfolgreichen Abfragen von rechts nach links geshiftet werden.
- delay: gemessene Verzögerung der Netzwerkübertragung (in Millisekunden)
- offset: Differenz zwischen Systemzeit und Referenzzeit (in Millisekunden)
- jitter: statistische Streuung des Offsets (in Millisekunden)

Durch mehrmaligen Aufruf dieses Befehls "peer" kann man verfolgen, wie sich der NTP Daemon langsam einschwingt. Alle 64 Sekunden (poll - Wert) wird ein neues Zeitlegramm von der Funkuhr eingelesen und ausgewertet. Der NTP Daemon benötigt ca. 3 bis 5 Minuten für die Initialisierungsphase. Dies wird mit einem Stern (\*) links neben dem Remote-Namen angezeigt.

Weicht die Rechnerzeit mehr als 1024 Sekunden von der UTC Zeit ab, beendet der NTP Daemon sich selbst; dies ist meist der Fall, wenn die aktuell eingestellte Uhrzeit nicht mit der Zeitzone übereinstimmt (siehe UNIX-Systemhandbuch Einstellen der Zeitzone unter "zic" oder "man zic").



## Anschluss der Referenzuhren

An der Rückseite des Gerätes stehen zwei 9 polige SUBD Buchsen für die seriellen Eingänge der Referenzuhren und zum Anschluss eines PPS (Puls Per Second) Impulses zur Verfügung. Die seriellen Schnittstellen müssen über RxD (Pin 2) und Ground (Pin 5) an die SUBD Buchsen angeschlossen werden. Für den PPS Eingang muss ein RS232 Pegel verwendet werden. Während der Bootphase erwartet der Lantime eine serielle Referenzuhr an der ersten Schnittstelle (Refclock-0). Als Schnittstellenparameter können die folgenden Zeitlegramme eingestellt werden.

|                   |           |                |
|-------------------|-----------|----------------|
| Meinberg Standard | 9600Baud  | 7E2 sekundlich |
| Meinberg Standard | 9600Baud  | 8N1 sekundlich |
| Uni Erlangen      | 19200Baud | 8N1 sekundlich |

Als serielles Telegramm kann das Meinberg Standard Zeitlegramm mit MEZ/MESZ oder UTC verwendet werden. Das Uni Erlangen Telegramm überträgt den Offset nach UTC als Wert in Minuten. Das Einstellen des Telegrammtyps wird einmalig bei der Inbetriebnahme über das LC-Display vorgenommen. Dabei sollte das Anschlusskabel zur Referenzuhr zuerst abgezogen werden. Eine Minute nach dem Einschalten des Gerätes erscheint die folgende Meldung und der Zeitserver wartet auf ein Telegramm von der Referenzuhr.

```
waiting for external NTP server or  
refclock at COM0 with 9600/7E2/STD
```

Mit der INC Taste kann dann der Telegrammtyp ausgewählt werden. Nach der Auswahl sollte die serielle Schnittstelle angeschlossen und der Zeitserver noch mal neu gestartet werden. An die zweite serielle Schnittstelle kann eine weitere Referenzuhr angeschlossen werden. Diese zweite serielle Referenz muss manuell in der Datei /mnt/flash/ntpconf.add aktiviert und konfiguriert werden. Öffnen Sie dazu im HTTP Interface den Punkt „NTP“. Über den Punkt „zusätzliche NTP Parameter bearbeiten“ fügen Sie die folgende Zeile hinzu:

```
server 127.127.8.1 mode 2 # Meinberg Standard Format 9600Baud 7E2
```

Der Parameter “mode” bestimmt den Typ des Zeitlegramms:

- mode 2: 9600Baud 7E2 Meinberg Standard
- mode 19: 9600Baud 8N1 Meinberg Standard
- mode 7: 19200Baud 8N1 Uni Erlangen

Außerdem kann noch ein externer NTP Server über Ethernet als Synchronisationsquelle benutzt werden. Dazu muss im Setup unter SETUP->ETHERNET\_LAN\_PARAMETER->EXT\_NTP\_SERVER die TCP/IP Adresse eines externen NTP Zeitservers eingetragen werden. Die entsprechenden Netzwerkparameter wie TCP/IP Adresse, Netzmaske und Gateway müssen so eingestellt sein, dass der externe NTP Server erreicht werden kann. Während der Initialisierungsphase können die Parameter entweder über die Tasten am Lantime oder über das HTTP Interface eingestellt werden. Über das HTTP Interface können insgesamt 3 externe NTP Zeitserver eingestellt werden.

## Bootphase des Linux Rechners

Das Linux Betriebssystem wird aus einer gepackten Datei von der Flash-Disk des Einplatinenrechners in eine RAM-Disk geladen. Das gesamte Dateisystem befindet sich nach dem Booten in der RAM-Disk. Dadurch wird gewährleistet, dass bei jedem Neustart ein initialer Zustand des Dateisystems zur Verfügung steht; nur einige Parameter-Dateien werden zusätzlich auf der Flashdisk gespeichert. Dieser Bootvorgang dauert ca. 1Minute. Während dieser Zeit wird auf dem LC-Display nur ein schwarzer Balken angezeigt. Nachdem das LINUX System hochgefahren ist, wird automatisch die Netzwerkfunktion initialisiert, das Programm zur Kommunikation mit der seriellen Schnittstelle gestartet. Da der interne Rechner keine eingebaute Zeitreferenz hat, wartet dieser so lange, bis er eine Zeitinformaton von der seriellen Schnittstelle (COM0) oder über das NTP Prototoll von einem externen NTP Zeitserver eingelesen hat.

```
waiting for refclock on COM0  
or external NTP server
```

Danach wird der NTPD (NTP Dämon) mit den entsprechenden Parametern gestartet. Dann beginnt die Synchronisationsphase des NTPD; hierbei synchronisiert er sich auf die angegebenen Referenzuhren, welches standardmäßig die lokale Hardwareuhr des Einplatinenrechners, die serielle Schnittstelle an der Rückseite oder ein externer NTP Server sind. Solange der NTPD nicht synchron mit der Referenz ist wird folgende Meldung auf dem LC-Display angezeigt:

```
RDT: ext. NTP server    Wed, 18.11.2002  
NTP: Not Sync         MEZ 10:04:10
```

Damit der NTPD sich auf eine serielle Referenzuhr synchronisieren kann, muss diese synchron sein. Bei einem externen NTP Server muss der Stratum-Wert kleiner als der Stratum-Wert der lokalen Referenzuhr des Einplatinen Rechners sein (dieser Wert ist einstellbar). Ist dies der Fall wird im LC-Display folgende Meldung angezeigt:

```
RDT: ext. NTP server    Wed, 18.11.2002  
NTP: Offset : 1ms      MEZ 10:04:10
```

Die zweite Zeile des LC-Displays bedeutet, dass der NTPD sich auf den externen NTP Server synchronisiert hat mit einem Offset von -1 ms. D.h., die Abweichung von der internen NTP Referenzzeit zum externen NTP Server beträgt aktuell -1 ms. Da es sich bei der internen Referenzzeit des NTP um PLL handelt, braucht es eine gewisse Zeit, bis der Offset optimiert ist. Es wird von dem NTPD gewährleistet, dass der Offset zur Referenzuhr nicht größer als +-128 ms wird; ansonsten wird die Zeit gesetzt. Typisch sind Offsetwerte um +-5 ms, nachdem der NTPD eingeschwungen ist.

## Benutzerschnittstellen zur Konfiguration

Das LANTIME bietet mehrere Möglichkeiten zur Konfiguration der Parameter:

|  |
|--|
| Command Line Interface (CLI) über TELNET<br>Command Line Interface über SSH<br>Command Line Interface über Terminal an der seriellen Schnittstelle (nur BGT Version)<br>HTTP Interface<br>Secure HTTP Interface (HTTPS)<br>Frontpanel LCD Interface<br>SNMP Management |
|--|

Zur ersten Inbetriebnahme des LANTIME muss das Frontpanel LCD Interface benutzt werden, um einmalig eine IP Adresse dem Gerät zu vergeben (siehe auch DHCP IPv4 oder AUTOCONF IPv6). Bei einem LANTIME im Baugruppenträger (BGT) oder einer Variante ohne LCD Interface muss die Inbetriebnahme über das serielle Interface an der Vorderseite der LANCPU mit Hilfe eines Terminal Programms, z.B. von einem Laptop, durchgeführt werden. Wurde einmal das Netzwerkinterface mit entweder einer IPv4 Adresse, Netzmaske und IPv4 GATEWAY oder über die IPv6 SCOPE-LINK Adresse initialisiert, kann von einem anderen Rechner im Netzwerk (remote) auf den LANTIME zugegriffen werden.

Um eine TELNET Verbindung zu dem LANTIME aufzubauen, geben Sie die folgenden Befehle von Ihrer Kommandozeile ein:

```
telnet 198.168.10.10 // IP Adresse vom LANTIME  
user: root  
password: timeserver
```

Mit dem Befehl "setup" kann dann das Konfigurationsprogramm gestartet werden.

Um eine SSH Verbindung zu dem LANTIME aufzubauen, geben Sie die folgenden Befehle von Ihrer Kommandozeile ein:

```
ssh root@198.168.10.10 // IP Adresse vom LANTIME  
password: timeserver
```

Mit dem Befehl "setup" kann dann das Konfigurationsprogramm gestartet werden.

Um eine HTTP Verbindung zu dem LANTIME aufzubauen, geben Sie die folgende Zeile in Ihrem WEB-Browser ein:

```
http://198.168.10.10 // IP Adresse vom LANTIME  
password: timeserver
```

Um eine Secure HTTP (HTTPS) Verbindung zu dem LANTIME aufzubauen, geben Sie die folgende Zeile in Ihrem WEB-Browser ein:

```
https://198.168.10.10 // IP Adresse vom LANTIME  
password: timeserver
```

## **Bedienelemente der Frontplatte**

### **LC Display**

Das zweizeilige LC-Display zeigt Daten des Empfängers wie Position und Zeit sowie den Status des NTPD. Außerdem können, mit Hilfe der unten beschriebenen Tasten, Betriebsparameter gezeigt und geändert werden. Der nächste Abschnitt beschreibt ausführlich alle Menüs. Eine Kurzreferenz befindet sich am Ende dieses Handbuchs.

### **Taste MENU**

Diese Taste schaltet nacheinander durch mehrere Menüs.

### **Taste CLR/ACK**

Mit Hilfe dieser Taste werden geänderte Betriebsparameter im batteriegepufferten Speicher abgelegt. Falls ein Eingabemenü verlassen wird, ohne diese Taste zu betätigen, werden alle bis dahin gemachten Änderungen verworfen.

### **Taste NEXT**

In einem Dateneingabemenü (LCD Cursor ist sichtbar) wird mit Hilfe dieser Taste der Cursor zu der zu ändernden Ziffer bewegt. In einem Menü, welches nur Daten anzeigt (Cursor nicht sichtbar), wird bei Betätigung dieser Taste ein eventuell vorhandenes Untermenü aufgerufen.

### **Taste INC**

Mit Hilfe dieser Taste wird bei der Dateneingabe die Ziffer bzw. der Buchstabe an der Cursorposition geändert.

## Konfiguration über LC-Display

Die Netzwerkparameter des LANTIME können bei der Erstinstallation über die Bedienelemente der Frontplatte konfiguriert werden. Drücken Sie dazu die MENU Taste so oft, bis Sie in das SETUP Menü gelangen. Gleich der erste Punkt im SETUP Menü sind die LAN PARAMETERS. Mit der NEXT Taste können Sie weitere SETUP Menü Punkte wählen. Mit der Taste CLR/ACK bestätigen Sie den Menü-Punkt LAN PARAMETERS. Es erscheint in der unteren Zeile das Untermenü TCP/IP ADDRESS. Auch hier können Sie mit der NEXT Taste die weiteren Netzwerkparameter NET MASK, DEFAULT GATEWAY, IPv6 Adresse, HOSTNAME, DOMAINNAME, NAMESERVER und REMOTE CONNECT auswählen. Mit der Taste CLR/ACK gelangen Sie dann in das Editiermenü der einzelnen Parameter. Im Editiermenü können Sie mit den Tasten NEXT und INC die einzelnen Parameter ändern. Erst wenn die Taste CLR/ACK nach dem Einstellen gedrückt wurde, wird der gerade editierte Wert zwischengespeichert. Drücken Sie im Editiermenü die Taste MENU, werden die eingestellten Werte verworfen und Sie gelangen zurück in das Setup-Hauptmenü (siehe auch Menu Setup). Die gesamten Einstellungen für die LAN PARAMETER werden erst gespeichert, wenn man in der Auswahl die MENU Taste drückt und das Speichern der Änderungen bestätigt.

Die TCP/IPv4 Adresse besteht aus 32 Bits und muss in einem Netzwerk eindeutig identifizierbar sein. Die IP-Adresse muss vom Netzwerkadministrator neu vergeben werden. Ebenso ist die Netzmaske vom Netzwerk fest vorgegeben. Eventuell muss auch die IP-Adresse des Default-Gateway angegeben werden.

Mit dem Programm PING kann von einer beliebigen anderen Arbeitsstation im Netzwerk getestet werden, ob eine Verbindung zum LANTIME hergestellt werden kann. Über den Setup Punkt REMOTE CONNECT können alle Zugriffe über Netzwerk (z.B. über TELNET, FTP oder HTTP) gesperrt werden. Dabei werden die entsprechenden Netzdienste alle gestartet oder gestoppt. Wurde über das HTTP-Interface oder das Setup Programm eine Änderung vorgenommen, kann auch die Anzeige "REMOTE CONNECT: partial enabled" erscheinen. Das NTP Protokoll wird bei jeder Änderung immer neu gestartet.

**WICHTIG:** Eine Verbindung über HTTP, HTTPS, SSH oder TELNET zum LAN-TIME ist nur möglich, wenn im Setup der Punkt REMOTE CONNECT aktiviert ist.

## Das LCD Menü im Einzelnen

### Hauptmenü

Das Hauptmenü wird angezeigt, wenn nach Einschalten des Geräts die Initialisierungsphase abgeschlossen ist. In der ersten Zeile im Display wird die vom NTPD aktuell ausgewählte Referenzuhr angezeigt. In der zweiten Zeile wird der Offset der oben angezeigten Referenzuhr zur lokalen Uhr angezeigt. Auf der rechten Seite wird die Uhrzeit und das Datum mit Zeitzone (immer UTC) dargestellt.

```
DCT: NORMAL OPERATION   Wed, 18.11.2008
NTP: Offset GPS: -1ms   MEZ 10:04:10
```

Die Zeitzone ist immer UTC (Universal Time Coordinated). Wird auf die lokale Uhr synchronisiert, wird in der zweiten Zeile der Stratum-Wert der lokalen Uhr angezeigt. Der Stratum-Wert der lokalen Uhr kann im NTP-Setup Menü von 0 bis 15 eingestellt werden.

Wenn die Taste NEXT gedrückt wird, zeigt ein Untermenü die Software-Versionen des LANTIME sowie die UA509 Flash Software:

```
LANTIME:4.05   SN:000000000000
DCT509 :4.02   SN:9008890
```

Beim zweiten Drücken der Taste NEXT wird die NTP Software Version, die Betriebssystem Version sowie die MAC Adresse der Netzwerkkarte angezeigt.

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

Beim dritten Drücken der Taste NEXT wird der „Fingerprint“ des aktuellen SSH Schlüssels angezeigt.

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

### DCT Statusmenü

Mittels der MENU Taste gelangt man in das Statusmenü der UA509. Unter diesem Punkt wird der Status der UA509-Decodierung zur Anzeige gebracht. Es können nacheinander folgende Texte erscheinen:

#### not sync now

```
DCT STATE:      not sync now
                FIELD: 106
```

Dieser Text zeigt an, dass das DCF-Signal gestört und die Uhr auf Quarzbasis läuft. Dieser Vorgang erfolgt nach dem Einschalten und nach Signalstörungen.

## sync

```
DCT STATE:      sync
                FIELD: 106
```

Die Synchronisation war erfolgreich und die interne Hardwareuhr wird nun minütlich mit dem DCF-Takt synchronisiert.

## FIELD

Hier wird der Wert der digitalisierten DCF-Feldstärke zur Anzeige gebracht, wobei ein logarithmischer Zusammenhang zwischen Feldstärke und angezeigtem Wert besteht. Er kann gut, wie im Kapitel Antennenmontage beschrieben, zur Ausrichtung der Antenne herangezogen werden.

## Menü Referenzuhr Status

Mittels der Menütaste gelangt man aus dem Menü DCT\_STATE in die Statusmenüs der Referenzuhren. Hier wird jeweils der Name der Referenzuhr, der aktuelle Status, der aktuelle Status als Kurztext und die letzten drei Offsetwerte (der neueste Wert steht immer links) zur NTP-Zeit angezeigt. Mit der Taste NEXT kann die nächste Referenz ausgewählt werden.

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

Der Status wird mit vier Ziffern "0000" angezeigt. Die ersten beiden Ziffern geben den aktuellen und die letzten beiden den letzten Status der Referenzuhr an. Folgende Zustände sind möglich:

|                      |  |
|----------------------|--|
| 00: clock okay       | Korrektter Empfang des DCF77 Signals         |
| 01: clock no reply   | Keinen Zeitstring empfangen                  |
| 02: clock bad format | Format des Zeitlegramms ist falsch           |
| 03: clock fault      | Uhr ist nicht synchron oder im Fehlerzustand |
| 04: clock bad signal | Uhr ist nicht synchron                       |
| 05: clock bad date   | Falsches Datum von der Uhr                   |
| 06: clock bad time   | Falsche Uhrzeit von der Uhr                  |

## Menü SETUP

Von diesem Menü aus können mehrere Untermenüs angewählt werden, die entweder der Parametrierung des Gerätes dienen oder eine bestimmte Betriebsart erzwingen. Nachdem mit Hilfe der Taste NEXT das gewünschte Untermenü ausgewählt wurde, kann durch Betätigung von CLR/ACK das Dateneingabemenü aufgerufen werden. In den Dateneingabemenüs werden zunächst die eingestellten Werte angezeigt. Diese können bei Bedarf mit Hilfe der Tasten NEXT und INC geändert werden. Wenn die Änderungen gespeichert werden sollen, muss die Taste CLR/ACK betätigt werden. Nachdem alle Änderungen in einem Untermenü beendet

sind und die MENU Taste gedrückt wurde, erscheint eine Abfrage, ob die Änderungen wirklich gespeichert werden sollen. Dient das Untermenü dazu, eine bestimmte Betriebsart zu erzwingen (z. B. Cold Boot), wird der Benutzer aufgefordert, seine Auswahl durch nochmalige Betätigung von INC zu bestätigen.

```
SETUP:   ETHERNET LAN PARAMETERS
```

## SETUP LAN PARAMETERS

In diesem Untermenü werden die Netzwerkparameter festgelegt. Bei der Erstinstallation des LANTIME müssen diese Parameter auf das vorhandene Netzwerk angepasst werden. Es können die folgenden Parameter eingestellt werden: **TCP/IP ADDRESS, NETMASK, DEFAULT GATEWAY, IPv6 ADDRESS, HOSTNAME, DOMAINNAME, NAMESERVER, SYSLOG SERVER, SNMP MANAGER, REMOTE CONNECT, RESET FACTORY SETTINGS und NET LINK MODE**. Alle Einstellungen beziehen sich hier immer nur auf die erste Ethernet Schnittstelle. Alle weiteren Schnittstellen müssen dann über das HTTP oder CLI Interface eingestellt werden. Über den Parameter REMOTE CONNECT ist es möglich alle Dienste wie TELNET, FTP und HTTP auf dem LANTIME zu sperren oder aber zu aktivieren. Differenzierte Einstellungen können dann später über den Netzwerkzugang gemacht werden. Die Werte für diese Parameter sollten beim Netzwerk Administrator erfragt werden. Bei jeder Änderung der Netzwerkparameter wird die Konfigurationsdatei neu geschrieben und der NTPD neu gestartet.

```
TCP/IP ADDRESS  
000.000.000.000
```

Wird der Menüpunkt **RESET FACTORY SETTINGS** aufgerufen und bestätigt, werden alle Netzwerk Parameter auf die Werkseinstellung zurückgesetzt.

```
Reset factory settings  
INC -> YES           MENU -> NO
```

Alle Parameter für die Konfiguration des Zeitservers werden in der Datei /mnt/flash/global\_configuration auf der Flash-Disk abgespeichert und sind auch nach einem Neustart gültig. Es wird empfohlen diese Datei nicht manuell zu bearbeiten, sondern alle Änderungen über die Konfigurations-Schnittstellen (HTTP, CLI oder SNMP) durchzuführen. Falls diese Datei nicht vorhanden ist, wird automatisch eine leere Datei beim nächsten Abspeichern angelegt. Die Konfigurationsdatei wird im Anhang mit dem Auslieferungszustand abgebildet.

Über den NET LINK MODE können die Parameter für Geschwindigkeit und Duplex der Netzwerkkarte eingestellt werden. Es stehen 5 Modi zur Verfügung: Autosensing, 10 MBit/Halb-Duplex, 100 MBit/Halb-Duplex, 10 MBit/Voll-Duplex, 100 MBit/Voll-Duplex. Standardmäßig werden die Schnittstellen auf Autosensing eingestellt.



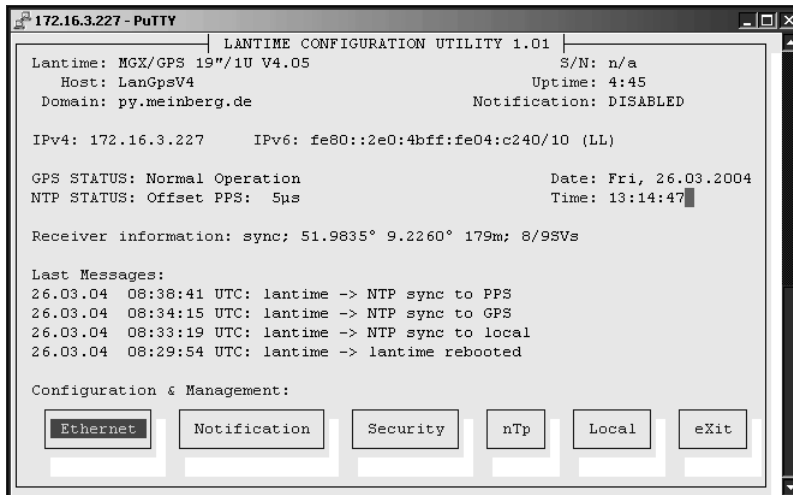
## Die grafischen Konfigurations-Schnittstellen

Beim LANTIME stehen neben dem SNMP Management zwei grafische Benutzerschnittstellen zur Verfügung: Zum einen über einen integrierten HTTP Server, womit der Benutzer mit jedem beliebigen WEB-Browser unabhängig vom Betriebssystem eine HTTP oder HTTPS Verbindung aufbauen kann. Zum anderen kann über eine TELNET oder SSH Verbindung ein Comand-Line-Interface (CLI) geöffnet werden, wo mit Hilfe des Programms "setup" eine textbasierte Benutzerschnittstelle gestartet wird. Bis auf wenige Ausnahmen sind das WEB-Interface und das CLI von den Möglichkeiten zur Konfiguration identisch (das CLI hat keine Statistikfunktion).



The screenshot shows the web interface of the Lantime configuration utility. At the top right is the MEINBERG logo. The title is "Lantime Konfigurationsprogramm 1.01". The interface is divided into several sections:

- System Information:** Lantime: MGX/GPS, SN: n/a, Host: LanGpsV4, IPv4: 172.16.3.226, Domain: py.meinberg.de, IPv6: fe80::2e0:4bff:fe06:746d/10 (Linklocal).
- Status:** GPS Status: Normal Operation, Betriebszeit: 2.09, NTP Status: Offset PPS: -3µs.
- Information des Empfängers:** sync; 51.9835° 9.2259° 178m; 9/9SVs. A note says "Es sind Notizen auf der Handbucheite vorhanden".
- Letzte Meldungen:** A scrollable list of log entries from 20.04.04, including NTP sync events and internal parameter changes.
- Konfiguration und Management:** A row of buttons: Ethernet, Benachrichtigung, Sicherheit, NTP, Lokal, Statistik, Handbuch, Ausloggen.
- Footer:** Contact information for Meinberg Funkuhren, including address, phone, fax, internet website, and email.



The screenshot shows the CLI interface of the Lantime configuration utility, accessed via PuTTY. The title is "172.16.3.227 - PuTTY". The interface displays the following information:

- System Information:** 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.
- IP Addresses:** IPv4: 172.16.3.227, IPv6: fe80::2e0:4bff:fe04:c240/10 (LL).
- Status:** 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:** A list of log entries from 26.03.04, including NTP sync events and a reboot.
- Configuration & Management:** A row of buttons: Ethernet, Notification, Security, nTp, Local, eXit.

Auf den oberen beiden Bildern werden das HTTP-Interface und das Comand-Line-Interface dargestellt. Das CLI kann immer nur von einem Benutzer gleichzeitig ausgeführt werden. Das HTTP-Interface kann gleichzeitig von mehreren Benutzern bedient werden. Dabei besteht die Gefahr, dass sich die einzelnen Sessions gegenseitig beeinflussen.

## Das HTTP Interface

Um eine HTTP Verbindung zu dem LANTIME aufzubauen, geben Sie die folgende Zeile in Ihrem WEB-Browser ein:

**http://198.168.10.10** // wobei die IP Adresse des LANTIME eingegeben werden muss

Es erscheint bei HTTP und HTTPS das gleiche Interface:



The screenshot shows the LANTIME web interface. At the top right is the MEINBERG logo. The main content area is divided into two columns. The left column contains system status information:

|          |                  |           |                 |
|----------|------------------|-----------|-----------------|
| REF :    | Normal Operation | Zeit:     | UTC 09:47:41    |
| NTP:     | stopped          | Datum:    | Thu, 23.03.2006 |
| Host:    | LantimeV5        | IP:       | 172.16.3.226    |
| Kontakt: | Meinberg         | Standort: | Germany         |

Below this is a login form titled "Login for configuration and statistic". It has fields for "User:" (with "root" entered) and "Password:" (with a green bar), and a "login" button.



On the right side of the interface is a graphic of a globe with a clock and a circuit board.

At the bottom of the page is a footer with contact information:

|   |  |  |
|---|--|--|
| Meinberg Funkuhren GmbH & Co. KG<br>Auf der Landwehr 22<br>D - 31812 Bad Pyrmont, Germany | Kontakt<br>Telefon: +49 (0) 52 81 / 93 09 - 0<br>Fax: +49 (0) 52 81 / 93 09 - 30 | Internet<br>Webseite: <a href="http://www.meinberg.de">http://www.meinberg.de</a><br>Email: <a href="mailto:info@meinberg.de">info@meinberg.de</a> |
|---|--|--|

Auf dieser Startseite wird der aktuelle Zustand vom LANTIME angezeigt, entsprechend den Informationen die auch auf dem LC-Display direkt am Gerät dargestellt werden. Die erste Zeile zeigt die Betriebsart des RDT an. Rechts oben wird die Uhrzeit mit der Zeitzone UTC angezeigt, darunter das Datum mit dem Wochentag. Links unten wird der aktuelle Status der NTP Software dargestellt; während der Synchronisationsphase des NTP mit der Referenzuhr (für ca. 5 min nach dem Einschalten) erscheint "NTP: not sync". Dieses wird auch angegeben wenn die Referenzuhr nicht synchron ist und der NTPD dann auf seine "LOCAL-CLOCK" zurück geschaltet hat. Die serielle Referenzuhr wird zum einen über die serielle Schnittstelle und zum anderen über den Sekundenimpuls an den NTP angebunden. Es sind also 2 Referenzuhren, einmal der serielle Zeitstring und zum anderen der PPS (Pulse Per Second), in der Konfiguration des NTP eingetragen. Dieses ist entsprechend im Status des NTP sichtbar; es wird entweder der Offset zur seriellen Anbindung oder zum Sekundenimpuls (PPS) angezeigt: "NTP: Offset RDT: 2ms" oder "NTP: Offset PPS: 1ms". Weiter unten kann der Benutzer und das Passwort zur Konfiguration eingegeben werden. Diese Startseite wird alle 30 Sekunden automatisch neu geladen, um die angezeigten Informationen zu aktualisieren. Dies ist zu beachten, wenn der Benutzer und das Passwort eingegeben wird.

## Konfiguration: Hauptmenü



### Lantime Konfigurationsprogramm 1.01

|          |                   |       |   |
|----------|-------------------|-------|---|
| Lantime: | MGX/RDT 1HE V4.13 | SN:   | n/a                                     |
| Host:    | LanRDTv4          | IPv4: | 172.16.3.237                            |
| Domain:  | py.meinberg.de    | IPv6: | fe80::2e0:4bff:fe06:fb88/10 (Linklocal) |

---

|                             |                  |               |       |
|-----------------------------|------------------|---------------|-------|
| RDT Status:                 | ext. NTP server  | Betriebszeit: | 7 min |
| NTP Status:                 | Offset EXT: -1ms |               |       |
| Information des Empfängers: | n/a              |               |       |

---

**Letzte Meldungen:**

```
31.08.04 09:32:58 UTC: lantime -> NTP sync to external NTP server
31.08.04 09:31:51 UTC: lantime -> NTP sync to local
31.08.04 09:28:33 UTC: lantime -> lantime rebooted
```

---

**Konfiguration und Management:**

---

|  |   |   |
|--|---|---|
| <small>Meinberg Funkuhren<br/>Auf der Landwehr 22<br/>D - 31812 Bad Pyrmont, Germany</small> | <small>Kontakt<br/>Telefon: 49 (0) 52 81 / 93 09 - 0<br/>Fax: 49 (0) 52 81 / 93 09 - 30</small> | <small>Internet<br/>Webseite: <a href="http://www.meinberg.de">http://www.meinberg.de</a><br/>Email: <a href="mailto:info@meinberg.de">info@meinberg.de</a></small> |
|--|---|---|


Nachdem man das Passwort erfolgreich eingegeben hat, gelangt man zur Hauptseite des Konfigurations- und Verwaltungsprogramms. Diese Seite gibt einen kurzen Überblick über die wichtigsten Einstellungen und Laufzeitparameter des Gesamtsystems. Oben links steht die LANTIME Variante mit der Versionsnummer für die LANTIME Software, wobei es sich um einen übergeordneten Softwarestand aller enthaltenen Module und Software Pakete handelt. Darunter wird der aktuelle Hostname und Domainname im Netzwerk geschrieben. Rechts daneben wird die Seriennummer (wie auf dem silbernen Aufkleber auf der Rückseite des Gerätes) und die IPv4 und IPv6 Adresse des ersten Ethernet Anschlusses angegeben.

Im zweiten Abschnitt wird der Status der RDT und des NTP wie oben schon beschrieben angezeigt, sowie zusätzliche Informationen zur Referenzuhr. Auf der rechten Seite wird die Betriebszeit des Systems seit dem letzten Neustart des LANTIMES angezeigt. Sind persönliche Notizen auf der Flash eingetragen worden, wird zusätzlich auf der rechten Seite ein entsprechender Hinweis gegeben.

Im dritten Abschnitt werden die wichtigsten Meldungen der Systemsoftware protokolliert und mit einem Zeitstempel dargestellt. Die letzten Einträge sind dabei immer ganz oben. Diese Ausgabe entspricht der Datei `"/var/log/lantime_messages"`, die nach jedem Neustart neu erstellt wird.

Über die Buttons im unteren Teil gelangt man in die unten beschriebenen Untermenüs.

# Konfiguration: Ethernet



Ethernet
Benachrichtigung
Sicherheit
NTP
Lokal
Statistik
Handbuch
Hauptmenü

## Ethernet Konfiguration

**Netzwerk Informationen:**

Hostname:   
 Domainname:   
 Nameserver 1:   
 Nameserver 2:   
 Syslogserver 1:   
 Syslogserver 2:

---

**Standard-Gateways:**

IPv4 Gateway:   
 IPv6 Gateway:

---

**Verfügbare Netzwerk Dienste:**

|         | Telnet                              | FTP                                 | SSH                                 | HTTP                                | HTTPS                               | SNMP                     | NETBIOS                  |
|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|
| Active: | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

---

**Verfügbare Internet Protokolle:**

|         | IPv4                                | IPv6                                |
|---------|-------------------------------------|-------------------------------------|
| Active: | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

---

**Verfügbare Schnittstellen: 3**

**Schnittstelle 0:**

|   |   |
|---|---|
| TCP/IP address: <input type="text" value="172.16.3.226"/><br>Netmask: <input type="text" value="255.255.255.0"/><br>DHCP-Client: <input type="checkbox"/><br>Net link mode: <input type="text" value="AUTO"/> | IPv6 1: <input type="text"/><br>IPv6 2: <input type="text"/><br>IPv6 3: <input type="text"/><br>Autoconf: <input checked="" type="checkbox"/><br>IP by Router Advertisement: <input type="text"/><br>Link local: <input type="text" value="fe80::2e0:4bff:fe0c:134c/64"/> |
|---|---|

**Schnittstelle 1:**

|  |   |
|--|---|
| TCP/IP address: <input type="text"/><br>Netmask: <input type="text"/><br>DHCP-Client: <input type="checkbox"/><br>Net link mode: <input type="text" value="AUTO"/><br>High availability bonding: <input type="text" value="Einzelverbindung"/> | IPv6 1: <input type="text"/><br>IPv6 2: <input type="text"/><br>IPv6 3: <input type="text"/><br>Autoconf: <input type="checkbox"/><br>Link local: <input type="text" value="fe80::260:6eff:fe30:721/64"/> |
|--|---|

**Schnittstelle 2:**

|  |   |
|--|---|
| TCP/IP address: <input type="text"/><br>Netmask: <input type="text"/><br>DHCP-Client: <input type="checkbox"/><br>Net link mode: <input type="text" value="AUTO"/><br>High availability bonding: <input type="text" value="Einzelverbindung"/> | IPv6 1: <input type="text"/><br>IPv6 2: <input type="text"/><br>IPv6 3: <input type="text"/><br>Autoconf: <input type="checkbox"/><br>Link local: <input type="text" value="fe80::260:6eff:fe30:722/64"/> |
|--|---|

---

**Zusätzliche Netzwerk Konfiguration:**

---

[ top ]

---

|   |  |  |
|---|--|--|
| Meinberg Funkuhren<br>Auf der Landwehr 22<br>D - 31812 Bad Pyrmont, Germany | Kontakt<br>Telefon: +49 (0) 52 81 / 93 09 - 0<br>Fax: +49 (0) 52 81 / 93 09 - 30 | Internet<br>Webseite: <a href="http://www.meinberg.de">http://www.meinberg.de</a><br>Email: <a href="mailto:info@meinberg.de">info@meinberg.de</a> |
|---|--|--|

In der Netzwerk Konfiguration werden alle Parameter bezüglich der Netzwerkschnittstellen konfiguriert. Im ersten Abschnitt werden der Hostname, der Domainname, zwei Nameserver und zwei Syslogserver eingetragen. Bei den Nameservern und Syslogservern können wahlweise IPv4- oder IPv6- Adressen eingetragen werden. Bei dem Syslogserver kann auch ein Hostname eingetragen werden.

## **SYSLOG Server**

Alle Informationen die auf dem LANTIME in das SYSLOG (/var/log/messages) geschrieben werden, können auf einen entfernten Server umgeleitet werden. Der SYSLOG Dämon des entfernten Servers muss entsprechend auf Empfang geschaltet werden, z.B. unter LINUX mit "syslogd -r", um die Syslog-Messages von anderen Servern empfangen zu können.

In der Konfiguration können unter dem Menüpunkt ETHERNET zwei IP-Adressen für SYSLOG Server angegeben werden. Sind beide Adressen auf 0.0.0.0 gesetzt wird der REMOTE SYSLOG-Dienst nicht verwendet.

Beachten Sie, dass alle SYSLOG Ausgaben auf dem Zeitserver unter /var/log/messages gespeichert werden und somit nach einem Neustart des Systems gelöscht sind. Ein täglich ausgeführtes Programm (CRON Job) prüft die Größe der Logg-Dateien und löscht diese, wenn sie zu groß werden.

## **Netzwerkdienste**

Im zweiten Abschnitt kann jeweils für IPv4 und IPv6 ein Default Gateway eingetragen werden.

Im dritten Abschnitt werden die möglichen Zugriffsarten angezeigt: TELNET, FTP, SSH, HTTP, HTTPS, SNMP und NETBIOS. Die einzelnen Dienste können über die Checkboxes aktiviert oder deaktiviert und werden direkt nach dem Abspeichern entsprechend gestartet oder beendet.

Im vierten Abschnitt können die Internet Protokolle IPv4 und IPv6 ausgewählt werden. Derzeit ist das IPv4-Protokoll noch zwingend notwendig und kann nicht abgeschaltet werden. Ein reiner IPv6-Betrieb kann nur dadurch erreicht werden, in dem alle IPv4-Adressen aller Netzwerkanschlüsse auf 0.0.0.0 gesetzt werden und gleichzeitig das DHCP für IPv4 abgeschaltet wird. In diesem Fall wird auf dem Zeitserver keine IPv4-Adresse konfiguriert und man kann nur über IPv6 auf das Gerät zugreifen. TELNET, FTP und NETBIOS sind derzeit nicht über IPv6 möglich. IPv4 und IPv6 können im Mischbetrieb aktiviert werden.

Im letzten Abschnitt werden die Parameter für die Netzwerkanschlüsse konfiguriert. Für jeden physikalischen Netzwerkanschluss (RJ45 Buchse) steht ein separater Abschnitt zur Verfügung. Es können maximal 9 Abschnitte je nach Hardwareausstattung in diesem Menü erscheinen. Auf der linken Seite stehen die Einstellungen für IPv4 und auf der rechten die für IPv6. Ist kein DHCP Client Betrieb für IPv4 aktiviert, so kann manuell eine IP-Adresse für den jeweiligen Netzwerkanschluss eingestellt werden. IPv4-Adressen bestehen aus 32 Bit und werden mit 4 dezimalen Werten zwischen 0 bis 255 durch jeweils einen Punkt getrennt eingegeben:

Beispiel: 192.168.10.2

Bitte wenden Sie sich an Ihren Netzwerk Administrator, der Ihnen eine gültige IPv4-Adresse speziell für Ihr Netzwerk vergibt. Ebenso verfahren Sie mit der Netzmaske.

Abhängig von der Anzahl der integrierten Netzwerkschnittstellen (optional) werden entsprechende Abschnitte für die Netzwerkkonfiguration eingeblendet.

## **DHCP IPv4**

Falls sich ein DHCP Server (Dynamik Host Configuration Protocol) im Netz befindet, kann die Netzwerkeinstellung auch automatisch vorgenommen werden. Um den DHCP Client des LANTIME zu aktivieren, muss 000.000.000.000 als TCP/IP Adresse im LC-Display eingetragen (Auslieferungszustand) oder hier die entsprechende Checkbox aktiviert werden (DHCP-Client). Die Netzwerkeinstellungen werden dann automatisch von einem DHCP-Server (muss sich bereits im Netzwerk befinden) vorgenommen. Die MAC Adresse der Netzwerkkarte wird nach zweimaligem Drücken der NEXT Taste im Hauptmenü vom LCD angezeigt. Im Untermenü "Setup LAN Parameter: TCP/IP-Address" wird die vom DHCP-Server vergebene Adresse angezeigt. Der DHCP-Client vom LANTIME ist nur für das IPv4 Netzwerk Protokoll einsetzbar. Über das HTTP-Interface oder das Setup Programm

kann der DHCP-Client über einen Schalter ein- und ausgeschaltet werden. Damit ist es auch möglich das IPv4 Interface zu deaktivieren, wenn man als TCP/IP Adresse eine 000.000.000.000 einträgt und den DHCP abschaltet.

Wurde der DHCP Client für den Netzwerkanschluss aktiviert, werden die vom DHCP Server automatisch vergebenen IP Adressen in den entsprechenden Feldern angezeigt.

## **IPv6 Adressen und Autoconf**

Im unteren Teil der Seite werden die Einstellungen für das IPv6 Protokoll eingetragen oder angezeigt. Dabei sind 3 globale IPv6 Adressen möglich. IPv6-Adressen haben 128 Bits und werden als Kette von 16-bit-Zahlen in Hexadezimal-Notation geschrieben, die durch Doppelpunkte getrennt werden. Folgen von Nullen können einmalig durch "::" abgekürzt werden.

**Beispiel:**

```
"::" ist die Adresse, die nur aus Nullen besteht.  
 ":::1" ist die Adresse, die aus Nullen und als letztem Bit einer 1  
 besteht. Das ist die Host Local Adresse von IPv6,  
 äquivalent  
 127.0.0.1 bei IPv4.  
 "fe80::0211:22FF:FE33:4455"  
 ist eine typische Link Local Adresse, was man an dem Prefix  
 "fe80" erkennt.
```

In URLs kollidiert der Doppelpunkt mit der Portangabe, daher werden IPv6-Nummern in URLs in eckige Klammern gesetzt ("http://[1080::8:800:200C:417A]:80/").

Ist das IPv6-Netzwerkprotokoll aktiviert, wird dem LANTIME automatisch immer eine Link-Local IPv6-Adresse in der Form "FE80::..." zugewiesen, die die eigene Hardwareadresse der Netzwerkkarte enthält. Die Hardwareadresse (MAC Adresse der Netzwerkkarte des Lantime (ETH0) wird angezeigt, wenn man zweimal die NEXT Taste aus dem Hauptmenü am LC-Display drückt. Befindet sich in dem IPv6 Netzwerk ein Router-Advertiser werden zusätzlich noch eine oder mehrere Link-Global IPv6 Adressen vergeben, wenn IPv6 Autoconf aktiviert wurde.

## **High availability bonding**

Nach IEEE802.3 ist es möglich, eine logische Netzwerkverbindung auf mehrere physikalische Verbindungen zu verschiedenen Switches aufzuteilen. Nur eine physikalische Verbindung wird zur gleichen Zeit verwendet. Offiziell als Bonding for High Availability bezeichnet, bieten es mehrere Hersteller unter verschiedenen Namen an: Link Aggregation, bonding, trunking, teaming. Hier kann ein Ethernet Port einer Bonding Gruppe zugeordnet werden. Es müssen mindestens zwei physikalische Ethernet Anschlüsse einer Bonding Gruppe hinzugefügt werden, damit das Bonding aktiviert wird. Der erste Ethernet Anschluss in einer Gruppe bestimmt die IP-Adresse und die Netzmaske der Bonding Gruppe. Aus technischen Gründen kann der ETH0 Anschluss nicht mit in eine Bonding Gruppe aufgenommen werden. Nur die zusätzlichen Anschlüsse (ETH1, ETH2, ...) können für das Bonding benutzt werden. Ein evtl. vorgeschalteter Netzwerk-Switch muss entsprechend für das Bonding konfiguriert werden.

## Zusätzliche Netzwerkkonfiguration

Mit Hilfe der „Zusätzliche Netzwerkkonfiguration bearbeiten“ können benutzerspezifische Kommandos zur Netzwerkeinstellung hinzugefügt werden. Die abgelegte Datei für die zusätzlichen Netzwerkkonfigurationen wird wie ein Script nach allen internen Konfigurationen ausgeführt. Somit ist es möglich, z.B. zusätzliche Netzwerk Routen zu definieren oder Alias einzurichten.

**MEINBERG**

Ethernet | Benachrichtigung | Sicherheit | NTP | Lokal | Statistik | Handbuch | Hauptmenü

### Ethernet Konfiguration

Inhalt von /mnt/flash/config/netconf.cmd:

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

Datei speichern | Schließen

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

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

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

Über den Schalter „Samba Konfiguration bearbeiten“ kann direkt die Datei „/etc/samba/smb.conf“ editiert werden.

**MEINBERG**

Ethernet | Benachrichtigung | Sicherheit | NTP | Lokal | Statistik | Handbuch | Hauptmenü

### Ethernet Konfiguration

Inhalt von /mnt/flash/config/samba/smb.cnf:

```
create mask = 0600
browseable = No
[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = ntadmin root
force group = ntadmin
create mask = 0664
directory mask = 0775
```

Datei speichern | Schließen

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

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

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)



# Konfiguration: Notification



## Benachrichtigungen

### Email Information:

Empfänger:

Absender:

Smarthost:

### Windows Messenger Information (WinPopup):

Mail Adresse 1:

Mail Adresse 2:

### SNMP Information:

SNMP manager 1:  Community:

SNMP manager 2:  Community:

### VP100/NET Anzeige Information:

Display 1:  Serial number:

Display 2:  Serial number:

### Benutzerdefinierte Benachrichtigung:

### Benachrichtigungen:

| Bedingung:  | Auslöser:                |                          |                          |                          |                          |
|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
|   | Email                    | Wmail                    | SNMP                     | VP100/NET                | Benutzer                 |
| NTP not sync  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| NTP stopped   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Server boot   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Receiver not responding                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Receiver not sync                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Config changed                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="button" value="Meldungen bearbeiten"/> |                          |                          |                          |                          |                          |

[ top ]

## Alarm Ereignisse

Über die "Benachrichtigung" (Alarm- und Status-Nachrichten) Einstellungen können unter verschiedenen Bedingungen ausgewählte Aktionen vom Zeitserver ausgeführt werden. Dies ist deswegen sinnvoll, weil der Zeitserver unbeobachtet die Zeit zur Verfügung stellt; wenn dann aber doch ein Fehler auftreten sollte, muss einem Verantwortlichen eine Nachricht (Alarmmeldung) gesendet werden, damit innerhalb kürzester Zeit darauf reagiert werden kann.

Bei diesem Zeitserver stehen die vier Aktionen EMAIL, SNMP-TRAP, WINDOWS POPUP MESSAGE und die Anzeige der Nachricht über das Großdisplay VP100/NET zur Verfügung. Jede Bedingung kann mit jeder Aktion beliebig verknüpft werden.

|                           |   |
|---------------------------|---|
| "NTP not sync"            | NTP nicht synchron zur Referenzzeit                 |
| "NTP stopped"             | NTP wurde angehalten (meist zu große Zeitabweichung |
| "Server boot"             | System wurde neu gestartet                          |
| "Receiver not responding" | keine Antwort von der Referenz Funkuhr              |
| "Receiver not sync"       | GPS Empfänger nicht synchronisiert                  |
| "Config changed"          | Systemparameter vom Benutzer geändert               |

Für jedes Ereignis kann in dem letzten Abschnitt der „Benachrichtigungen“ ein beliebiger „Auslöser“ zugeordnet werden. Die entsprechenden Einstellungen für die fünf verschiedenen Aktionen werden in den oberen Abschnitten vorgenommen.

## Alarm EMAIL

In verschiedenen Systemzuständen können E-Mails mit den entsprechenden Zuständen automatisch vom LANTIME versendet werden. In dem Abschnitt "EMAIL Information" können die Absender Adresse (From:), die EMAIL Adresse (To:) und ein eventuell vorhandener EMAIL-SMARTHOST (ausgehender Mailserver) angegeben werden. Diese Einstellungen können nicht über das LCD-Frontpanel geändert werden. Folgende Hinweise zur Konfiguration der EMAILs sollten beachtet werden:

- Der Hostname und der Domainname sollte dem E-Mail-Smarthost bekannt sein
- Es muss ein gültiger Nameserver eingetragen sein
- Der Domainnamen-Teil der Absender Adresse (From:) sollte gültig sein

## Windows Popup Message

Microsoft Windows stellt mit dem WinPopup (Windows Mail) ein lokales Benachrichtigungswerkzeug zur Verfügung. Damit können über das Windows eigene Protokoll-Nachrichten direkt an Rechner im lokalen Netzwerk versendet werden. Für diese Nachrichten braucht das NETBIOS nicht aktiviert werden. Es muss der „Microsoft Client für Windows Netzwerke“ aktiviert sein. Im zweiten Abschnitt kann der Rechnername von bis zu zwei Windows Rechnern angegeben werden. Jede Nachricht wird mit einem Zeitstempel und der Benachrichtigung im Klartext versehen:



## Alarm SNMP-TRAP

In den Einstellungen für die SNMP TRAPs als Benachrichtigung und Alarmmeldung können zwei unabhängige SNMP Manager (SNMP TRAP Receiver) als IPv4, IPv6 oder Hostname eingestellt werden. Zusätzlich muss zu jedem SNMP Manager ein sogenannter Community String (eine Art Gruppenpasswort) eingestellt werden (default: „public“). Diese sind nicht mit den SNMP Community Strings des internen SNMPD zu verwechseln, die auf der Security Seite beschrieben werden.

## VP100/NET Display

Die Großanzeige VP100/NET dient zur Anzeige von Uhrzeit und Datum. Diese Anzeige hat eine integrierte Netzwerkkarte und einen SNTP Client. Die Zeit wird von einem beliebigen NTP Zeitserver über das SNTP Protokoll abgeholt und damit die interne Uhr nachgeregelt. Diese Anzeige kann auch beliebige Texte als Laufschriften darstellen. Alle Alarmmeldungen können als Textmeldung auf dem Display angezeigt werden. Wenn ein ausgewähltes Ereignis auftritt, wird diese Meldung 3 mal hintereinander als Laufschrift auf dem Display angezeigt.

Dazu müssen im vierten Abschnitt die IP Adresse und die Seriennummer der VP100/NET eingetragen werden. Die Seriennummer des Displays wird angezeigt, wenn man die rote SET Taste 4 mal drückt. Es muss die gesamte Nummer in das Feld eingetragen werden.

Die Schnittstelle zu dem VP100/NET Display kann auch direkt über ein LINUX Tool von der Kommandozeile angesteuert werden. Damit ist es möglich noch weitere Nachrichten, z.B. aus eigenen Scripten oder CRON Jobs auf dem Display darzustellen. Beim Aufruf des Kommandozeilen Programms ohne Parameter werden alle Parameter und eine kleine Anleitung angezeigt (siehe Anhang).

## Benutzerdefinierte Benachrichtigung

Über den Benachrichtigungspunkt „Benutzer“ kann ein frei definierbares Skript automatisch bei einer Bedingung ausgeführt werden. Über die Punkte „Benutzerdefiniertes Benachrichtigungsskript anzeigen“ und „Bearbeiten“ kann dieses Skript angezeigt und bearbeitet werden. Das Skript ist auf der Flash unter /mnt/flash/user\_defined\_notification zu finden. Dem Skript wird als Parameter der Index und der zugehörige Alarmtext übergeben. Der Index der Test-Bedingung ist dabei 0.

## Alarm Texte

Über den extra Button „Edit messages“ können alle Texte, die als Nachricht versendet werden, frei eingestellt werden. Diese Informationen werden in der Datei /mnt/flash/notification\_messages gespeichert.



**Benachrichtigungen**

Benachrichtigungen: Bitte passen sie die Meldungen Ihren Bedürfnissen an

| Bedingung:              | Angepasste Bedingung: |
|-------------------------|-----------------------|
| NTP not sync            |                       |
| NTP stopped             |                       |
| Server boot             |                       |
| Receiver not responding |                       |
| Receiver not sync       |                       |
| Config changed          |                       |
| Vorgegebene Meldungen   |                       |

[ top ]

---

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

Kontakt  
 Telefon: 49 (0) 52 81 / 93 09 - 0  
 Fax: 49 (0) 52 81 / 93 09 - 30

Internet  
 Webseite: <http://www.meinberg.de>  
 Email: [info@meinberg.de](mailto:info@meinberg.de)

# Konfiguration: Sicherheit



- Ethernet
- Benachrichtigung
- Sicherheit
- NTP
- Lokal
- Statistik
- Handbuch
- Hauptmenü

## Sicherheits Management

### Login:

Neues Passwort:

Wiederholung:

### SSH Schlüsselgenerierung:

### HTTPS Zertifikat:

### NTP autokey:

NTP autokey Passwort:

### NTP symmetrische Schlüssel:

### SNMP:

Lese-Community:

Lese/Schreib Community:

SNMP Kontakt:

SNMP Standort:   
[Die Werte können auf der LOKAL-Seite editiert werden](#)

Benutzername:

Authentifikations Ausdruck:

Ausdruck wiederholen:

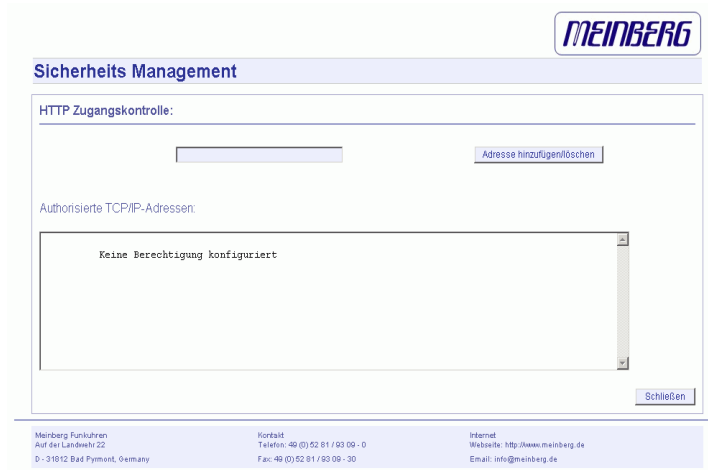
[ top ]

## Passwort

Über die Sicherheitsverwaltung können alle sicherheitsrelevanten Einstellungen für den Zeitserver vorgenommen werden. In dem ersten Abschnitt „Login“ kann das Zugangs Passwort für SSH, TELNET, FTP, HTTP und HTTPS eingestellt werden. Das Passwort wird verschlüsselt auf dem internen Flash abgelegt und kann nur mit Hilfe eines „Factory Reset“ in den Ursprungszustand („timeserver“) zurückgesetzt werden (siehe auch Konfiguration über das LCD).

## HTTP Zugangsberechtigung

Über den Punkt „HTTP-Zugangsberechtigung konfigurieren“ kann der Zugriff auf das HTTP(S) Interface auf bestimmte IP-Adressen beschränkt werden. Nur die IP-Adressen, die in dieser Liste enthalten sind, können sich auf der HTTP Seite einloggen.



Wenn der Zugang verweigert wurde, erscheint das folgende Bild:



## SSH Secure Shell Login

Über das „Secure Shell Login“ (SSH) ist es möglich eine gesicherte Verbindung zum LANTIME aufzubauen. Alle Daten werden während der Übertragung über das Ethernet verschlüsselt. Somit werden auch keine lesbaren Kennwörter über das Netzwerk gesendet. Die aktuelle LANTIME Version unterstützt SSH1 und SSH2 über IPv4 und IPv6. Um diesen Dienst nutzen zu können, muss der SSHD in den Netzwerkeinstellungen aktiviert werden und ein SSH Schlüssel auf dem Zeitserver erzeugt werden. Von einem entfernten Rechner kann dann mit dem Kommando „ssh“ eine Secure Shell geöffnet werden:

```
sshroot @ 192.168.16.111
```

Beim ersten Zugriff muss das neue Zertifikat bestätigt werden und dann wird man nach dem Passwort („timeserver“) gefragt.

Über den Schalter „Generate SSH key“ kann ein neuer Schlüssel erzeugt werden. Dieser Schlüssel kann dann per „Cut & Paste“ in die lokale SSH Konfiguration des Clients übertragen werden. Mit dem Schalter „SSH Schlüssel anzeigen“ kann der aktuelle Schlüssel auf dem LANTIME angezeigt werden.



The screenshot shows the Meinberg Sicherheits Management web interface. At the top right is the Meinberg logo. Below it is a header for 'Sicherheits Management'. The main content area displays the output of an SSH key generation process, titled 'Inhalt von /tmp/ssh\_key\_output:'. The output text is as follows:

```
Generating public/private rsal key pair.  
Your identification has been saved in /mnt/flash/packages/ssh/etc/ssh/ssh_host_key.  
Your public key has been saved in /mnt/flash/packages/ssh/etc/ssh/ssh_host_key.pub.  
The key fingerprint is:  
13:63:f9:0b:05:55:36:64:6e:15:26:66:8c:88:35:ef Lan@psV4  
  
ssh_host_key.pub:  
1024 35  
1181797084099888106352061408244913592379990069689893511137896883043098128881958877637550575924321400  
6046737685070802076734467764470295565387989794303343740516322391440766086723221967892410974182743411  
9318903611718337065721559589075960146892061332257641685908798178978932389500108552658852983781432882  
424106851 Lan@psV4
```

At the bottom right of the output area is a 'Schließen' button. Below the main content area is a footer with contact information for Meinberg Funkuhren, including address, phone, fax, internet website, and email.

## SSL Zertifikat für HTTPS erstellen

HTTPS ist der Standard für die verschlüsselte Übertragung von Daten zwischen Browser und Webserver. Er beruht auf X.509-Zertifikaten. Grundlage sind unsymmetrische Verschlüsselungsverfahren. Der Zeitserver verwendet diese Zertifikate, um sich gegenüber einem Client zu authentifizieren. Bei der ersten Verbindung HTTPS zu diesem Server muss einmal dieses Zertifikat angenommen werden. Bei weiteren Zugriffen wird das Zertifikat dann mit dem gespeicherten verglichen. Bei der Annahme des Zertifikates genügt es normalerweise immer mit „Weiter“ zu antworten und das Zertifikat unbefristet anzunehmen.

Über den Schalter „SSL Zertifikat für HTTP erzeugen“ kann ein neues Zertifikat für eine gesicherte HTTP Verbindung erstellt werden. Es erscheint ein Formular, auf dem die genauen Nutzerdaten wie Organisation, Name, Emailadresse und der Standort angegeben werden müssen.

MEINBERG

HHTPs Zertifikat erzeugen

Bitte folgende Felder ausfüllen:

Land:  (2 Buchstaben)

Ort:

Firma:

Allgemeiner Name:

Email-Adresse:

mit Diffie-Hellman Parameter erzeugen

SSL Zertifikat erzeugen Zurück

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

Kontakt  
Telefon: +49 (0) 52 81 / 93 00 - 0  
Fax: +49 (0) 52 81 / 93 00 - 30

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

Nach der erfolgreichen Erzeugung des SSL Zertifikats wird das gesamte Ergebnis angezeigt.

MEINBERG

Sicherheits Management

Inhalt von /www/filetmp:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBoQdg8LrOEsslmBOA2Oe1u8FLc3JRS+Bx0TQhbcNBOAPeFz+4a
pZvYrY8E0+neK2bepLZvhlMy5enFzU01IGIA4Tq3k/CzEtDcZBngdvoXLA8y8e
WnRg6Z3gr3j0eB07XMLJQ2vooK7Rg86VnCAKRS52hexGZDVKQ14F41YvQ1IAAB
Ae9BALHLHfl+/EhytWVZ+M6I+/F421R1aeXDRvtOR7LhgRHpIjafnMANNRkVYC2Q
+41bNFMUtmf5vLr3u2hgTUI0mLV2f4GLBHLSP6CfuZLo6/x0cWYXJRNaxpMwZ
oRidgeC3aB6bvqE008TVEI8m0Jmpe2vBck1fWQjgfQ8+AkEA9+svF4TL/fdC
B181x345E34E2KxPK2j39MntZ23mM3c2pwoN0u09mLn24mU1a6eR/IM
1L8dYHAt+uTRA0Tqo5+m8TbnIv/5Lr/XWQ/cfVvQ0e2Iy83aZJMnc8x6UZSFR
c01cS2nr46da1jFOV7v9IFA2c9cM6G21aCQC28c46827w8VpEVLWegqj05L
-----
```

Schließen

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

Kontakt  
Telefon: +49 (0) 52 81 / 93 00 - 0  
Fax: +49 (0) 52 81 / 93 00 - 30

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

Zusätzlich kann ein eigenes Zertifikat mittels des Buttons „HTTPS-Zertifikat importieren“ eingespielt werden.

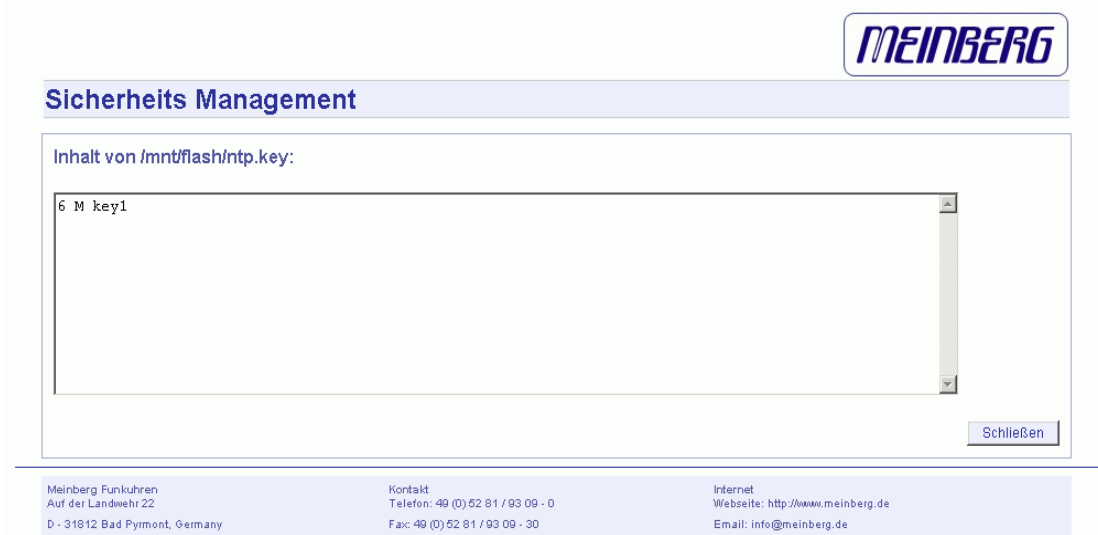


## NTP Schlüssel und Zertifikate

Im vierten und fünften Abschnitt können die symmetrischen Schlüssel und die Autokey Zertifikate für den NTP angelegt und erzeugt werden (siehe auch NTP Authentication).

Über den Punkt „Neues NTP Autokey Zertifikat erzeugen“ wird automatisch ein beglaubigtes (trusted) Zertifikat erzeugt. Dieses Zertifikat ist abhängig von dem eingestellten Hostnamen. Das Zertifikat muss immer erneuert werden, wenn der Hostname des Zeitservers geändert wurde. Die Zertifikate werden mit dem internen Tool „ntp-keygen -T“ erzeugt. Die öffentlichen und privaten Schlüssel werden im Verzeichnis „/etc/ntp/“ abgelegt. Bitte lesen Sie hierzu auch das Kapitel über NTP Autokey.

Über die beiden Punkte „NTP MD5 Schlüssel anzeigen“ und „NTP MD5 Schlüssel erzeugen“ können die symmetrischen NTP Keys verwaltet werden. Bitte lesen Sie hierzu auch das Kapitel über die symmetrischen Keys.




The screenshot shows the 'Sicherheits Management' interface of a Meinberg device. At the top right is the 'MEINBERG' logo. Below it is a header 'Sicherheits Management'. The main content area is titled 'Inhalt von /mnt/flash/ntp.key:' and contains a text box with the text '6 M key1'. A 'Schließen' button is located at the bottom right of the text box. At the bottom of the page, there is a footer with contact information for Meinberg Funkuhren, including address, phone, fax, internet website, and email.

|   |  |  |
|---|--|--|
| Meinberg Funkuhren<br>Auf der Landwehr 22<br>D - 31812 Bad Pyrmont, Germany | Kontakt<br>Telefon: 49 (0) 52 81 / 93 09 - 0<br>Fax: 49 (0) 52 81 / 93 09 - 30 | Internet<br>Webseite: <a href="http://www.meinberg.de">http://www.meinberg.de</a><br>Email: <a href="mailto:info@meinberg.de">info@meinberg.de</a> |
|---|--|--|

## SNMP Parameter

Im letzten Abschnitt können die Parameter für den SNMP eingetragen werden. Bei Änderungen von grundlegenden Änderungen der SNMP Parameter muss das Gerät neu gestartet werden oder der SNMP Dienst über die Ethernet Einstellungen einmal aus- und wieder eingeschaltet werden. Weitere Informationen zu den Eigenschaften des SNMP befinden sich in einem späteren Kapitel.

## Konfiguration: NTP



EthernetBenachrichtigungSicherheitNTPLokalStatistikHandbuchHauptmenü

### NTP Management

**NTP Konfiguration:**

|                              |                      |            |                      |  |                                 |
|------------------------------|----------------------|------------|----------------------|--|---------------------------------|
| Externe NTP Serveradresse 1: | <input type="text"/> | Schlüssel: | <input type="text"/> | <input type="checkbox"/> Autokey verwenden | <input type="checkbox"/> Prefer |
| Externe NTP Serveradresse 2: | <input type="text"/> | Schlüssel: | <input type="text"/> | <input type="checkbox"/> Autokey verwenden | <input type="checkbox"/> Prefer |
| Externe NTP Serveradresse 3: | <input type="text"/> | Schlüssel: | <input type="text"/> | <input type="checkbox"/> Autokey verwenden | <input type="checkbox"/> Prefer |
| Externe NTP Serveradresse 4: | <input type="text"/> | Schlüssel: | <input type="text"/> | <input type="checkbox"/> Autokey verwenden | <input type="checkbox"/> Prefer |
| Externe NTP Serveradresse 5: | <input type="text"/> | Schlüssel: | <input type="text"/> | <input type="checkbox"/> Autokey verwenden | <input type="checkbox"/> Prefer |

---

Stratum der lokalen Uhr:

Local clock deaktivieren

Vertrauenswürdiger Schlüssel:

NTP Broadcast Adresse:

Broadcast Intervall:

NTP Trusttime:  Tage ▼  
0=Standard-Trusttime des Empfängers wird verwendet

|        | Autokey                  | PPS                                 |
|--------|--------------------------|-------------------------------------|
| Aktiv: | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Zusätzliche NTP Parameter bearbeitenAktuelle NTP Konfiguration anzeigen

NTP-Berechtigung konfigurieren

---

SpeichernZurücksetzenZurück

|   |  |  |
|---|--|--|
| Meinberg Funkuhren GmbH & Co. KG<br>Auf der Landwehr 22<br>D - 31812 Bad Pyrmont, Germany | Kontakt<br>Telefon: +49 (0) 52 81 / 93 09 - 0<br>Fax: +49 (0) 52 81 / 93 09 - 30 | Internet<br>Webseite: <a href="http://www.meinberg.de">http://www.meinberg.de</a><br>Email: <a href="mailto:info@meinberg.de">info@meinberg.de</a> |
|---|--|--|

In der NTP Konfiguration werden alle zusätzlichen Parameter neben der standardmäßigen Konfiguration des Zeitservers, eingestellt. Diese Standard Konfiguration besteht als erstes aus der „local clock“, welche der Hardwareuhr des Betriebssystems entspricht und immer dann benutzt wird, wenn die anderen Referenzuhren nicht mehr zur Verfügung stehen (z.B. wenn diese nicht synchronisiert haben). Der Stratum-Wert dieser „local clock“ wird sehr hoch gesetzt (default: 12) damit die angeschlossenen Benutzer ein Umschalten auf diese nicht sehr genaue Zeit registrieren und entsprechend darauf reagieren können. Die „Local Clock“ kann auch abgeschaltet werden, wenn zum Beispiel bei einem Ausfall der Referenzuhr keine Zeit mehr den Clients zur Verfügung gestellt werden soll. Als zweites wird die

serielle Schnittstelle der Referenzuhr als erste Referenzuhr eingestellt. Da diese Referenzzeit nur über die serielle Schnittstelle angebunden ist, kann hiermit vom NTP nur eine Genauigkeit um 1 ms erreicht werden. Die eigentliche Genauigkeit (um 10 Mikrosekunden) wird erst über den ATOM Treiber des NTP erreicht, welche direkt über das Betriebssystem den PPS (Pulse Per Second) der Referenzuhr auswertet. Die Standard Konfiguration hat folgendes Aussehen:

```
# *** 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
```

Über diese Konfigurationsseite können zusätzliche NTP Parameter eingestellt werden. Im oberen Teil können bis zu 5 externe NTP Server als Redundanz zu der internen Referenzuhr angegeben werden. Dabei kann wahlweise, ein symmetrischer Schlüssel eingegeben werden und AUTOKEY aktiviert werden. Der „Prefer“ Schalter kann gesetzt werden, wenn eine externe Referenz bevorzugt verwendet werden soll. Die interne Referenzuhr hat immer ein „Prefer“ gesetzt und hat dazu einen besseren Stratum als alle anderen Referenzuhren. Das Setzen mehrerer „Prefer“ macht dann Sinn, wenn einige NTP-Server zeitweise nicht erreichbar oder ausgefallen sind.

Über den Punkt „Stratum of local clock“ wird der Stratum-Wert der lokalen Referenzuhr angegeben. Dieser Wert wird dann wichtig, wenn alle Referenzuhren ausgefallen sind; dann schaltet der NTP auf seine „local clock“. Die NTP Clients entscheiden mit Hilfe des Stratum-Wertes, ob sie die Zeit des NTP Servers akzeptieren. Der Stratumwert kann nur von der „Local clock“ gesetzt werden.

Mit dem Punkt „Local trusted key“ kann eine Liste aller symmetrischen Schlüssel durch Komma getrennt eingegeben werden, die vom NTP akzeptiert werden.

Soll zusätzlich die NTP Zeit als Broadcast im lokalen Netzwerk verteilt werden, kann hier eine gültige Broadcast Adresse eingegeben werden. Beachten Sie, dass ab der Version NTP 4 Broadcast immer mit Authentication benutzt werden muss. Im Folgenden wird eine Beispiel-Konfiguration für einen NTP Client mit symmetrischer Authentifizierung gezeigt:

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

Die NTP Trusttime gibt die Zeit an, wie lange der NTP die GPS Referenzzeit noch akzeptiert, wenn diese in den Freilauf Zustand (nicht mehr synchron) wechselt. Die Freilauf-Genauigkeit der Referenzuhr hängt direkt mit dem eingebauten Quarz zusammen. Standardmäßig ist ein TCXO Quarz im Lantime GPS eingebaut. Wird dieser Wert auf Null gesetzt, ist der Default Wert gültig. Die Default Trusttime Werte sind wie folgt:

Lantime/GPS : 96 Stunden  
Lantime/PZF : 0,5 Stunden  
Lantime/RDT: 0,5 Stunden  
Lantime/NDT: 96 Stunden

Im nächsten Punkt können die beiden Optionen AUTOKEY und PPS für den Zeitserver aktiviert werden, wobei PPS sich auf die zusätzliche Referenzuhr über den Sekundenimpuls bezieht.

Nach jedem Neustart und nach allen Änderungen der Konfiguration wird immer eine neue Datei **/etc/ntp.conf** vom LANTIME automatisch generiert, d.h. man kann keine Änderungen direkt an dieser Datei vornehmen. Wenn weitere Einstellungen am NTP (Authentication, Restriction ...) benötigt werden, die nicht mit den oben beschriebenen Parametern erreicht werden können, muss eine zusätzliche Konfigurationsdatei bearbeitet werden. Wenn die NTP Parameter permanent geändert werden sollen, muss eine Datei **/mnt/flash/ntpconf.add** erstellt werden, welche dann automatisch beim Booten oder Ändern der NTP Parameter an die Datei **/etc/ntp.conf** angehängt wird. Über den Punkt „Zusätzliche NTP Parameter bearbeiten“ kann diese zusätzliche Datei bearbeitet und verwaltet werden.

**MEINBERG**

### NTP Management

Inhalt von /mnt/flash/ntpconf.add:

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

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

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

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

Über den Punkt „Aktuelle NTP Konfiguration anzeigen“ wird die aktuelle NTP Konfigurationsdatei angezeigt. Diese Datei wird vom System automatisch bei jedem Neustart und Neukonfiguration erzeugt und kann daher nicht direkt bearbeitet werden.

**MEINBERG**

**NTP Management**

Inhalt von /etc/ntp.conf:

```
# *** Localize ***
# NTP.CONF for VERS17 with ONLY ERLANGEN (do not modify)
server 127.127.1.0 # local clock
fudge 127.127.1.0 stratum 12 # local stratum
server 127.127.8.0 mode 155 prefer # SES-17 VME Erlangen PES
fudge 127.127.8.0 sname1 0.004000 # calibration value
fudge 127.127.8.0 flags 0 flags 1
server 127.127.22.0 ntpgo-1 6 ntpgo-1 6 # ATOM (EPS)
fudge 127.127.22.0 flags 0 flags 0
enable pps
enable stats
enable /var/log/
statistics loopstats
driftfile /etc/ntp.drift
# Edit /etc/fstab/ntpconf.add to add additional NTP parameters
```

Schließen

MEINBERG Funkuhren  
Auf der Lahnstraße 22  
D - 31812 Bad Pyrmont, Germany      Kontakt  
Telefon: +49 (0)52 81 / 93 09 - 0  
Fax: +49 (0)52 81 / 93 09 - 30      Internet  
Webseite: http://www.meinberg.de  
Email: info@meinberg.de

Über den Punkt „NTP-Berechtigung konfigurieren“ können bestimmte NTP Clients über IP Adresse und Netzmaske explizit freigegeben werden. Wird ein Eintrag in dieser Liste gemacht werden automatisch alle anderen IP-Adressen ausgeblendet, d.h. nur die Benutzer aus dieser Liste haben NTP-Zugriff (dürfen die Zeit anfragen) auf den Zeitserver.

**MEINBERG**

**NTP Management**

NTP Zugangsberechtigung hinzufügen:

IP-Adresse:

Netzmaske:  (nur IPv4)

Aktuelle NTP Berechtigungen:

|  |   |
|--|---|
| <input type="button" value="Berechtigung zurücknehmen"/> | restrict 172.16.3.13 mask 255.255.255.255 |
| <input type="button" value="Berechtigung zurücknehmen"/> | restrict 172.16.5.0 mask 255.255.255.0    |

Meinberg Funkuhren  
Auf der Lahnstraße 22  
D - 31812 Bad Pyrmont, Germany      Kontakt  
Telefon: +49 (0)52 81 / 93 09 - 0  
Fax: +49 (0)52 81 / 93 09 - 30      Internet  
Webseite: http://www.meinberg.de  
Email: info@meinberg.de

Die folgenden Eintragungen werden automatisch in der NTP Konfigurationsdatei gemacht:

```
#NTP RESTRICTION SECTION - LAST MODIFIED: Wed Jan 5 07:47:58 2005
restrict 0.0.0.0 mask 0.0.0.0 ignore # block IPv4 completely
restrict 127.0.0.1 mask 255.255.255.255 # allow localhost
restrict ::0 ignore # block IPv6 completely

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

In diesem Beispiel wird die Adresse 172.16.3.13 für alle NTP Zugriffe freigeschaltet und zusätzlich alle Adressen aus dem Subnetz 172.16.5.xxx.

## NTP Authentication

NTP bietet in der Version 2 und 3 ein Authentication Verfahren über symmetrische Schlüssel. Wird ein Paket in diesem Authentication Mode verschickt, so wird an jedes ein 32-bit Key ID und eine cryptografische 64/128-bit Checksumme des Paketes, erstellt entweder mit Data Encryption Standard (DES) oder Message Digest (MD5) Algorithmen, angehängt. Beide Algorithmen bieten ausreichenden Schutz vor Manipulation der Inhalte. Zu beachten ist, dass die Verbreitung des DES in den USA sowie in Kanada Einschränkungen unterliegt, während MD5 zur Zeit davon nicht betroffen ist. Mit jedem der beiden Algorithmen berechnet der empfangende Partner die Checksumme und vergleicht sie mit der im Paket enthaltenen. Beide Partner müssen hierfür den gleichen Encryption Key mit der dazugehörigen gleichen Key ID haben. Dieses Feature bedarf einiger kleiner Modifikationen an der Standard Paket Verarbeitung. Diese Modifikationen werden in der Konfigurationsdatei aktiviert. Im Authentication Mode werden Partner als unglaubwürdig und für eine Synchronisation nicht geeignet gekennzeichnet, wenn sie entweder unauthenticierte Pakete, authentifizierte Pakete die nicht entschlüsselt werden können oder authentifizierte Pakete, die einen falschen Key benutzen, senden. Zu beachten ist, dass ein Server der viele Keys kennt (identifiziert durch viele Key IDs) möglicherweise nur einen Teil dieser verwendet. Dies ermöglicht dem Server einen Client, der eine authentifizierte Zeitinformation verlangt, zu bedienen ohne diesem selbst zu trauen. Einige zusätzliche Konfigurationen sind erforderlich um die Key ID zu spezifizieren, die jeden Partner auf Authentizität prüft. Die Konfigurationsdatei für einen Server Authentication Mode kann wie folgt aussehen:

```
# 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 (7) for accessing server variables
controlkey 15               # key (6) for accessing server variables
```

Der Authentication Mode wird automatisch aktiviert, wenn ein Key benutzt wird und die Pfade für die Keys entsprechend eingestellt sind. Mit **keys /mnt/flash/ntp.keys** wird der Pfad für die Keys festlegt. In der **trustedkey**-Zeile werden die Keys angegeben, die als uncompromised bekannt sind; der Rest sind verfallene oder compromised Keys. Beide Sätze von Keys müssen in der unten beschriebenen Datei **ntp.keys** deklariert werden. Dies ermöglicht es, alte Keys zu reaktivieren, während das wiederholte Senden von Keys minimiert wird. Die **requestkey 15** Zeile deklariert den Key für mode-6 control messages wie in RFC-1305 spezifiziert und vom **ntpq** Utility Programm benutzt, während die Zeile **controlkey 15** den Key für mode-7 private control messages deklariert, wie vom **ntpdc** Utility Programm benutzt wird. Diese Keys werden benutzt um die Daemon Variablen vor unberechtigten Modifikationen zu schützen.

Die Datei **ntp.keys** beinhaltet eine Liste der Keys und zugehöriger IDs, die der Server kennt und muss deshalb auf nicht lesbar gesetzt werden. Vom Lantime werden keine DES Keys aus der Benutzeroberfläche unterstützt. Der Inhalt kann wie folgt aussehen:

```
# 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
```

Die erste Spalte der Datei beinhaltet die Key ID, die zweite Spalte das Format des Keys und die dritte den Key selbst. Es gibt vier Key-Formate: Ein **A** steht für einen DES Key mit bis zu acht 7-Bit ASCII Characters, bei dem jeder Character für ein Key-Octet steht (wie bei einem Unix Passwort). Ein **S** steht für einen DES Key als Hex Ziffer, bei welchem das niederwertigste Bit (LSB) jedes Octets das ungerade Parity Bit ist. Ein mit **N** gekennzeichnete Key ist wiederum als Hex Ziffer geschrieben, jedoch im NTP Standard Format mit dem höchwertigen Bit (HSB) jedes Octets als das ungerade Parity Bit. Ein mit **M** gekennzeichnete Key ist ein MD5 Key mit bis zu 31 ASCII Zeichen. Zu Beachten ist, dass die Zeichen ' ', '#', '\t', '\n' und '\0' weder im DES noch im MD5 ASCII Key verwendet werden können! Key 0 (zero) ist reserviert für spezielle Zwecke und sollte deshalb hier nicht auftauchen. Vom Lantime werden über das Benutzerinterface nur MD5 Keys unterstützt.

## **NTP Autokey**

NTP Version 4 unterstützt neben den symmetrischen Schlüsseln zusätzlich noch das sogenannte Autokey-Verfahren. Die Echtheit der empfangenen Zeit auf den NTP-Clients wird durch symmetrische Schlüssel sehr gut sichergestellt. Allerdings ist für eine höhere Sicherheit der periodische Austausch der verwendeten Schlüssel nötig, um einen Schutz, z.B. vor Replay-Attacken (d.h. Angriffen, bei denen aufgezeichneter Netzwerkverkehr einfach noch einmal abgespielt wird), zu erreichen.

Bei Netzwerken mit sehr vielen Clients kann dieses Austauschen der symmetrischen Schlüssel allerdings mit sehr viel Aufwand verbunden sein, weil auf jedem Client die Schlüssel für den/die NTP Server ausgetauscht werden müssen. Aus diesem Grund wurde von den NTP Entwicklern das Autokey-Verfahren eingeführt, das mit einer Kombination aus Gruppenschlüsseln (group keys) und öffentlichen Schlüsseln (public keys) arbeitet. Alle NTP Clients können somit die Zeitangaben, die sie von Servern ihrer eigenen Autokey-Gruppe erhalten, auf Echtheit überprüfen.

Beim Autokey-Verfahren werden sogenannte sichere Gruppen (secure groups) gebildet, in denen NTP Server und Clients zusammengefasst sind. Es gibt drei verschiedene Typen von Mitgliedern in einer solchen Gruppe:

### **a) Trusted Host**

Ein oder mehrere vertrauenswürdige NTP Server. Um diesen Status zu erhalten, muss der Server ein als „Trusted“ gekennzeichnetes selbst-signiertes Zertifikat besitzen. Er sollte auf dem niedrigsten Stratum Level der Gruppe operieren.

### **b) Host**

Ein oder mehrere NTP Server, die kein „Trusted“-Zertifikat besitzen, sondern nur ein selbstsigniertes Zertifikat (ohne die „Trusted“-Kennzeichnung).

### **c) Client**

Ein oder mehrere NTP-Client-Systeme, die im Gegensatz zu den beiden erstgenannten Typen die Zeit lediglich empfangen und nicht in der Gruppe weiterverteilen. Alle Mitglieder der Gruppe (Trusted Hosts, Hosts und Clients) müssen im Besitz des gleichen Gruppenschlüssels sein. Der Gruppenschlüssel wird von einer Trusted Authority (TA) generiert und muss dann manuell auf alle Gruppenmitglieder verteilt werden (auf einem sicheren Weg, z.B. mittels scp). Die Rolle der TA kann ein Trusted Host in der Gruppe übernehmen (zum Beispiel ein Lantime), es ist aber auch ohne Probleme möglich, den Gruppenschlüssel von einem nicht der Gruppe zugehörigen TA-Host erzeugen zu lassen.

Die verwendeten Public Keys können auf den Trusted Hosts der Gruppe periodisch manuell neu erzeugt werden (das ist sowohl im Webinterface als auch über das CLI-Setupprogramm möglich, über den Punkt „Generate new NTP public key“ im Bereich „NTP Autokey“ auf der Seite „Security Management“) und damit dann automatisch an alle anderen Mitglieder der Gruppe verteilt werden. Der Gruppenschlüssel bleibt



gleich und somit entfällt das manuelle Update von Schlüsseln für alle Gruppenmitglieder.

Ein Lantime kann in einer solchen Autokey-Gruppe sowohl TA und Trusted Host als auch einfacher Host sein.

Um den Lantime als TA und Trusted Host zu konfigurieren, schalten Sie das Autokey-Verfahren ein und initialisieren Sie per HTTPS-Webinterface den Gruppenschlüssel („Generate groupkey“). Dafür ist ein Crypto-Passwort nötig, das Sie ebenfalls im Webinterface ändern können. Den so erzeugten Gruppenschlüssel müssen Sie dann vom Lantime herunterladen (z.B. über das HTTPS-Webinterface) und dann auf alle Clients und weiteren NTP Server der Gruppe kopieren (und diese Systeme ebenfalls für die Verwendung von Autokey konfigurieren).

Die ntp.conf aller Gruppenmitglieder muss folgende Zeilen enthalten:

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

Dabei ist „cryptosecret“ in diesem Fall das Crypto-Passwort, das zum Erstellen des Group Keys und aller Public Keys verwendet wurde. Bitte beachten Sie, dass das Crypto-Passwort im Klartext in der ntp.conf steht und somit auf Nicht-Lantime-Systemen sichergestellt sein sollte, dass nur „root“ diese Datei einsehen kann.

Die Clients müssen zusätzlich noch den Eintrag der verwendeten NTP-Server ergänzen, um eine Nutzung von Autokey in Verbindung mit diesen Servern einzuschalten. Das sieht z.B. so aus:

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

In diesem Beispiel wird der NTP Server time.meinberg.de mit Autokey verwendet, während time2.meinberg.de ohne jegliche Überprüfung der Echtheit der Zeit akzeptiert wird.

Möchten Sie den Lantime zwar als Trusted Host verwenden, aber eine andere TA nutzen, dann erzeugen Sie mithilfe dieser Trusted Authority einen Gruppenschlüssel und binden ihn z.B. mithilfe des Webinterfaces auf Ihrem Lantime ein (auf Seite „Security Management“ im Bereich „NTP autokey“ den Menüpunkt „Upload groupkey“).

Wenn Sie den Lantime als einfachen NTP Server (nicht „trusted“) verwenden möchten, dann müssen Sie den Gruppenschlüssel Ihrer Gruppe hochladen („Security Management“ / „NTP autokey“ / „Upload groupkey“) und ein eigenes, selbstsigniertes Zertifikat erzeugen (ohne es als „Trusted“ zu markieren). Da beim Generieren eines Zertifikats über das Webinterface oder das CLI-Setupprogramm grundsätzlich immer als „Trusted“ markierte Zertifikate erstellt werden, müssen Sie zum Erstellen von Zertifikaten ohne „Trusted“-Merkmal das Programm ntp-keygen manuell auf dem Lantime aufrufen (in einer SSH-Sitzung):

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

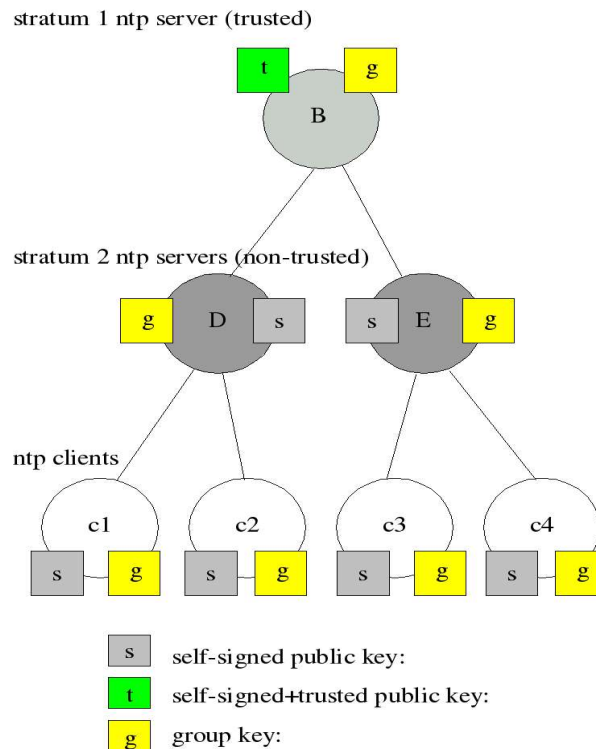
Anschließend müssen die neu generierten ntpkeys manuell auf die Flash Disk kopiert werden:

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

Auch hier ist „cryptosecret“ wieder das verwendete Crypto-Passwort, das mit dem Crypto-Passwort in der ntp.conf übereinstimmen muss.

Eine detaillierte Anleitung zu ntp-keygen finden Sie auf der NTP-Homepage (<http://www.ntp.org>).

Beispiel:



Diese Autokey-Gruppe besteht aus einem Stratum-1-Server (B) sowie zwei Stratum-2-Servern (D, E) und mehreren Clients (im Schaubild sind 4 Clients abgebildet, c1 - c4). B ist der Trusted Host der Gruppe. Er besitzt den Gruppenschlüssel sowie ein als „Trusted“ gekennzeichnetes, selbstsigniertes Zertifikat.

D und E sind NTP Server, die als Hosts der Gruppe nicht Trusted sind. Sie besitzen den Gruppenschlüssel und ein selbstsigniertes Zertifikat (das nicht als „Trusted“ markiert wurde). Die Clients besitzen jeweils den Gruppenschlüssel und ebenfalls ein selbstsigniertes Zertifikat.

Um die gesamte Gruppe mit neuen Schlüsseln zu versorgen, muss lediglich auf B ein neuer „t“-Schlüssel generiert werden. Er wird dann automatisch an D und E verteilt, die dann gegenüber den Clients eine ununterbrochene Kette von Zertifikaten bis zu einem Trusted Host nachweisen können und somit als glaubwürdig eingestuft werden.

Mehr über die technischen Hintergründe und genauen Abläufe des Autokey-Verfahrens können Sie auf der NTP-Homepage (<http://www.ntp.org>) nachlesen.

# Konfiguration: Lokal



- Ethernet
- Benachrichtigung
- Sicherheit
- NTP
- Lokal
- Statistik
- Handbuch
- Hauptmenü

## Lokale Konfiguration

### Lantime Dienste:

- Lantime neu starten
- Manuelle Konfiguration
- Sende Testbenachrichtigungen
- NTP Drift Datei sichern
- Auslieferungszustand herstellen
- SNMP MIB Dateien herunterladen

### Lantime Benutzerverwaltung:

- Benutzer administrieren

### Lantime Informationen anzeigen:

- Alle Meldungen anzeigen
- Versionsinformationen anzeigen
- Lantime Optionen anzeigen
- GPS Informationen anzeigen

### Lantime Firmware update:

- Durchsuchen...
- Firmware update starten

### Lantime Konfiguration:

- Konfiguration prüfen
- Diagnose-Informationen speichern

### Allgemeine Informationen:

- Kontakt:
- Standort:
- Sprache des WEB-Interface:

Speichern

Zurücksetzen

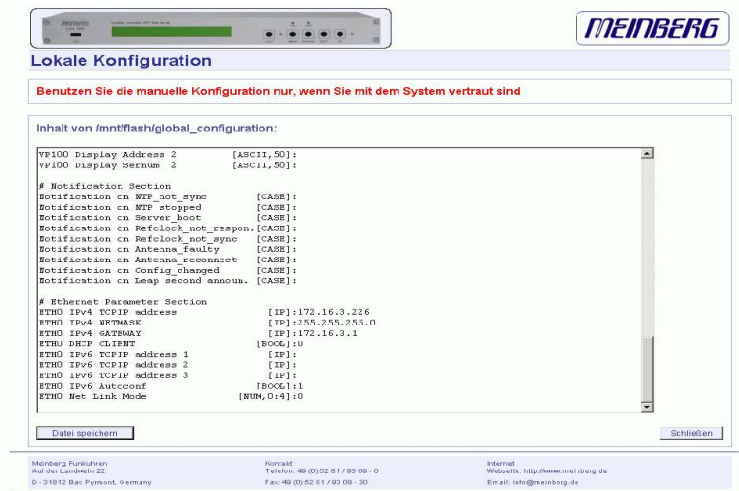
Zurück

[ top ]

## Administrative Funktionen

Im ersten Abschnitt werden verschiedene Funktionen für den Administrator zur Verfügung gestellt. Über den Punkt „Lantime neu starten“ wird ein Shutdown auf dem System ausgeführt. Das System braucht ca. eine halbe Minute für den Bootvorgang. Die Referenzuhr bekommt damit keinen RESET.

Über den Punkt „Manuelle Konfiguration“ gelangt man in ein Editierfenster, worin die gesamte Konfiguration (siehe Anhang) editiert werden kann. Beim Beenden dieses Fensters wird gefragt, ob die geänderte Konfiguration dann aktiviert werden soll.



Über den Punkt „Sende Testbenachrichtigung“ wird eine Test Alarmmeldung für alle konfigurierten Aktionen erzeugt. D.h., wenn in der Ereigniskonfiguration eine E-Mail-Adresse korrekt eingestellt wurde, wird an diese eine Test-E-Mail gesendet.

Über den Punkt „NTP Drift Datei speichern“ wird die Datei /etc/ntp.drift auf der Flashdisk abgespeichert. NTP benutzt dieses Driftfile, um die Kompensation der Ungenauigkeit der Rechneruhr nach einem Neustart des NTP direkt zur Verfügung zu haben. Dadurch schwingt sich der NTP schneller ein. Dieser Wert sollte nur dann gespeichert werden, wenn der NTP für längere Zeit (> ein Tag) sich auf die Referenzuhr synchronisiert hat. Dieses wird einmal bei der Auslieferung des Gerätes im Werk ausgeführt.

Über den Punkt „Auslieferungszustand herstellen“ werden alle Einstellungen auf den Auslieferungszustand zurückgesetzt. Dabei wird die alte Konfiguration unter /mnt/flash/global\_configuration.old gespeichert und dann durch die Datei /mnt/flash/factory.conf ersetzt. Dabei wird auch das Standard Passwort „timeserver“ wieder aktiviert. Nach diesem Vorgang sollten alle Zertifikate neu gesetzt werden, weil auch der Hostname geändert wurde.

Über den Punkt „SNMP MIB Dateien herunterladen“ können alle Meinberg SNMP MIB Dateien, die speziell für den LANTIME angepasst wurden, als ZIP Datei heruntergeladen werden, um diese dann bei einem SNMP Manager zu installieren.

## Benutzerverwaltung

Zur Administration des LANTIME können eigene Benutzer angelegt werden. Dabei werden 3 Benutzergruppen unterschieden. Die Gruppe „Super-User“ hat alle Rechte zur Administration. Die Gruppe Administrator kann nur über die Benutzerschnittstellen HTTP und das Comand Line Interface (CLI) über Telnet, SSH oder Terminal Änderungen vornehmen; beim Einloggen über eine Kommandozeile wird direkt das Setup Interface gestartet und beim Beenden wird die Session direkt geschlossen. Somit hat der Administrator keinen direkten Zugriff auf Linux Befehle. Die Benutzergruppe Info hat die gleichen Einschränkungen wie der Administrator und kann zusätzlich keine Veränderungen an der Konfiguration vornehmen.

**MEINBERG**

Ethernet Benachrichtigung Sicherheit NTP Lokal Statistik Handbuch Hauptmenü

### Lokale Konfiguration

Benutzerverwaltung:

Benutzer hinzufügen:

Passwort:

Gruppenzugehörigkeit:  Super-User  
 Administrator  
 Info

Vorhanden Benutzer:

| Benutzername | Gruppe     | Option  |
|--------------|------------|---|
| root         | Super-User |   |
| gast         | Info-User  | <input type="button" value="Benutzer löschen"/> |
| admin        | Admin-User | <input type="button" value="Benutzer löschen"/> |

Meinberg Funkuhren GmbH & Co. KG  
Johf. Aul. Landwehr 22  
D - 31812 Bad Pyrmont, Germany

Kontakt:  
Telefon: +49 (0) 52 81 / 93 00 - 0  
Fax: +49 (0) 52 81 / 93 00 - 30

Internet:  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

Über die Benutzerverwaltung können neue Benutzer jeweils mit Passwort und Gruppenzugehörigkeit angelegt und gelöscht werden. Zum Ändern eines Benutzers muß dieser erst gelöscht und dann neu angelegt werden. Im unteren Teil der Benutzerverwaltung wird eine Liste aller Benutzer angezeigt. Der Benutzer „root“ ist fest vorgegeben und hat immer Super-User Rechte. Das Passwort von „root“ kann nur über die Seite Sicherheit/Login geändert werden.

## Administrative Informationen

Über den Punkt „Alle Meldungen anzeigen“ wird die aktuelle SYSLOG Datei angezeigt. In dieser Datei werden von allen Programmen, wie auch von dem aktuellen Betriebssystem Kernel, die Meldungen abgelegt. In einem extra Fenster wird die gesamte Datei /var/log/messages angezeigt. Diese Datei steht in der RAM-DISK und wird nach jedem Neustart gelöscht. Ist ein externer SYSLOG-Server konfiguriert, werden alle Lantime SYSLOG-Einträge dort hin gesendet und können so dauerhaft gespeichert werden.

**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 `tty1' from  
 `172.16.3.45'  
 Mar 15 14:01:17 LanGpsV4 login[15711]: root login on `tty1' from `172.16.3.45'

Der Punkt „Versionsinformationen anzeigen“ zeigt die aktuelle Version des LANTIME und der Softwarekomponenten an.



Der Punkt „Lantime Optionen anzeigen“ zeigt die Optionen der integrierten Komponenten an.



## Software Update

Über den Punkt „Lantime Firmware update“ kann ein automatisches Update auf dem LANTIME gestartet werden. Dazu wird eine spezielle Datei von der Firma Meinberg benötigt, um ein solches Update auszuführen. Über den Schalter „Browse“ kann die Update Datei auf dem lokalen PC ausgewählt werden. Diese wird auf den LANTIME herunter geladen und nach einer erneuten Abfrage wird dann das Update gestartet. Welche Software auf dem LANTIME damit erneuert wird, hängt nur von der Update Datei ab.



The screenshot shows a software update confirmation dialog box. At the top right is the **MEINBERG** logo. Below it is a header bar with the text **Lokale Konfiguration**. The main area contains the question: "Soll die nachstehende Aktion wirklich ausgeführt werden?". Below this is a line of text: "lantime update - wenn Sie ein Voll-Update durchführen , müssen sie danach das Gerät neu starten". At the bottom of the main area are two buttons: "OK" on the left and "ABBRUCH" on the right. Below the main area is a footer bar with contact information:

|   |  |  |
|---|--|--|
| Meinberg Funkuhren<br>Auf der Landwehr 22<br>D - 31812 Bad Pyrmont, Germany | Kontakt<br>Telefon: +49 (0) 52 81 / 93 09 - 0<br>Fax: +49 (0) 52 81 / 93 09 - 30 | Internet<br>Webseite: <a href="http://www.meinberg.de">http://www.meinberg.de</a><br>Email: <a href="mailto:info@meinberg.de">info@meinberg.de</a> |
|---|--|--|

## Automatische Konfigurationsprüfung

Über den Punkt „Konfiguration prüfen“ können alle aktuellen Einstellungen des Zeitserverns getestet werden. Dabei werden alle Werte auf Plausibilität geprüft und alle eingestellten IP-Adressen auf Erreichbarkeit. Alle Werte, die rot gekennzeichnet werden, sollten besonders geprüft werden. Es wird auch die Erreichbarkeit der eingestellten IP-Adressen geprüft – dies kann u.U. einiges an Zeit beanspruchen.



### Lokale Konfiguration

#### Prüfen der Konfiguration

##### Ethernet:

|               |                 |    |
|---------------|-----------------|----|
| Hostname:     | lantimeGregoire | ok |
| Nameserver 1: | 172.16.3.1      | ok |
| IPv4 Gateway: | 172.16.3.1      | ok |

##### Ethernet interface 0:

|                 |                 |    |
|-----------------|-----------------|----|
| TCP/IP address: | 172.16.3.228    | ok |
| Netmask:        | 255.255.255.000 | ok |

##### Benachrichtigung:

|               |                            |    |
|---------------|----------------------------|----|
| To address:   | gregoire.diehl@meinberg.de | ok |
| From address: | LantimeGregoire            | ok |
| CC:           | info@meinberg.de           | ok |
| Smarthost:    | gateway                    | ok |

##### NTP:

|                                |              |    |
|--------------------------------|--------------|----|
| External NTP server address 1: | 172.16.3.227 | ok |
|--------------------------------|--------------|----|

#### Prüfe die Erreichbarkeit jeder eingetragenen Adresse

##### Ethernet:

|               |            |           |
|---------------|------------|-----------|
| Nameserver 1: | 172.16.3.1 | reachable |
| IPv4 Gateway: | 172.16.3.1 | reachable |

##### Benachrichtigung:

|                   |         |           |
|-------------------|---------|-----------|
| E-Mail Smarthost: | gateway | reachable |
|-------------------|---------|-----------|

##### NTP:

|                                |              |           |
|--------------------------------|--------------|-----------|
| External NTP server address 1: | 172.16.3.227 | reachable |
|--------------------------------|--------------|-----------|

Zurück

[ top ]

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

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

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)



## **Diagnose Informationen speichern**

Mit Hilfe der Service Informationen kann der technische Support der Firma Meinberg sich ein genaues Bild von dem aktuellen Zustand Ihres Lantime machen. Nach der Aktivierung dieses Buttons werden alle Konfigurationsdateien und Einstellungen des Lantimes in einer Textdatei zusammengefasst und gepackt. Dieses Zusammenstellen der Informationen kann einige Zeit dauern; drücken Sie nicht nochmals den Button, während dieses Vorgangs, da einige Webbrowser den Vorgang abbrechen. Danach kann eine Datei „config.zip“ herunter geladen und auf dem lokalen PC gespeichert werden. Diese Datei sollten Sie bei Fragen oder Problemen mit Ihrem Lantime an die Service Mitarbeiter als Anhang einer Mail zusenden und dabei Ihr Problem genau beschreiben.

## **Sprache des WEB-Interface**

Über den Punkt „Sprache des WEB-Interface“ kann die Ausgabe der Texte in der HTTP Benutzerschnittstelle auf Deutsch oder Englisch eingestellt werden. Die Änderung erfolgt beim nächsten Neuladen der aktuellen Seite.

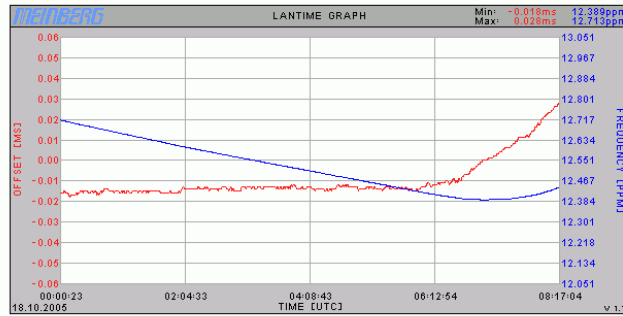
# Konfiguration: Statistik



- Ethernet
- Benachrichtigung
- Sicherheit
- NTP
- Lokal
- Statistik
- Handbuch
- Hauptmenü

## Statistik

Statistik:



Verfügbare Logdateien:

Loopstats zusammenführen

### Lantime Information:

S/N: n/a  
 GPS167 :4.14 S/N:10071930  
 NTP Version: 4.2.0b@1.1409-o Mon Oct 17 08:47:14 UTC 2005 (1)  
 Kernel Version: 2.6.12  
 System Version: 502  
 ETHERNET HWaddr 00:E0:4B:0C:13:4C  
 Uptime: 21 h  
 Mem free: 0 kB  
 Disk free: 18378 kb

### Ausgabe des Befehls "ntpq -p":

| remote      | refid    | st | t | when | poll | reach | delay | offset | jitter |
|-------------|----------|----|---|------|------|-------|-------|--------|--------|
| LOCAL(0)    | LOCAL(0) | 12 | I | 40   | 64   | 377   | 0.000 | 0.000  | 0.004  |
| +GENERIC(0) | .GPS.    | 0  | I | 42   | 64   | 377   | 0.000 | 0.027  | 0.004  |
| oPPS(0)     | .PPS.    | 0  | I | 13   | 64   | 377   | 0.000 | 0.028  | 0.004  |

### Ausgabe des Befehls "ntpq -c 'cv assID'":

```

device="Meinberg GPS16x receiver",
timecode="w0218.10.05; 2; 08:17:17; +00:00; ; 51.9827N 9.2258E 174mx03vx00",
poll=1190, noreply=0, badformat=0, baddata=0, fudgetime1=4.400,
stratum=0, refid=GPS, flags=4,
refclock_ppstime="c6ff2e0c.fffe7dc0 Tue, Oct 18 2005 8:17:16.999",
refclock_time="c6ff2e0d.00000000 Tue, Oct 18 2005 8:17:17.000",
refclock_status="UTC DISPLAY; TIME CODE; PPS; POSITION; (LEAP INDICATION; PPS SIGNAL; POSITION)",
refclock_format="Meinberg GPS Extended",
refclock_states=""NOMINAL: 21:19:30 (100.00%); running time: 21:19:30"
    
```

### NTP Zugriffsinformation:

| fernadresse | port | lokale Adresse | anzahl | m | ver | code | avglen | erste |
|-------------|------|----------------|--------|---|-----|------|--------|-------|
| 127.0.0.1   | 3968 | 127.0.0.1      | 108496 | 7 | 2   | 0    | 0      | 0     |
| 172.16.3.13 | 123  | 172.16.3.226   | 1434   | 3 | 4   | 0    | 16     | 4     |
| 172.16.3.5  | 123  | 172.16.3.226   | 228    | 3 | 4   | 0    | 896    | 419   |
| 172.16.3.79 | 123  | 172.16.3.226   | 206    | 3 | 4   | 0    | 83     | 60945 |

Anzahl Clients: 4

[Zurück](#)

[ top ]

## Statistik Informationen

Im ersten Abschnitt wird eine grafische Darstellung des Fortschrittes der Synchronisation dargestellt. NTP speichert diese Statistik Informationen in so genannten „Loopstats“ Dateien ab, welche hier grafisch als Kurve dargestellt wird. Die rote Linie beschreibt den Offset zwischen der Referenzuhr (GPS) und der Systemzeit. Die blaue Linie gibt den Frequenzfehler der Systemzeit wieder (PPM, parts per million). Oben rechts in der Grafik sind die Messbereiche der roten und der blauen Linie dargestellt. Es können maximal 24 Stunden dargestellt werden. War das LANTIME längere Zeit in Betrieb kann im Auswahlfeld unter der Grafik einer der letzten 10 Tage dargestellt werden. Über den Punkt „Loopstats zusammenführen“ werden alle vorhandenen „Loopstats“ Dateien zu einer Datei zusammengefasst und in einer Grafik dargestellt. Damit ist es möglich den gesamten Verlauf der maximal letzten 10 Tage darzustellen. Alle Zeitangaben beziehen sich auf UTC.

Im nächsten Teil werden Informationen über die Versionsnummer der Lantime Software, der GPS Software und des Betriebssystems sowie Kundeninformation und die Hardware Adresse (MAC address) der ersten Netzwerkschnittstelle angezeigt. Danach werden Speicher- und Diskinformationen angezeigt. Der **Mem free** Parameter gibt die aktuellen Speicherplatz an. Der gesamte verfügbare Speicher beträgt 32 MB und wird dynamisch vom Betriebssystem verwaltet. Der **Disk free** Parameter gibt die aktuell freie Speicherkapazität der RAM-Disk wieder. Die RAM-Disk hat eine Kapazität von 32 MB. Der **Uptime** Parameter zeigt dem Benutzer, wie lange das System nach dem letzten Booten schon läuft.

Im nächsten Abschnitt werden in einer Liste die Zugriffe von allen Benutzern aufgelistet, die auf den NTP des Zeitservers zugegriffen haben: also eine Liste aller NTP-Clients. Diese kann sehr lang werden. Benutzer, die lange nicht mehr auf den NTP zugegriffen haben, werden automatisch gelöscht. Diese Liste wird automatisch von NTP intern verwaltet. Genauere Informationen zu den Parametern „code, avglen und first“ konnten wir derzeit nicht finden. Eine Namensauflösung der IP Adressen konnten wir nicht aktivieren, da die dafür beanspruchte Zeit zu großen Antwortverzögerungen führt.

Darunter befindet sich die Ausgabe von dem Befehl „ntpq -p“, welcher eine Liste aller aktuellen Referenzuhren(peers) des NTP anzeigen.

### Folgende Informationen werden angezeigt:

---

|           |   |
|-----------|---|
| - remote: | Auflistung aller verfügbaren Zeit-Server (ntp.conf)   |
| - refid:  | Referenznummer  |
| - st:     | aktueller Stratum-Wert (Hierarchieebene)  |
| - when:   | wann die letzte Abfrage stattgefunden hat<br>(in Sekunden)  |
| - poll:   | in welchem Intervall der Zeitserver abgefragt wird  |
| - reach:  | oktale Darstellung eines 8 Bit Speichers, in welchem die erfolgreichen Abfragen von rechts nach links geshiftet werden. |
| - delay:  | gemessene Verzögerung der Netzwerkübertragung<br>(in Millisekunden)   |
| - offset: | Differenz zwischen Systemzeit und Referenzzeit<br>(in Millisekunden)  |
| - jitter: | statistische Streuung des Offsets (in Millisekunden)  |

Im letzten Abschnitt werden NTP spezifische Informationen zur eingebauten Referenzuhr ausgegeben. Neben dem aktuellen und dem alten Status wird der Name der Referenzuhr und der letzte empfangene Zeitstring und die Laufzeiten aufgeschlüsselt nach dem Status „NOMINAL“ und „FAULT“.

## Konfiguration: Handbuch

The screenshot shows the 'Manual' configuration page for Meinberg. It features a 'MEINBERG' logo at the top right. The page is divided into two main sections: 'Verfügbare Dokumente:' and 'Eigene Notizen:'. The 'Verfügbare Dokumente:' section contains a table with columns for Dateiname, Sprache, Typ, Datum, Größe, and Option. Two documents are listed: '1he\_langps\_ebt\_v4' (german, pdf, 2005-01-05, 2266.22kb) and '1he\_langps\_ebt\_v4\_e' (english, pdf, 2005-01-05, 2451.00kb). Below the table, there is a note about Adobe's Acrobat Reader and a 'herunterladen' link. The 'Eigene Notizen:' section contains a table with columns for Dateiname, Sprache, Typ, Datum, Größe, and Optionen. One note is listed: 'Wartungs Informationen' (de, txt, 2005-01-05, 0.11kb). Below the table, there is a 'Notiz hinzufügen' button and a 'Zurück' button. At the bottom, there is contact information for Meinberg Funkuhren, including address, phone, fax, internet, website, and email.

| Dateiname           | Sprache | Typ | Datum      | Größe     | Option                        |
|---------------------|---------|-----|------------|-----------|-------------------------------|
| 1he_langps_ebt_v4   | german  | pdf | 2005-01-05 | 2266.22kb | <a href="#">herunterladen</a> |
| 1he_langps_ebt_v4_e | english | pdf | 2005-01-05 | 2451.00kb | <a href="#">herunterladen</a> |

2 Dokumente verfügbar

Sie benötigen Adobe's Acrobat Reader, um die meisten Dokumente zu öffnen [herunterladen](#)

| Dateiname              | Sprache | Typ | Datum      | Größe  | Optionen  |
|------------------------|---------|-----|------------|--------|---|
| Wartungs Informationen | de      | txt | 2005-01-05 | 0.11kb | <a href="#">anzeigen</a> <a href="#">bearbeiten</a> <a href="#">löschen</a> |

[Notiz hinzufügen](#) [Zurück](#)

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

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

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

In dieser Konfiguration werden die Dokumentationen für den LANTIME und die Benutzer spezifischen Notizen verwaltet. Im oberen Teil werden die einzelnen Handbücher zum Download für dieses Gerät zur Verfügung gestellt. Dabei wird der Name der Dokumentation, die jeweilige Sprache, der Typ der Datei (z.B. Textdatei oder PDF Datei), das Datum, die Größe in Bytes und zusätzliche Optionen angezeigt. Über den Punkt „download“ kann jedes Dokument herunter geladen werden und mit einem lokalen Textverarbeitungsprogramm oder PDF-Viewer angezeigt werden.

Im zweiten Teil werden die frei definierbaren Notizen angezeigt. Hier können vom Benutzer frei zugängliche Notizen und Anmerkungen abgelegt werden. Über den Punkt „anzeigen“ wird die Datei in einem Fenster angezeigt. Über den Punkt „Bearbeiten“ wird die jeweilige Notiz bearbeitet und über „Löschen“ wird diese gelöscht.

The screenshot shows the 'Manual' configuration page for Meinberg, displaying the content of a user note. The page features a 'MEINBERG' logo at the top right. The main content area shows the text of the note: 'Inhalt von [www.manual/customer/de/Wartungs Informationen.txt](http://www.manual/customer/de/Wartungs Informationen.txt):  
17.12.2004 Inbetriebnahme des Zeitservers  
20.12.2004 Freigabe des Zeitservers  
21.12.2004 alle Urlaub'. Below the text, there is a 'Schließen' button. At the bottom, there is contact information for Meinberg Funkuhren, including address, phone, fax, internet, website, and email.

Inhalt von [www.manual/customer/de/Wartungs Informationen.txt](http://www.manual/customer/de/Wartungs Informationen.txt):

17.12.2004 Inbetriebnahme des Zeitservers  
20.12.2004 Freigabe des Zeitservers  
21.12.2004 alle Urlaub

[Schließen](#)

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

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

Internet  
Webseite: <http://www.meinberg.de>  
Email: [info@meinberg.de](mailto:info@meinberg.de)

Über den Punkt „Notiz hinzufügen“ wird eine neue Notiz angelegt. In einem Menü muss man dazu den Namen der Datei angeben, unter der diese Notiz gespeichert werden soll (ohne Pfadangabe) und zusätzlich noch die Angabe in welcher Sprache die Notiz verfasst wird.

## Das Kommandozeilen Interface

Das Kommandozeilen Interface (CLI Comand-Line-Interface) kann über eine TELNET oder SSH Verbindung geöffnet werden, indem mit Hilfe des Programms "setup" eine Blockzeichen orientierte Benutzerschnittstelle gestartet wird.

```
LANTIME CONFIGURATION UTILITY 1.01
Lantime: MGX/RDT 1HE V4.13          S/N: n/a
Host: LanRDTv4                    Uptime: 40 min
Domain: py.meinberg.de            Notification: DISABLED

IPv4: 172.16.3.237      IPv6: fe80::2e0:4bff:fe06:fb88/10 (LL)

RDT STATUS: ext. NTP server          Date: Tue, 31.08.2004
NTP STATUS: Offset EXT: -18ms       Time: 10:08:01

Receiver information: n/a

Last Messages:
31.08.04 09:32:58 UTC: lantime -> NTP sync to external NTP server
31.08.04 09:31:51 UTC: lantime -> NTP sync to local
31.08.04 09:28:33 UTC: lantime -> lantime rebooted

Configuration & Management:
Ethernet  Notification  Security  nTp  Local  eXit
```

Diese Seite gibt einen kurzen Überblick über die wichtigsten Einstellungen und Laufzeitparameter des Gesamtsystems. Oben links ist die LANTIME Variante mit der Versionsnummer für die LANTIME Software, wobei es sich um einen übergeordneten Softwarestand aller enthaltenen Module und Software Pakete handelt. Darunter wird der aktuelle Hostname und Domainname im Netzwerk geschrieben. Rechts daneben wird die Seriennummer (wie auf dem silbernen Aufkleber auf der Rückseite des Gerätes) und die IPv4 und IPv6 Adresse des ersten Ethernet Anschlusses.

Im zweiten Abschnitt wird der Status der Referenzuhr und des NTP wie oben schon beschrieben angezeigt, sowie zusätzliche Informationen zur Referenzuhr. Auf der rechten Seite wird die Uptime des gesamten Systems seit dem letzten Neustart des LANTIMES angezeigt.

Im dritten Abschnitt werden die letzten Meldungen der Systemsoftware protokolliert und mit einem Zeitstempel dargestellt. Die letzten Einträge sind dabei immer ganz oben. Diese Ausgabe entspricht der Datei "/var/log/lantime\_messages", die nach jedem Neustart neu erstellt wird.

Über die Buttons im unteren Teil gelangt man in die unten beschriebenen Untermenüs.

## 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   <SMB>          DISABLED
               <SNMP>          ENABLED

<IPv6 protocol:> ENABLED

Ethernet 0

SAVE  CLOSE
```

In der Netzwerk Konfiguration werden alle Parameter bezüglich der Netzwerkschnittstellen konfiguriert. Im ersten Abschnitt werden der Hostname, der Domainname, zwei Nameserver und zwei Syslogserver eingetragen. Bei den Nameservern und Syslogservern können wahlweise IPv4- oder IPv6-Adressen eingetragen werden.

Alle Informationen die auf dem LANTIME in das SYSLOG (/var/log/messages) geschrieben werden, können auf einen entfernten Server umgeleitet werden. Der Syslog Dämon des entfernten Servers muss entsprechend auf Empfang geschaltet werden, z.B. unter LINUX mit "syslogd -r", um die Syslog-Messages von anderen Servern empfangen zu können.

In der Konfiguration können unter dem Menüpunkt ETHERNET zwei IP Adressen für SYSLOG Server angegeben werden. Sind beide Adressen auf 0.0.0.0 gesetzt wird der REMOTE SYSLOG-Dienst nicht gestartet.

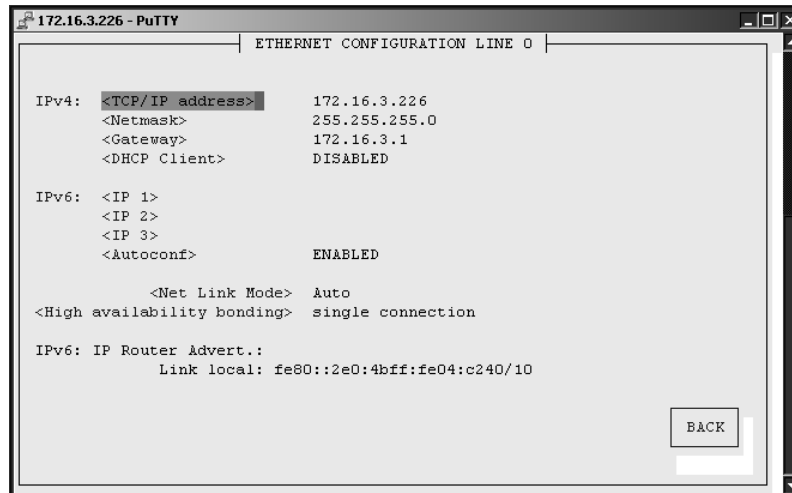
Beachten Sie, dass alle SYSLOG Ausgaben auf dem Zeitserver unter var/log/messages gespeichert werden und somit nach einem Neustart des Systems gelöscht sind. Ein täglicher CRON Job prüft die Größe der Logg-Dateien und löscht diese, wenn sie zu groß werden.

Im zweiten Abschnitt kann jeweils für IPv4 und IPv6 ein Default Gateway eingetragen werden.

Im dritten Abschnitt werden die möglichen Netzwerkprotokolle angezeigt: TELNET, FTP, SSH, HTTP, HTTPS, SNMP und NETBIOS. Die einzelnen Protokolle können über die Check-Boxen aktiviert oder deaktiviert und werden direkt nach dem Abspeichern entsprechend gestartet oder beendet.

Im vierten Abschnitt können die Internet Protokolle IPv4 und IPv6 ausgewählt werden. Derzeit ist das IPv4 Protokoll noch zwingend notwendig und kann nicht

abgeschaltet werden. Ein reiner IPv6 Betrieb kann nur dadurch erreicht werden, in dem alle IPv4 Adressen aller Netzwerkanschlüsse auf Null gesetzt werden und gleichzeitig das DHCP für IPv4 abgeschaltet wird. In diesem Fall wird auf dem Zeitserver keine IPv4 Adresse konfiguriert und man kann nur über IPv6 auf das Gerät zugreifen. TELNET, FTP und NETBIOS sind derzeit nicht über IPv6 möglich. IPv4 und IPv6 können im Mischbetrieb aktiviert werden.



Hier werden die Parameter für die Netzwerkanschlüsse konfiguriert. Für jeden physikalischen Netzwerkanschluss (RJ45 Buchse) steht eine solche Seite zur Verfügung. Es können maximal 9 Seiten je nach Hardwareausstattung in diesem Menü erscheinen. Oben auf der Seite stehen die Einstellungen für IPv4 und weiter unten die für IPv6. Ist kein DHCP Client Betrieb für IPv4 aktiviert, so kann manuell eine IP Adresse für den jeweiligen Netzwerkanschluss eingestellt werden. IPv4 Adressen bestehen aus 32 Bit und werden mit 4 dezimalen Werten zwischen 0 bis 255, durch jeweils einen Punkt getrennt, eingegeben:

Beispiel: 192.168.10.2

Bitte wenden Sie sich an Ihren Netzwerk Administrator, der Ihnen eine gültige IPv4 Adresse speziell für Ihr Netzwerk vergibt. Ebenso verfahren Sie mit der Netzmaske.

Falls sich ein DHCP Server (Dynamik Host Configuration Protocol) im Netz befindet, kann die Netzwerkeinstellung auch automatisch vorgenommen werden. Um den DHCP Client des LANTIME zu aktivieren, muss 000.000.000.000 als TCP/IP Adresse im LC-Display eingetragen (Auslieferungszustand) oder hier die entsprechende Checkbox aktiviert werden. Die Netzwerkeinstellungen werden dann automatisch von einem DHCP Server (muss sich bereits im Netzwerk befinden) vorgenommen. Die MAC-Adresse der Netzwerkkarte wird nach zweimaligem Drücken der NEXT Taste im Hauptmenü angezeigt. Im Untermenü "Setup Lan Parameter: TCP/IP Adresse" wird die vom DHCP Server vergebene Adresse angezeigt. Der DHCP Client vom LANTIME ist nur für das IPv4 Netzwerk Protokoll einsetzbar. Über das HTTP-Interface oder das Setup Programm kann der DHCP Client über einen Schalter ein- und ausgeschaltet werden. Damit ist es auch möglich



das IPv4-Interface zu deaktivieren, wenn man als TCP/IP Adresse eine 000.000.000.000 einträgt und den DHCP abschaltet.

Wurde der DHCP Client für den Netzwerkanschluss aktiviert, werden die vom DHCP Server automatisch vergebenen IP Adressen in den entsprechenden Feldern angezeigt.

Auf der rechten Seite werden die Einstellungen für das IPv6-Protokoll eingetragen oder angezeigt. Dabei sind 3 globale IPv6-Adressen möglich. IPv6-Adressen haben 128 Bits und werden als Kette von 16-bit-Zahlen in Hexadezimal-Notation geschrieben, die durch Doppelpunkte getrennt werden. Folgen von Nullen können einmalig durch "::" abgekürzt werden.

Beispiel:

```
"::" ist die Adresse, die nur aus Nullen besteht.  
"::1" ist die Adresse, die aus Nullen und als letztem Bit einer 1  
besteht. Das ist die Host Local Adresse von IPv6,  
äquivalent  
127.0.0.1 bei IPv4.  
"fe80::0211:22ff:fe33:4455"  
ist eine typische Link Local Adresse, was man an dem Prefix  
"fe80" erkennt.
```

```
In URLs kollidiert der Doppelpunkt mit der Portangabe, daher werden  
IPv6-Nummern in URLs in eckige Klammern gesetzt  
("http://[1080::8:800:200c:417a]:80/").
```

Ist das IPv6-Netzwerkprotokoll aktiviert, wird dem LANTIME automatisch immer eine Link-Local IPv6 Adresse in der Form "FE80::..." zugewiesen, die die eigene Hardwareadresse der Netzwerkkarte enthält. Befindet sich in dem IPv6 Netzwerk ein Router-Advertiser werden zusätzlich noch eine oder mehrere Link-Global IPv6-Adressen vergeben, wenn IPv6 Autoconf aktiviert wurde.

Über den letzten Punkt kann das „High availability bonding“ eingestellt werden, wenn mehrere Ethernet Anschlüsse (optional) integriert sind. Nach IEEE802.3 ist es möglich, eine logische Netzwerkverbindung auf mehrere physikalische Verbindungen zu verschiedenen Switches aufzuteilen. Nur eine physikalische Verbindung wird zur gleichen Zeit verwendet. Offiziell als Bonding for High Availability bezeichnet, bieten es mehrere Hersteller unter verschiedenen Namen an: Link Aggregation, bonding, trunking, teaming. Hier kann ein Ethernet Port einer Bonding Gruppe zugeordnet werden. Es müssen mindestens zwei physikalische Ethernet Anschlüsse einer Bonding Gruppe hinzugefügt werden, damit das Bonding aktiviert wird. Der erste Ethernet Anschluss in einer Gruppe bestimmt die IP-Adresse und die Netzmaske der Bonding Gruppe. Aus technischen Gründen kann der ETH0 Anschluss nicht mit in eine Bonding Gruppe aufgenommen werden. Nur die zusätzlichen Anschlüsse (ETH1, ETH2, ...) können für das Bonding benutzt werden. Ein evtl. vorgeschalteter Netzwerk-Switch muss entsprechend für das Bonding konfiguriert werden.

## CLI Notification

```

NOTIFICATION CONFIGURATION
Email:      <To address>
            <From address>
            <Smarthost>

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>

```

Über die "Notification" (Alarm- und Status-Nachrichten) Einstellungen können unter verschiedenen Bedingungen ausgewählte Aktionen vom Zeitserver ausgeführt werden. Dies ist deswegen sinnvoll, weil der Zeitserver unbeobachtet die Zeit zur Verfügung stellt; wenn dann aber doch ein Fehler auftreten sollte, muss einem Verantwortlichen eine Nachricht (Alarmmeldung) gesendet werden, damit innerhalb kürzester Zeit darauf reagiert werden kann.

Bei diesem Zeitserver stehen die vier Aktionen EMAIL, SNMP-TRAP, WINDOWS POPUP MESSAGE und die Anzeige der Nachricht über das Großdisplay VP100/NET zur Verfügung. Jede Bedingung kann mit jeder Aktion beliebig verknüpft werden.

|                           |   |
|---------------------------|---|
| "NTP not sync"            | NTP nicht synchron zur Referenzzeit                 |
| "NTP stopped"             | NTP wurde angehalten (meist zu große Zeitabweichung |
| "Server boot"             | System wurde neu gestartet                          |
| "Receiver not responding" | keine Antwort von der Referenzuhr                   |
| "Receiver not sync"       | Referenzuhr nicht synchronisiert                    |
| "Config changed"          | Systemparameter vom Benutzer geändert               |

Für jedes Ereignis kann in dem letzten Abschnitt der „Notification Conditions“ eine beliebige „Trigger“ Aktion zugeordnet werden. Die entsprechenden Einstellungen für die vier verschiedenen Aktionen werden in den oberen Abschnitten vorgenommen.

In verschiedenen Systemzuständen können E-Mails mit den entsprechenden Zuständen automatisch vom LANTIME versendet werden. In dem Abschnitt "EMAIL Information" können die Absender Adresse (From:), die EMAIL Adresse (To:), ein eventuell vorhandener EMAIL-SMARTHOST (ausgehender Mailserver)

angegeben werden. Diese Einstellungen können nicht über das LCD-Frontpanel geändert werden. Folgende Hinweise zur Konfiguration der EMAILs sollten beachtet werden:

- Der Hostname und der Domainname sollte dem E-Mail-Smarthost bekannt sein
- Es muss ein gültiger Nameserver eingetragen sein
- Der Domainnamen-Teil der Absender Adresse (From:) sollte gültig sein

Microsoft Windows stellt mit dem WinPopup (Windows Mail) ein lokales Benachrichtigungswerkzeug zur Verfügung. Damit können über das Windows eigene Protokoll-Nachrichten direkt an Rechner im lokalen Netzwerk versendet werden. Für diese Nachrichten braucht das NETBIOS nicht aktiviert werden. Es muss der „Microsoft Client für Windows Netzwerke“ aktiviert sein. Im zweiten Abschnitt kann der Rechnername von bis zu zwei Windows Rechnern angegeben werden. Jede Nachricht wird mit einem Zeitstempel und der Benachrichtigung im Klartext versehen.

In den Einstellungen für die SNMP TRAPs als Benachrichtigung und Alarmmeldung können zwei unabhängige SNMP Manager (SNMP TRAP Receiver) als IPv4, IPv6 oder Hostname eingestellt werden. Zusätzlich muss zu jedem SNMP Manager eine sogenannte Community String (eine Art Gruppenpasswort) eingestellt werden (default: „public“). Diese sind nicht mit den SNMP Community Strings des internen SNMPD zu verwechseln, die auf der Security Seite beschrieben werden.

Die Großanzeige VP100/NET dient zur Anzeige von Uhrzeit und Datum. Diese Anzeige hat eine integrierte Netzwerkkarte und einen SNTP Client. Die Zeit wird von einem beliebigen NTP Zeitserver über das SNTP Protokoll abgeholt und damit die interne Uhr nachgeregelt. Diese Anzeige kann auch beliebige Texte als Laufschriften darstellen. Alle Alarmmeldungen können als Textmeldung auf dem Display angezeigt werden. Wenn ein ausgewähltes Ereignis auftritt, wird diese Meldung 3 mal hinter einander als Laufschrift auf dem Display angezeigt.

Dazu müssen im vierten Abschnitt die IP-Adresse und die Seriennummer der VP100/NET eingetragen werden. Die Seriennummer des Displays wird angezeigt, wenn man die rote Set Taste 4 mal drückt. Es muss die gesamte Nummer in das Feld eingetragen werden.

Die Schnittstelle zu dem VP100/NET Display kann auch direkt über ein LINUX Tool von der Kommandozeile angesteuert werden. Damit ist es möglich noch weitere Nachrichten, z.B. aus eigenen Scripten oder CRON Jobs auf dem Display darzustellen. Beim Aufruf des Kommandozeilen Programms ohne Parameter werden alle Parameter und eine kleine Anleitung angezeigt (siehe Anhang).

Über den Benachrichtigungspunkt „User“ kann ein frei definierbares Skript automatisch bei einer Bedingung ausgeführt werden. Über die Punkte „Show user defined script“ und „Edit user defined script“ kann dieses Skript angezeigt und

bearbeitet werden. Das Skript ist auf der Flash unter /mnt/flash/user\_defined\_notification zu finden. Dem Skript wird als Parameter der Index und der zugehörige Alarmtext übergeben. Der Index der Test-Bedingung ist dabei 0.

| NOTIFICATION CONDITIONS                          |                                     |                          |                          |                          |                          |
|--|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Sending notification under following conditions: |                                     |                          |                          |                          |                          |
| Condition:                                       | E-Mail                              | SNMP                     | WinMail                  | Display                  | User                     |
| NTP not sync                                     | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| NTP stopped                                      | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Server boot                                      | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Receiver not responding                          | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Receiver not sync                                | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Config changed                                   | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

## CLI Security

```
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
Please edit Contact & Location on the LOCAL page

SAVE  CLOSE
```

Über das Security Management können alle sicherheitsrelevanten Einstellungen für den Zeitserver vorgenommen werden. In dem ersten Abschnitt „Login“ kann das Zugangs Passwort für SSH, TELNET, FTP, HTTP und HTTPS eingestellt werden. Das Passwort wird verschlüsselt auf dem internen Flash abgelegt und kann nur mit Hilfe eines „Factory Reset“ in den Ursprungszustand („timeserver“) zurückgesetzt werden (siehe auch Konfiguration über das LCD).

Über das „Secure Shell Login“ ist es möglich eine gesicherte Verbindung zum LANTIME aufzubauen. Alle Daten werden während der Übertragung über das Ethernet verschlüsselt. Somit werden auch keine lesbaren Kennwörter über das Netzwerk gesendet. Die aktuelle LANTIME Version unterstützt SSH1 und SSH2 über IPv4 und IPv6. Um diesen Dienst nutzen zu können, muss der SSHD in den Netzwerkeinstellungen aktiviert werden und ein SSH Schlüssel auf dem Zeitserver erzeugt werden. Von einem entfernten Rechner kann dann mit dem Kommando „ssh“ eine Secure Shell geöffnet werden:

```
sshroot @ 192.168.16.111
```

Beim ersten Zugriff muss das neue Zertifikat bestätigt werden und dann wird man nach dem Passwort („timeserver“) gefragt.

Über den Schalter „Generate SSH key“ kann ein neuer Schlüssel erzeugt werden. Dieser Schlüssel kann dann per „Cut & Paste“ in die lokale SSH Konfiguration des Clients übertragen werden. Mit dem Schalter „Show SSH key“ kann der aktuelle Schlüssel auf dem LANTIME angezeigt werden.

Über den Schalter „Generate SSL certificate for HTTP“ kann ein neues Zertifikat für eine gesicherte HTTP Verbindung erstellt werden. Es erscheint ein Formular, wo die genauen Nutzerdaten wie Organisation, Name, Emailadresse und der Standort angegeben werden müssen.

Nach der erfolgreichen Erzeugung des SSL Zertifikats wird das gesamte Ergebnis angezeigt.

Im dritten Abschnitt können die symmetrischen Schlüssel und die Autokey Zertifikate für den NTP angelegt und erzeugt werden.

Über den Punkt „Generate new NTP public key“ wird automatisch ein beglaubigtes (trusted) Zertifikat erzeugt. Dieses Zertifikat ist abhängig von dem eingestellten Hostnamen. Das Zertifikat muss immer erneuert werden, wenn der Hostname des Zeitserver geändert wurde. Die Zertifikate werden mit dem internen Tool „ntp-keygen -T“ erzeugt. Die öffentlichen und privaten Schlüssel werden im Verzeichnis „/etc/ntp/“ abgelegt. Bitte lesen Sie hierzu auch das Kapitel über NTP Autokey.

Über die beiden Punkte „Show NTP MD5 key“ und „Edit NTP MD5 keys“ können die symmetrischen NTP Keys verwaltet werden. Bitte lesen Sie hierzu auch das Kapitel über die symmetrischen NTP Keys.

Im letzten Abschnitt können die Parameter für den SNMP eingetragen werden. Bei Änderungen von grundlegenden Änderungen der SNMP Parameter muss das Gerät neu gestartet werden oder der SNMP Dienst über die Ethernet Einstellungen einmal aus und wieder eingeschaltet werden. Weitere Informationen zu den Eigenschaften des SNMP befinden sich in einem späteren Kapitel.

## 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

In der NTP Konfiguration werden alle zusätzlichen Parameter neben der standardmäßigen Konfiguration des Zeitservers eingestellt. Diese Standard Konfiguration besteht als erstes aus der „local clock“, welches der Hardwareuhr des Betriebssystems entspricht und immer dann benutzt wird, wenn die anderen Referenzuhren nicht mehr zur Verfügung stehen (z.B. wenn diese nicht synchronisiert haben). Der Stratum-Wert dieser „local clock“ wird sehr hoch gesetzt (default: 12) damit die angeschlossenen Benutzer ein Umschalten auf diese nicht sehr genaue Zeit registrieren und entsprechend darauf reagieren können. Als zweites wird die serielle Schnittstelle der Referenzuhr (in diesem Fall die GPS) als erste Referenzuhr eingestellt. Da diese Referenzzeit nur über die serielle Schnittstelle angebunden ist, kann hiermit vom NTP nur eine Genauigkeit um 1 ms erreicht werden. Die eigentliche Genauigkeit (um 10 Mikrosekunden) wird erst über den ATOM Treiber des NTP erreicht, welche direkt über das Betriebssystem den PPS (Pulse Per Second) der Referenzuhr auswertet. Die Standard Konfiguration hat folgendes Aussehen:

```
# *** 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 0.004400 # calibration value
fudge 127.127.8.0 flag2 0 flag3 1
server 127.127.22.0 minpoll 6 maxpoll 6 # ATOM (PPS)
fudge 127.127.22.0 flag2 0 f lag3 0 # enable PPS API
enable pps
enable stats
statsdir /var/log/
statistics loopstats
driftfile /etc/ntp.drift
```

Über diese Konfigurationsseite können zusätzliche NTP Parameter eingestellt werden. Im oberen Teil können bis zu 5 unterschiedliche externe NTP Server als Redundanz zu der internen Referenzuhr angegeben werden. Dabei kann wahlweise ein symmetrischer Schlüssel eingegeben werden und AUTOKEY aktiviert werden.

Über den Punkt „Stratum of local clock“ wird der Stratum-Wert der lokalen Referenzuhr angegeben.

Mit dem Punkt „Trusted key“ kann eine Liste aller symmetrischen Schlüssel durch Komma getrennt eingegeben werden, die vom NTP akzeptiert werden.

Soll zusätzlich die NTP Zeit als Broadcast im lokalen Netzwerk verteilt werden, kann hier eine gültige Broadcast Adresse eingegeben werden. Beachten Sie, dass ab der Version NTP 4 Broadcast immer mit Authentication benutzt werden muss.

Die NTP Trusttime gibt die Zeit an, wie lange der NTP die GPS Referenzzeit noch akzeptiert, wenn diese in den Freilauf Zustand (nicht mehr synchron) wechselt. Die Freilauf-Genauigkeit der Referenzuhr hängt direkt mit dem eingebauten Quarz zusammen. Standardmäßig ist ein TCXO Quarz im Lantime GPS eingebaut. Wird dieser Wert auf Null gesetzt, ist der Default Wert gültig. Die Default Trusttime Werte sind wie folgt:

Lantime/GPS : 96 Stunden  
Lantime/PZF : 0,5 Stunden  
Lantime/RDT: 0,5 Stunden  
Lantime/NDT: 96 Stunden

Im nächsten Punkt können die beiden Optionen AUTOKEY und PPS für den Zeitserver aktiviert werden, wobei PPS sich auf die zusätzliche Referenzuhr über den Sekundenimpuls bezieht.

Nach jedem Neustart und nach allen Änderungen der Konfiguration wird immer eine neue Datei **/etc/ntp.conf** vom LANTIME automatisch generiert, d.h. man kann keine Änderungen direkt an dieser Datei vornehmen. Wenn weitere Einstellungen am NTP (Authentication, Restriction ...) benötigt werden, die nicht mit den oben beschriebenen Parametern erreicht werden können, muss eine zusätzliche Konfigurationsdatei bearbeitet werden. Wenn die NTP Parameter permanent geändert werden sollen, muss eine Datei **/mnt/flash/ntpconf.add** erstellt werden, welche dann automatisch beim Booten oder Ändern der NTP Parameter an die Datei **/etc/ntp.conf** angehängt wird. Über den Punkt „Edit additional NTP parameter“ kann diese zusätzliche Datei bearbeitet und verwaltet werden.



## NTP Authentication

NTP bietet in der Version 2 und 3 ein Authentication Verfahren über symmetrische Schlüssel. Wird ein Paket in diesem Authentication Mode verschickt, so wird an jedes ein 32-bit Key ID und eine cryptografische 64/128-bit Checksumme des Paketes, erstellt entweder mit Data Encryption Standard (DES) oder Message Digest (MD5) Algorithmen, angehängt. Beide Algorithmen bieten ausreichenden Schutz vor Manipulation der Inhalte. Zu beachten ist, dass die Verbreitung des DES in den USA sowie in Kanada Einschränkungen unterliegt, während MD5 zur Zeit davon nicht betroffen ist. Mit jedem der beiden Algorithmen berechnet der empfangende Partner die Checksumme und vergleicht sie mit der im Paket enthaltenen. Beide Partner müssen hierfür den gleichen Encryption Key mit der dazugehörigen gleichen Key ID haben. Dieses Feature bedarf einiger kleiner Modifikationen an der Standard Paket Verarbeitung. Diese Modifikationen werden mit der **enable authenticate** in Konfigurationsdatei aktiviert. Im Authentication Mode werden Partner als ungläubwüdig und für eine Synchronisation nicht geeignet gekennzeichnet, wenn sie entweder unauthentisierte Pakete, authentifizierte Pakete die nicht entschlüsselt werden können oder authentifizierte Pakete, die einen falschen Key benutzen, senden. Zu beachten ist, dass ein Server der viele Keys kennt (identifiziert durch viele Key IDs) möglicherweise nur einen Teil dieser verwendet. Dies ermöglicht dem Server einen Client, der eine authentifizierte Zeitinformation verlangt, zu bedienen ohne diesem selbst zu trauen. Einige zusätzliche Konfigurationen sind erforderlich um die Key ID zu spezifizieren, die jeden Partner auf Authentizität prüft. Die Konfigurationsdatei (siehe **Manuelle NTP Konfiguration**) für einen Server im Authentication Mode Authentication Mode kann wie folgt aussehen:

```
# 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 (7) for accessing server variables
controlkey 15               # key (6) for accessing server variables
```

Der Authentication Mode wird automatisch aktiviert, wenn ein Key benutzt wird und die Pfade für die Keys entsprechend eingestellt sind. Mit **keys /mnt/flash/ntp.keys** wird der Pfad für die Keys festlegt. In der **trustedkey** Zeile werden die Keys angegeben, die als uncompromised bekannt sind; der Rest sind verfallene oder compromised Keys. Beide Sätze von Keys müssen in der unten beschriebenen Datei **ntp.keys** deklariert werden. Dies ermöglicht es, alte Keys zu reaktivieren, während das wiederholte Senden von Keys minimiert wird. Die **requestkey 15** Zeile deklariert den Key für mode-6 control messages wie in RFC-1305 spezifiziert und vom **ntpq** Utility Programm benutzt, während die Zeile **controlkey 15** den Key für mode-7 private control messages deklariert, wie vom **ntpd** Utility Programm benutzt wird. Diese Keys werden benutzt um die Daemon Variablen vor unberechtigten Modifikationen zu schützen.

Die Datei **ntp.keys** beinhaltet eine Liste der Keys und zugehöriger IDs, die der Server kennt und muss deshalb auf nicht lesbar gesetzt werden. Der Inhalt kann wie folgt aussehen:

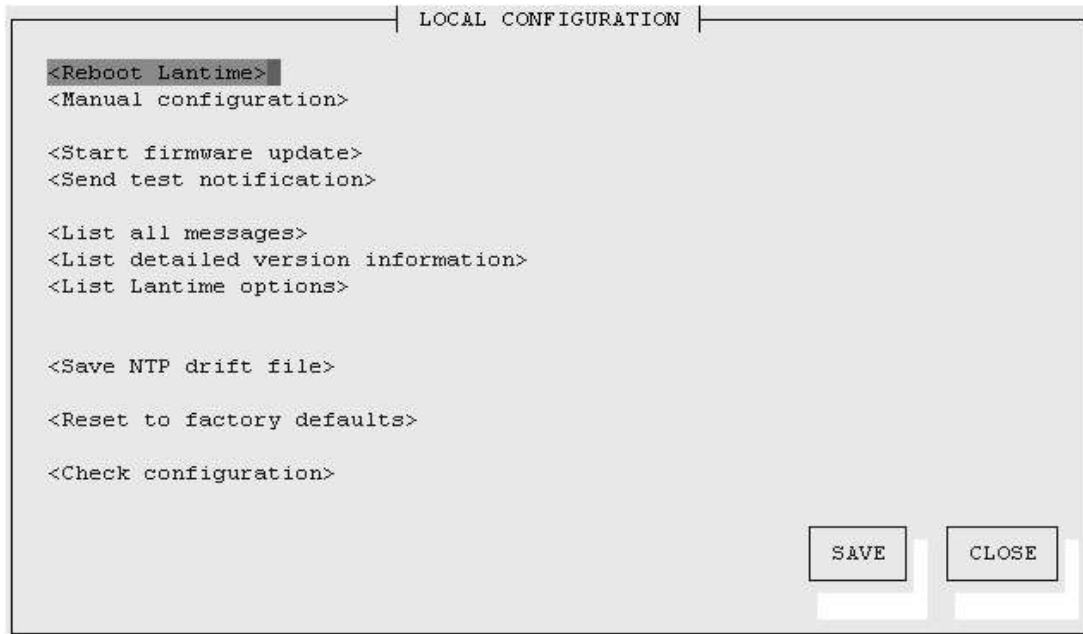
```

# 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

```

Die erste Spalte der Datei beinhaltet die Key ID, die zweite Spalte das Format des Keys und die dritte den Key selbst. Es gibt vier Key-Formate: Ein **A** steht für einen DES Key mit bis zu acht 7-Bit ASCII Characters, bei dem jeder Character für ein Key-Octet steht (wie bei einem Unix Passwort). Ein **S** steht für einen DES Key als Hex Ziffer, bei welchem das niederwertigste Bit (LSB) jedes Octets das ungerade Parity Bit ist. Ein mit **N** gekennzeichnete Key ist wiederum als Hex Ziffer geschrieben, jedoch im NTP Standard Format mit dem höchstwertigen Bit (HSB) jedes Oktets als das ungerade Parity Bit. Ein mit **M** gekennzeichnete Key ist ein MD5 Key mit bis zu 31 ASCII Zeichen. Zu Beachten ist, dass die Zeichen ' ', '#', '\t', '\n' und '\0' weder im DES noch im MD5 ASCII Key verwendet werden können! Key 0 (zero) ist reserviert für spezielle Zwecke und sollte deshalb hier nicht auftauchen.

## CLI Local



Im ersten Abschnitt werden verschiedene Funktionen für den Administrator zur Verfügung gestellt. Über den Punkt „Reboot Lantime“ wird ein Shutdown auf dem System ausgeführt. Das System braucht ca. eine halbe Minute für den Bootvorgang. Die Referenzuhr bekommt damit keinen RESET.

Über den Punkt „Manual configuration“ gelangt man in ein Editierfenster, worin die gesamte Konfiguration (siehe Anhang) editiert werden kann. Beim Beenden dieses Fensters wird gefragt, ob die geänderte Konfiguration dann aktiviert werden soll.

Über den Punkt „Send test notification“ wird eine Test Alarmmeldung für alle konfigurierten Aktionen erzeugt. D.h., wenn in der Ereigniskonfiguration eine E-Mail-Adresse korrekt eingestellt wurde, wird an diese eine Test-E-Mail gesendet.

Über den Punkt „Save NTP drift file“ wird die Datei `/etc/ntp.drift` auf der Flashdisk abgespeichert. NTP benutzt dieses Driftfile, um die Kompensation der Zeitungenauigkeit der Rechneruhr nach einem Neustart des NTP direkt zur Verfügung zu haben. Dadurch schwingt sich der NTP schneller ein. Dieser Wert sollte nur dann gespeichert werden, wenn der NTP für längere Zeit (> ein Tag) sich auf die Referenzuhr synchronisiert hat. Dieses wird einmal bei der Auslieferung des Gerätes im Werk ausgeführt.

Über den Punkt „Reset to factory defaults“ werden alle Einstellungen auf den Auslieferungszustand zurückgesetzt. Dabei wird die alte Konfiguration unter `/mnt/flash/global_configuration.old` gespeichert und dann durch die Datei `/mnt/flash/factory.conf` ersetzt. Dabei wird auch das Standard Passwort „timeserver“ wieder aktiviert. Nach diesem Vorgang sollten alle Zertifikate neu gesetzt werden, weil auch der Hostname geändert wurde.

Zur Administrierung des LANTIME können eigene Benutzer angelegt werden. Dabei werden 3 Benutzergruppen unterschieden. Die Gruppe „Super-User“ hat alle Rechte zur Administrierung. Die Gruppe Administrator kann nur über die Benutzerschnittstellen HTTP und das Comand Line Interface (CLI) über Telnet, SSH oder Terminal Änderungen vornehmen; beim Einloggen über eine Kommandozeile wird direkt das Setup Interface gestartet und beim Beenden wird die Session direkt geschlossen. Somit hat der Adminitator keinen direkten Zugriff auf Linux Befehle. Die Benutzergruppe Info hat die gleichen Einschränkungen wie der Administrator und kann zusätzlich keine Veränderungen an der Konfiguration vornehmen.

Über die Benutzerverwaltung können neue Benutzer jeweils mit Passwort und Gruppenzugehörigkeit angelegt und gelöscht werden. Zum Ändern eines Benutzers muß dieser erst gelöscht und dann neu angelegt werden. Im unteren Teil der Benutzerverwaltung wird eine Liste aller Benutzer angezeigt. Der Benutzer „root“ ist fest vorgegeben und hat immer Super-User Rechte. Das Passwort von „root“ kann nur über die Seite Sicherheit/Login geändert werden.

Über den Punkt „List all messages“ wird die aktuelle SYSLOG Datei angezeigt. In dieser Datei werden von allen Programmen, wie auch von dem aktuellen Betriebssystem Kernel, die Meldungen abgelegt. In einem extra Fenster wird die gesamte Datei /var/log/messages angezeigt. Diese Datei steht in der RAM-DISK und wird nach jedem Neustart gelöscht. Über einem externen SYSLOG Server kann diese Datei auf einen externen Rechner umgeleitet werden.

Der Punkt „List detailed version information“ zeigt die aktuelle Version des LANTIME und der Softwarekomponenten an.

Der Punkt „List Lantime Options“ zeigt die Optionen der integrierten Komponenten an.

Über den Punkt „Start firmware update“ kann ein automatisches Update auf dem LANTIME gestartet werden. Dazu wird eine spezielle Datei von der Firma Meinberg benötigt, um ein solches Update auszuführen. Über den Schalter „Browse“ kann die Update Datei auf dem lokalen PC ausgewählt werden. Diese wird auf den LANTIME herunter geladen und nach einer erneuten Abfrage wird dann das Update gestartet. Welche Software auf dem LANTIME damit erneuert wird, hängt nur von der Update Datei ab.

Der NTP speichert den Korrekturwert für das Nachregeln der Systemzeit in einer Datei ab, damit beim nächsten Neustart das Einschwingverhalten verkürzt wird. Mit dem Punkt „Save NTP drift file“ wird diese temporäre Datei auf die Flashdisk geschrieben. Dieser Vorgang wird bei Auslieferung werksseitig durchgeführt.

Mit dem Punkt „Reset to factory defaults“ werden alle Einstellungen auf den Auslieferungszustand zurückgesetzt. Dabei wird auch die IP Adresse gelöscht und der DHCP aktiviert.

Mit „Check configuration“ können alle aktuellen Einstellungen des Zeitserver getestet werden. Dabei werden alle Werte auf Plausibilität geprüft und alle eingestellten IP-Adressen auf Erreichbarkeit. Alle Werte, die rot gekennzeichnet werden, sollten besonders geprüft werden. Es wird auch die Erreichbarkeit der eingestellten IP-Adressen geprüft – dies kann u.U. einiges an Zeit beanspruchen.

## SNMP Server

Das Simple Network Management Protocol (SNMP) wurde für die einheitliche Verwaltung verschiedener Netzwerktypen entwickelt. SNMP operiert auf der Anwendungsebene unter Einsatz von TCP/IP Transport Protokollen, so dass es unabhängig von der zugrundeliegenden Netzwerk-Hardware arbeitet. Das SNMP Design basiert auf zwei Komponenten: dem Agenten und dem Manager. SNMP ist eine Client Server Architektur, in der der Agent den Server und der Manager den Client repräsentiert. Das LANTIME hat einen SNMP Agenten integriert, der speziell zum Abfragen der Statusinformationen von NTP und der Referenzuhr entwickelt wurde. Er verfügt über eine Schnittstelle, welche den Zugriff auf alle Elemente der Gerätekonfiguration bietet. Diese Elemente werden in mehreren Datenstrukturen verwaltet, die sich Management Information Base (MIB) nennen. Das LANTIME verfügt über die Standard NET-SNMP MIBs und basiert auf SNMPv1 (RFC 1155, RFC 1157), SNMPv2 (RFC1901-1908) und SNMPv3. Folgende SNMP Version ist installiert:

|                            |   |
|----------------------------|---|
| 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,<br>notification, target, agent_mibs, agentx<br>agent_mibs, utilities, meinberg, mibII/ipv6 |
| Authentication support:    | MD5 SHA1  |
| Encryption support:        | DES   |

Über den von Meinberg speziell entwickelten SNMP-Agent können die wichtigsten Zustände des Zeitserver abgefragt werden. Dabei werden Statusinformationen vom NTP und der angeschlossenen Referenzuhr als Text und als Value zur Verfügung gestellt. Um sich alle Statusinformationen des Zeitserver von einem entfernten Rechner anzeigen zu lassen, kann man beispielsweise über den „snmpwalk“ Befehl eine komplette Liste aller Statusinformationen anzeigen lassen:

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

```

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

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

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

```

Über die Standard MIB können keine Zugriffe auf das NTP vorgenommen werden; es kann nur auf System- und Netzwerkparameter zugegriffen werden (z.B. von einem Client Rechner mittels dem Befehl: "snmpget").

Nur über die Meinberg eigene SNMP-MIB lässt sich eine Konfiguration aller Parameter des Zeitservers durchführen, die auch über das HTTP- oder Command Line Interface eingestellt werden können.

## Konfiguration über SNMP

Der LANTIME Zeitserver kann über verschiedene Benutzerschnittstellen konfiguriert werden. Neben der Konfiguration über das Webinterface (HTTP bzw. HTTPS) und dem Shell-Zugang (Telnet bzw. SSH) ist das Abfragen und Einstellen der Parameter auch über SNMP möglich.

Der SNMP Agent des Zeitservers versteht SNMP V1 ,V2c und V3 und ist per UDP und TCP erreichbar (IPv4 und IPv6).

Um den Zeitserver per SNMP konfigurieren zu können, sind neben der generellen Erreichbarkeit des Zeitservers über das Netzwerk (mit einem der oben angegebenen Netzwerkprotokolle) folgende Voraussetzungen zu erfüllen:

- a) SNMP muss aktiviert sein
- b) In der SNMP Konfiguration muss der Schreibzugriff auf die Parameter aktiviert werden
- c) Die MIBs für den Zeitserver müssen auf den SNMP-Clients vorhanden und eingebunden sein
- d) Sie müssen den SNMPW-Schreibzugriff aktivieren, indem Sie eine RWCOMMUNITY einstellen

Sowohl a) als auch b) werden in den Kapiteln über das Webinterface und den Shellzugang beschrieben. Die unter c) angesprochenen MIB-Dateien finden Sie auf dem Zeitserver im Verzeichnis /usr/local/share/snmp/mibs, es handelt sich um die Dateien, deren Namen mit „MBG-SNMP-“ anfängt. Kopieren Sie diese Dateien (z.B. mittels FTP) in das MIB-Verzeichnis des/der Clients und geben Sie diese in der Konfiguration Ihrer SNMP Clientsoftware an. Alternativ können Sie ein gepacktes TAR Archiv mit allen MIBs über das Webinterface des Zeitservers herunterladen (Menüpunkt „Local“ - „Download SNMP MIB files“).

Auch Punkt d) lässt sich über das Webinterface oder den Shellzugang einstellen. Siehe dazu ebenfalls die entsprechenden Abschnitte über Webinterface und Shellzugang.



## Beispiele SNMP Konfiguration

Bei den nachfolgenden Beispielen findet die Software net-snmp Verwendung, ein SNMP - Open Source Projekt. Weitere Informationen sowie Download-Möglichkeiten finden Sie unter [www.net-snmp.org](http://www.net-snmp.org)!

Um sich den Konfigurationszweig der Zeitserver MIB anzeigen zu lassen, können Sie beispielsweise folgende Befehlszeile auf einem Unix-Rechner mit installierten net-snmp-Tools eingeben:

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

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

Um einen Parameter zu ändern, kann man bei net-snmp den Befehl snmpset nutzen:

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

```
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgHostname.0 = STRING: helloworld
root@testhost:/#
```

Bitte beachten Sie, dass der SNMP-Request bei Konfigurationsänderungen einen ausreichenden Timeout hat (im obigen Beispiel durch den Parameter „-t 10“ auf 10 Sekunden gesetzt) und keine Retries ausgeführt werden sollten (im Beispiel erreicht durch „-r 0“). Da nach einer Konfigurationsänderung die Parameter vom Zeitserver neu eingelesen werden müssen, dauert es ein wenig, bis der SNMP-Set-Request vom Zeitserver bestätigt wird.

Um mehrere Parameter zu verändern und erst danach das Neueinlesen der Parameter durch den Zeitserver zu erreichen, müssen Sie alle zu ändernden Parameter in einem einzigen Request schicken. Das erreicht man bei net-snmp / snmpset durch die Angabe mehrerer Parameter in einem Aufruf:

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

```
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgHostname.0 = STRING: helloworld
MBG-SNMP-LANTIME-CFG-MIB::mbgLtCfgDomainname.0 = STRING: internal.meinberg.de
root@testhost:/#
```

Die einzelnen SNMP-Variablen werden im Abschnitt „SNMP Konfigurationsreferenz“ beschrieben. Es empfiehlt sich, auch die Meinberg MIBs zu lesen.

## **Weitere Konfigurationsmöglichkeiten**

Da der Zeitserver eine Standardversion des net-snmp SNMP-Daemons ausführt (erweitert um eigene Agent-Funktionalität), können alle Konfigurationsmöglichkeiten des SNMPD genutzt werden. Die Konfigurationsdatei des SNMP Daemons befindet sich nach dem Bootvorgang in /usr/local/share/snmp, als Dateiname wird snmpd.conf verwendet.

Während der Bootphase wird diese Datei dynamisch erzeugt, d.h. sie wird „zusammengebaut“ aus einem Template und den in der Zeitserver-Konfiguration angegebenen (für SNMP relevanten) Parameter.

Falls Sie über die in der Zeitserver-Konfiguration hinausgehende Einstellungen für den SNMPD verwenden möchten (um z.B. detailliertere Sicherheitseinstellungen vorzunehmen, mehrere verschiedene Communities verwenden, etc.), können Sie Ihre Einstellungen in der Datei /mnt/flash/packages/snmp/etc/snmpd\_conf.default vornehmen. Bitte beachten Sie, dass an diese Datei wie beschrieben beim Bootvorgang noch Parameter angehängt werden, bevor sie als /usr/local/share/snmp/snmpd.conf vom SNMPD verwendet wird.

## **Senden von Befehlen an den Zeitserver per SNMP**

Neben der Möglichkeit, den Zeitserver per SNMP zu konfigurieren, kann man auch einige spezielle Befehle über diese Schnittstelle ausführen lassen. Dafür wird eine SNMP-Variable (mbgLtCmdExecute) auf einen Integerwert gesetzt. Folgende Befehle sind möglich:

### **Reboot(1)**

Setzt man die mbgLtCmdExecute Variable auf den Wert 1, leitet der Zeitserver einen Reboot ein (nach einer kurzen Wartezeit von ca. 3-5 Sekunden).

### **FirmwareUpdate(2)**

Eine zuvor per FTP Upload auf den Zeitserver kopierte Firmware-Datei /www/update.tgz wird installiert. Bitte beachten Sie, dass diese Datei ein bestimmtes Format haben muss und i.d.R. nur von Meinberg zur Verfügung gestellt wird.

### **ReloadConfig(3)**

Die Parameter der Zeitserver-Konfiguration (/mnt/flash/global\_configuration) werden neu eingelesen, danach werden einige Dienste beendet und neu gestartet (z.B. NTPD, HTTPD, HTTPSD, etc.), damit eventuelle Konfigurationsänderungen wirksam werden können. Bitte beachten Sie, dass der SNMPD hierbei nicht neu gestartet wird.

### **GenerateSSHKey(4)**

Es wird ein neuer Schlüssel für den SSH Zugang generiert.

### **GenerateHTTPSKey(5)**

Es wird ein neuer Schlüssel für den HTTPS Zugang generiert.

### **ResetFactoryDefaults(6)**

Die Zeitserver-Konfiguration wird auf den Zustand bei der Auslieferung zurückgesetzt. Danach wird diese Default-Konfiguration durch ein automatisches ReloadConfig aktiviert.

### **GenerateNewNTPAutokeyCert(7)**

Es wird ein neuer Schlüssel für das NTP Autokey Feature generiert.

### **SendTestNotification(8)**

Es wird eine Testnachricht über alle Benachrichtungstypen verschickt, für die Angaben gemacht wurden.

### **Ein Beispiel für die Nutzung dieses Features:**

(Wir verwenden wieder den Befehl snmpset aus dem net-snmp-Projekt)

```
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:~#
```

Dieser Befehl veranlasst den Zeitserver, komplett neu zu starten (Reboot). Sie können anstelle des Integerwertes auch den Befehlsnamen verwenden, so wie er in der MIB Datei MBG-SNMP-LANTIME-CMD.txt angegeben wird (und auch oben bei der Auflistung der möglichen Befehle). Um die Konfiguration neu einzulesen (weil Sie z.B. vorher manuell per FTP-Upload eine neue Konfigurationsdatei auf den Zeitserver geladen haben), gehen Sie mit net-snmp folgendermaßen vor:

```
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:~#
```

Bitte beachten Sie, dass auch hier keine Retries erlaubt werden sollten (Parameter „-r 0“) und ein ausreichender Timeout angegeben wird („-t 10“ für 10 Sekunden).

## Konfiguration des Zeitservers via SNMP: Referenz

Die MIB des Zeitservers gliedert sich folgendermaßen:

| SNMP Objekt      | Bezeichnung   | Beschreibung                                |
|------------------|---------------|---|
| enterprises.5597 | mbgSNMP       | Root node der Meinberg-MIB                  |
| mbgSNMP.3        | mbgLantime    | Root node der Lantime MIB                   |
| mbgLantime.1     | mbgLtNtp      | Lantime NTP Statusvariablen                 |
| mbgLantime.2     | mbgLtRefclock | Lantime Referenzzeitquellen-Statusvariablen |
| mbgLantime.3     | mbgLtTraps    | Lantime SNMP Traps                          |
| mbgLantime.4     | mbgLtCfg      | Lantime Konfigurationsvariablen             |
| mbgLantime.5     | mbgLtCmd      | Lantime Steuerbefehle                       |

Weitere Angaben können Sie den mitgelieferten Meinberg-MIBs entnehmen.

Referenz Lantime SNMP Konfigurationsvariablen:

| <i>SNMP Zweig</i> | <i>Variable</i>       | <i>Datentyp</i>                               | <i>Beschreibung</i>                                   |
|-------------------|-----------------------|---|---|
| mbgLtCfgNetwork   | mbgLtCfgHostname      | string  | Der Hostname des Zeitservers                          |
|                   | mbgLtCfgDomainname    | string  | Der Domainname des Zeitservers                        |
|                   | mbgLtCfgNameserver1   | string (IPv4 oder IPv6-Adresse)               | IP-Adresse des ersten Nameservers                     |
|                   | mbgLtCfgNameserver2   | string (IPv4 oder IPv6-Adresse)               | IP-Adresse des zweiten Nameservers                    |
|                   | mbgLtCfgSyslogserver1 | string (IPv4 oder IPv6-Adresse oder Hostname) | IP-Adresse oder Hostname des ersten Syslog-Servers    |
|                   | mbgLtCfgSyslogserver2 | string (IPv4 oder IPv6-Adresse oder Hostname) | IP-Adresse oder Hostname des zweiten Syslog-Servers   |
|                   | mbgLtCfgTelnetAccess  | integer (0 = disabled, 1 = enabled)           | Telnet-Zugang zum Zeitserver aktiv?                   |
|                   | mbgLtCfgFTPAccess     | integer (0 = disabled, 1 = enabled)           | FTP-Zugang zum Zeitserver aktiv?                      |
|                   | mbgLtCfgHTTPAccess    | integer (0 = disabled, 1 = enabled)           | Webinterface aktiv?                                   |
|                   | mbgLtCfgHTTPSAccess   | integer (0 = disabled, 1 = enabled)           | Verschlüsseltes Webinterface aktiv?                   |
|                   | mbgLtCfgSNMPAccess    | integer (0 = disabled, 1 = enabled)           | SNMP-Daemon aktiv?                                    |
|                   | mbgLtCfgSambaAccess   | integer (0 = disabled, 1 = enabled)           | LANManager-Zugang aktiv?                              |
|                   | mbgLtCfgIPv6Access    | integer (0 = disabled, 1 = enabled)           | IPv6-Protokoll aktiviert?                             |
|                   | mbgLtCfgSSHAccess     | integer (0 = disabled, 1 = enabled)           | SSH-Zugang zum Zeitserver aktiv?                      |
| mbgLtCfgNTP       | mbgLtCfgNtpServer1IP  | string (IPv4 oder IPv6-Adresse oder Hostname) | Erster externer NTP-Server                            |
|                   | mbgLtCfgNtpServer1KEY | integer                                       | Verweis auf zu verwendenden Key für ersten NTP-Server |

| <b>SNMP Zweig</b> | <b>Variable</b>                    | <b>Datentyp</b>                               | <b>Beschreibung</b>   |
|-------------------|------------------------------------|---|---|
|                   | mbgLtCfgNtpServer2IP               | string (IPv4 oder IPv6-Adresse oder Hostname) | Zweiter externer NTP-Server   |
|                   | mbgLtCfgNtpServer2KEY              | integer                                       | Verweis auf zu verwendenden Key für zweiten NTP-Server  |
|                   | mbgLtCfgNtpServer3IP               | string (IPv4 oder IPv6-Adresse oder Hostname) | Dritter externer NTP-Server   |
|                   | mbgLtCfgNtpServer3KEY              | integer                                       | Verweis auf zu verwendenden Key für dritten NTP-Server  |
|                   | mbgLtCfgStratumLocalClock          | integer(0..15)                                | Stratum-Wert der internen Systemuhr des Zeitserver  |
|                   | mbgLtCfgNTPTrustedKey              | integer                                       | Verweis auf den zu verwendenden Key für die interne Referenzzeitquelle  |
|                   | mbgLtCfgNTPBroadcastIP             | string (IPv4 oder IPv6-Adresse)               | IP-Adresse, die für NTP-Broadcasts (oder Multicasts) verwendet wird   |
|                   | mbgLtCfgNTPBroadcastKey            | integer                                       | Verweis auf den zu verwendenden Key für ausgehende NTP-Broadcasts   |
|                   | mbgLtCfgNTPBroadcastAutokey        | integer (0 = disabled, 1 = enabled)           | Autokey für NTP Broadcasts verwenden?   |
|                   | mbgLtCfgAutokeyFeature             | integer (0 = disabled, 1 = enabled)           | Autokey Feature des NTP Servers aktivieren?   |
|                   | mbgLtCfgAtomPPS                    | integer (0 = disabled, 1 = enabled)           | Atom PPS (pulse per second) aktiviert?  |
| mbgLtCfgEMail     | mbgLtCfgEMailTo                    | string (Liste von EMail-Adressen)             | Eine oder mehrere EMail-Adressen (durch Semikolon getrennt), die Warnungen und Alarmmeldungen vom Lantime per Mail empfangen sollen |
|                   | mbgLtCfgEMailFrom                  | string (EMail-Adresse)                        | Die EMail-Adresse, die als Absender der per Mail verschickten Warnungen und Alarmmeldungen verwendet wird                           |
|                   | mbgLtCfgEMailSmarthost             | string (IPv4 oder IPv6-Adresse oder Hostname) | Der SMTP-Host, der für das Verschicken der per Mail verschickten Warnungen und Alarmmeldungen verwendet wird                        |
| mbgLtCfgSNMP      | mbgLtCfgSNMPTrapReceiver1          | string (IPv4 oder IPv6-Adresse oder Hostname) | Erster Rechner, der als SMTP-Traps verschickte Warnungen und Alarmmeldungen empfangen soll  |
|                   | mbgLtCfgSNMPTrapReceiver1Community | string  | Die SNMP Community, die beim Verschicken der SNMP-Traps an den ersten Rechner verwendet wird  |
|                   | mbgLtCfgSNMPTrapReceiver2          | string (IPv4 oder IPv6-Adresse oder Hostname) | Zweiter Rechner, der als SMTP-Traps verschickte Warnungen und Alarmmeldungen empfangen soll   |
|                   | mbgLtCfgSNMPTrapReceiver2Community | string  | Die SNMP Community, die beim Verschicken der SNMP-Traps an den zweiten Rechner verwendet wird                                       |
|                   | mbgLtCfgSNMPCOMMUNITY              | string  | Die SNMP Community, die Nur-Lese-Rechte hat und somit lediglich Status und Konfigurationsvariablen abfragen kann (SNMP V2c)         |
|                   | mbgLtCfgSNMPRWCommunity            | string  | Die SNMP Community, die Schreib-Lese-Rechte hat und somit Status abfragen und Konfigurationsvariablen setzen kann (SNMP V2c)        |

| <i>SNMP Zweig</i>   | <i>Variable</i>                     | <i>Datentyp</i>                               | <i>Beschreibung</i>  |
|---------------------|-------------------------------------|---|--|
|                     | mbgLtCfgSNMPContact                 | string  | Kontaktinformationen (z.B. Name eines Ansprechpartners) des Zeitservers  |
|                     | mbgLtCfgSNMPLocation                | string  | Standortangaben (z.B. Gebäude/Raum) des Zeitservers  |
| mbgLtCfgWinpopup    | mbgLtCfgWMailAddress1               | string  | Erster Empfänger von per Windows Popup Messages verschickten Warnungen und Alarmmeldungen  |
|                     | mbgLtCfgWMailAddress2               | string  | Zweiter Empfänger von per Windows Popup Messages verschickten Warnungen und Alarmmeldungen   |
| mbgLtCfgWalldisplay | mbgLtCfgVP100Display1IP             | string (IPv4 oder IPv6-Adresse oder Hostname) | Hostname oder IP-Adresse des ersten Wanddisplays, auf dem Warnungen und Alarmmeldungen angezeigt werden sollen   |
|                     | mbgLtCfgVP100Display1SN             | string (Hexstring)                            | Die Seriennummer des ersten Wanddisplays, auf dem Warnungen und Alarmmeldungen angezeigt werden sollen (kann am Display im Konfigurations-Menü abgefragt werden)   |
|                     | mbgLtCfgVP100Display2IP             | string (IPv4 oder IPv6-Adresse oder Hostname) | Hostname oder IP-Adresse des zweiten Wanddisplays, auf dem Warnungen und Alarmmeldungen angezeigt werden sollen  |
|                     | mbgLtCfgVP100Display2SN             | string (Hexstring)                            | Die Seriennummer des zweiten Wanddisplays, auf dem Warnungen und Alarmmeldungen angezeigt werden sollen (kann am Display im Konfigurations-Menü abgefragt werden)  |
| mbgLtCfgNotify      | mbgLtCfgNotifyNTPNotSync            | string (Kombination)                          | Keine, eine oder durch Komma getrennte Kombinationen von Benachrichtigungstypen<br><br>email=Senden einer EMail,<br>wmailSenden einer Winpopup-Meldung<br>snmp=Senden eines SNMP-Traps,<br>disp=Anzeige auf Wanddisplay, für das Ereignis „NTP nicht synchron“ |
|                     | mbgLtCfgNotifyNTPStopped            | string (Kombination)                          | (siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „NTP Daemon gestoppt“  |
|                     | mbgLtCfgNotifyServerBoot            | string (Kombination)                          | (siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Zeitserver Bootvorgang“   |
|                     | mbgLtCfgNotifyRefclockNotResponding | string (Kombination)                          | (siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Referenzzeitquelle antwortet nicht“   |
|                     | mbgLtCfgNotifyRefclockNotSync       | string (Kombination)                          | (siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Referenzzeitquelle nicht synchron“  |
|                     | mbgLtCfgNotifyAntennaFaulty         | string (Kombination)                          | (siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „GPS Antenne nicht angeschlossen oder defekt“  |
|                     | mbgLtCfgNotifyAntennaReconnect      | string (Kombination)                          | (siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „GPS Antenne wieder OK“  |

| <i>SNMP Zweig</i> | <i>Variable</i>                   | <i>Datentyp</i>                           | <i>Beschreibung</i>   |
|-------------------|-----------------------------------|---|---|
|                   | mbgLtCfgNotifyConfigChanged       | string<br>(Kombination)                   | (siehe mbgLtCfgNotifyNTPNotSync)<br>für das Ereignis „Konfiguration<br>geändert“  |
|                   | mbgLtCfgNotifyLeapSecondAnnounced | string<br>(Kombination)                   | (siehe mbgLtCfgNotifyNTPNotSync)<br>für das Ereignis „Schaltsekunde<br>angekündigt“   |
| mbgLtCfgEthernet  | mbgLtCfgEthernetIf0IPv4IP         | string (IPv4 IP-<br>Adresse)              | IPv4-Adresse des ersten<br>Netzwerkinterfaces des Zeitservers   |
|                   | mbgLtCfgEthernetIf0IPv4Netmask    | string (IPv4<br>Netzmaske)                | IPv4-Netzmaske des ersten<br>Netzwerkinterfaces des Zeitservers   |
|                   | mbgLtCfgEthernetIf0IPv4Gateway    | string (IPv4 IP-<br>Adresse)              | IPv4-Adresse des Default Gateways<br>des ersten Netzwerkinterfaces des<br>Zeitservers   |
|                   | mbgLtCfgEthernetIf0DHCPClient     | integer (0 =<br>disabled, 1 =<br>enabled) | Konfiguration des ersten<br>Netzwerkinterfaces des Zeitservers<br>per DHCP aktiviert?   |
|                   | mbgLtCfgEthernetIf0IPv6IP1        | string (IPv6 IP-<br>Adresse)              | Erste IPv6-IP-Adresse des ersten<br>Netzwerkinterfaces des Zeitservers  |
|                   | mbgLtCfgEthernetIf0IPv6IP2        | string (IPv6 IP-<br>Adresse)              | Zweite IPv6-IP-Adresse des ersten<br>Netzwerkinterfaces des Zeitservers   |
|                   | mbgLtCfgEthernetIf0IPv6IP3        | string (IPv6 IP-<br>Adresse)              | Dritte IPv6-IP-Adresse des ersten<br>Netzwerkinterfaces des Zeitservers   |
|                   | mbgLtCfgEthernetIf0IPv6Autoconf   | integer (0 =<br>disabled, 1 =<br>enabled) | IPv6 - Konfiguration des ersten<br>Netzwerkinterfaces des Zeitservers<br>per Autoconf aktiviert?  |
|                   | mbgLtCfgEthernetIf0NetlinkMode    | integer (0..4)                            | Konfiguration der Ethernet-<br>Geschwindigkeit des ersten<br>Netzwerkinterfaces des Zeitservers<br><br>0 = Autosensing,<br>1 = 10Mbit/s Half Duplex,<br>2= 10Mbit/s Full Duplex,<br>3=100Mbit/s Half Duplex,<br>4=100Mbit/s Full Duplex |

Für alle weiteren im Zeitserver vorhandenen Ethernet Schnittstellen im SNMP-Zweig „mbgLtCfgEthernet“ wird lediglich „If0“ durch „Ifx“ ersetzt, wobei das „x“ die Nummer der entsprechenden Netzwerkschnittstelle darstellt. Beispiel: die IPv4-IP-Adresse der dritten Ethernet Schnittstelle wird mit mbgLtCfgEthernetIf2IPv4IP angesprochen.

## SNMP Traps

Zusätzlich werden vom LANTIME so genannte SNMP-Traps generiert. Dabei handelt es sich um Messages über das SNMP Protokoll, welche asynchron zu bestimmten Bedingungen gesendet werden. Diese Traps können von einem SNMP Trap Dämon empfangen werden: z.B. unter LINUX: "snmptrapd -p" (-p steht für Ausgabe auf der Console; -s steht für Ausgabe ins Syslogfile). Die entsprechenden MIB Dateien können Sie auf dem LANTIME unter /usr/local/share/snmp/mibs/ finden, wobei die LANTIME spezifischen Werte in der MBG\_SNMP\*.txt enthalten sind. Diese MIB kann auch über das Webinterface geladen und dann in Ihren SNMP-Manager importiert werden.

Die folgenden SNMP-Traps werden gesendet:

|                           |   |
|---------------------------|---|
| "NTP not sync"            | NTP nicht synchron zur Referenzzeit                 |
| "NTP stopped"             | NTP wurde angehalten (meist zu große Zeitabweichung |
| "Server boot"             | System wurde neu gestartet                          |
| "Receiver not responding" | keine Antwort von der GPS                           |
| "Receiver not sync"       | GPS Empfänger nicht synchronisiert                  |
| "Antenna faulty"          | GPS Antenne nicht angeschlossen                     |
| "Antenna reconnect"       | GPS Antenne wieder angeschlossen                    |
| "Config changed"          | Systemparameter vom Benutzer geändert               |
| „Leap second announced“   | Schaltsekunde angekündigt                           |

In der Konfiguration können unter dem Menüpunkt NOTIFICATION zwei IP Adressen für SNMP Manager angegeben werden. Die SNMP Traps werden dann zu den eingestellten SNMP Managern gesendet.



## SNMP TRAP Referenz

Alle möglichen Traps können unter der mbgLtTraps Struktur in der Meinberg MIB gefunden werden. Für jedes Notification Ereignis des Zeitservers existiert ein eigener TRAP. Bitte beachten Sie, dass die SNMP TRAPS nur dann gesendet werden, wenn Sie für das jeweilige Ereignis (z.B. NTP not sync) die Benachrichtigungsart „SNMP trap“ konfiguriert haben, ansonsten wird kein TRAP erzeugt/gesendet. Alle TRAPS werden mit einem String Parameter versehen, der eine zum Ereignis passende Textmeldung enthält. Diese Meldungen können Sie an Ihre Bedürfnisse anpassen (siehe entsprechender Abschnitt in den Kapiteln über das Webinterface bzw. das CLI Setup). Folgende Traps sind möglich:

mbgLtTrapNTPNotSync (mbgLtTraps.1): Wenn der NTP Daemon (ntpd) seine Synchronisation verliert, wird dieser TRAP erzeugt und an den/die konfigurierten SNMP trap receiver gesendet.

mbgLtTrapNTPStopped (mbgLtTraps.2): Dieser TRAP wird gesendet, wenn der NTP Daemon gestoppt wird (manuell oder aufgrund eines Fehlers).

mbgLtTrapServerBoot (mbgLtTraps.3): Nach Beendigung jedes Bootprozesses wird dieser Trap generiert.

mbgLtTrapReceiverNotResponding (mbgLtTraps.4): Falls der Empfänger der eingebauten Referenzzeitquelle nicht auf Anfragen des Zeitservers reagiert, wird dieser TRAP gesendet.

mbgLtTrapReceiverNotSync (mbgLtTraps.5): Bei einem Verlust der Synchronisation der Referenzzeitquelle wird den SNMP trap receivers dieser TRAP gesendet.

mbgLtTrapAntennaFaulty (mbgLtTraps.6): Dieser TRAP wird erzeugt, falls die Verbindung zur Antenne der eingebauten Referenzzeitquelle unterbrochen wird.

mbgLtTrapAntennaReconnect (mbgLtTraps.7): Sobald die Antenne wieder korrekt funktioniert, wird dieser TRAP generiert.

mbgLtTrapConfigChanged (mbgLtTraps 8): Bei Konfigurationsänderungen des Zeitservers wird die Konfiguration neu eingelesen, danach wird dieser TRAP erzeugt.

mbgLtTrapLeapSecondAnnounced (mbgLtTraps 9): Dieser TRAP wird gesendet, wenn dem GPS Empfänger eine Schaltsekunde angekündigt worden ist.

mbgLtTrapTestNotification (mbgLtTraps 99): Dieser Test- TRAP wird gesendet, wenn Sie im Webinterface oder CLI Setup Tool eine Testnotification veranlassen und dient lediglich dazu, den Empfang von SNMP Traps zu testen.

## **Anhang: Technische Daten**

### **Nur Service-/Fachpersonal: Austausch der Lithium-Batterie**

Die Lithiumbatterie auf der Hauptplatine hat eine Lebensdauer von mindestens 10 Jahren. Sollte ein Austausch erforderlich werden, ist folgender Hinweis zu beachten:

### **VORSICHT!**

**Explosionsgefahr bei unsachgemäßem Austausch der Batterie. Ersatz nur durch denselben oder einen vom Hersteller empfohlenen gleichwertigen Typ. Entsorgung gebrauchter Batterien nach Angaben des Herstellers.**

### **Technische Daten Lantime Multipack**

|              |  |
|--------------|--|
| GEHÄUSE:     | Baugruppenträger, Schroff EUROPAC lab HF<br>Frontplatte 1HE/84TE (43 mm hoch / 483 mm breit) |
| SCHUTZART:   | IP20   |
| ABMESSUNGEN: | 483 mm x 43 mm x ca.290 mm (B x H x T)   |

## Sicherheitshinweise für Geräte

Dieses Einbaugerät wurde entsprechend den Anforderungen des Standards IEC950 "Sicherheit von Einrichtungen der Informationstechnik, einschließlich elektrischer Büromaschinen" entwickelt und geprüft.

Beim Einbau des Einbaugerätes in ein Endgerät (z.B. Gehäuseschrank) sind zusätzliche Anforderungen gem. Standard IEC 950 zu beachten und einzuhalten.

- o Das Gerät wurde für den Einsatz in Büro- oder ähnlicher Umgebung entwickelt und darf auch nur in solchen Räumen betrieben werden. Für Räume mit größerem Verschmutzungsgrad gelten schärfere Anforderungen.
- o Das Gerät wurde für den Einsatz bei einer maximalen Umgebungstemperatur von 40 °C geprüft.
- o Die Lüftungsöffnungen dürfen nicht abgedeckt werden.
- o Das Gerät ist ein Gerät der Schutzklasse 1 und darf nur an eine geerdete Steckdose angeschlossen werden (TN-System).
- o Zum sicheren Betrieb muss das Gerät durch eine Installationssicherung von max. 16 A abgesichert werden.
- o Der Brandschutz muss im eingebauten Zustand sichergestellt sein.
- o Die Trennung des Gerätes vom Netz erfolgt durch Ziehen des Netzsteckers.
- o Das Gerät darf nur von Fach-/Servicepersonal geöffnet werden.

## CE-Kennzeichnung

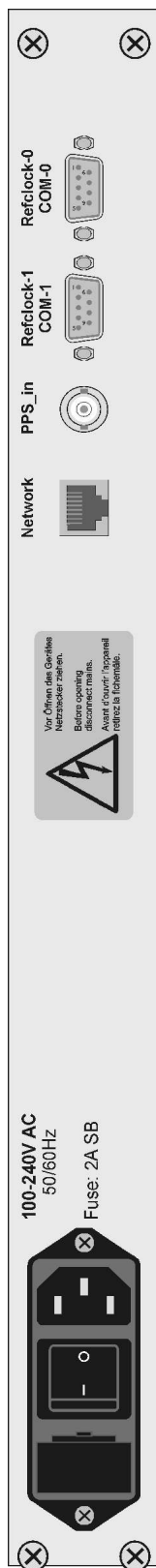


|                            |  |
|----------------------------|--|
| Niederspannungsrichtlinie: | EN 60950   |
|                            | Sicherheit von Einrichtungen der Informationstechnik, einschließlich elektrischer Büromaschinen  |
| EMV-Richtlinie:            | EN50081-1  |
|                            | Elektromagnetische Verträglichkeit, Fachgrundnorm Störaussendung, Teil 1: Wohnbereich, Geschäfts- und Gewerbebereiche sowie Kleinindustrie |
|                            | EN50082-2  |
|                            | Elektromagnetische Verträglichkeit, Fachgrundnorm Störfestigkeit Teil 2: Industriebereich  |

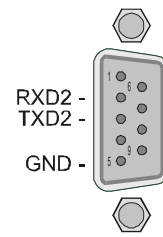
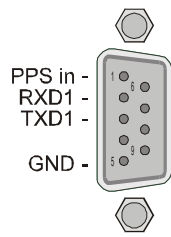
## Rückwandanschlüsse

| <u>Bezeichnung</u> | <u>Steckverbindung</u>                 | <u>Art</u>        | <u>Kabel</u>                      |
|--------------------|--|-------------------|-----------------------------------|
| Netzwerk           | RJ-45                                  | Ethernet          | Datenleitung geschirmt            |
| Refclock-0         | SubD 9 pol-Buchse                      | RS232             | Koax geschirmt                    |
| Refclock-1         | SubD 9 pol-Buchse                      | RS232             | Koax geschirmt                    |
| PPS in             | SubD 9 pol-Buchse                      | TTL oder RS232    | Koax geschirmt *<br>optional über |
| PPS in             | Lötbrücke im Gehäuse<br>BNC-Buchse     | TTL oder RS232    | Koax geschirmt                    |
| Netz               | Kaltger. Stecker<br>nach EN60320 – C13 | 95-240 V AC ±10 % | Kaltgeräteanschlusskabel          |

# Rückansicht LANTIME

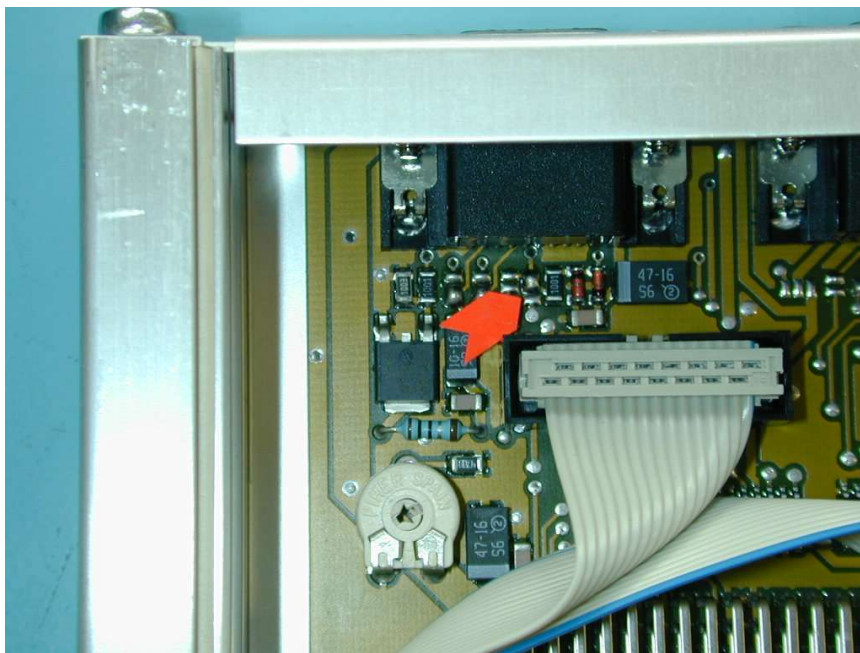


## SUB-D Steckerbelegung

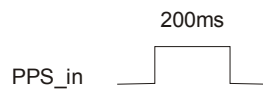


Refclock-0

Refclock-1



Um den PPS-IN über die SUBD Buchse anzuschließen, muss das Gehäuse geöffnet werden und die Lötbrücke wie auf dem Bild angedeutet nach oben gesetzt werden. Der PPS-IN kann entweder TTL oder RS232 Pegel haben.



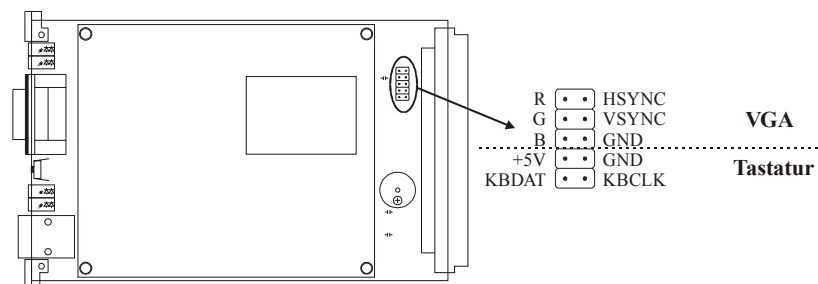
## Technische Daten LAN CPU

|                               |  |
|-------------------------------|--|
| PROZESSOR:                    | Geode™ GX1 mit 266 MHz   |
| HAUPTSPEICHER:                | 32 MB (bis 64 MB erweiterbar)  |
| CACHESPEICHER:                | 16 KB 2nd Level Cache  |
| FLASHDISK:                    | 8 MB (bis maximal 72 MB)   |
| NETZWERK<br>ANBINDUNG:        | 10/100 MBIT über RJ45-Buchse<br>DAVICOM DM9102AEthernet NIC Con<br>troller   |
| SERIELLE -<br>SCHNITTSTELLEN: | Vier serielle RS232-Ports<br>16550 kompatibel mit FIFO<br>davon: eine Schnittstelle über 9-poligen DSUB-<br>Stecker<br>drei Schnittstellen über 96-polige VG-Leiste<br>(nur TxD, RxD, DCD) |
| PARALLELE<br>SCHNITTSTELLE:   | Ein LPT-Port über 96-polige VG-Leiste  |
| IDE-BUS:                      | Primary IDE-Bus über 96-polige VG-Leiste   |
| VGA-ANSCHLUSS:                | Über 10-polige Stiftleiste   |
| TASTATURANSCHLUSS:            | Über 10-polige Stiftleiste   |
| STATUSANZEIGE:                | - Netzversorgung<br>- 'Connect', 'Activity' und 'Speed' der<br>Netzwerkverbindung<br>- Zwei freie LEDs nach Kundenanforderung (L1,L2)  |
| STROMVERSORGUNG:              | 5 V ± 5 %, ca. 1 A   |
| FRONTPLATTE:                  | 3 HE / 4 TE (128 mm hoch x 20,3 mm breit)  |
| STECKVERBINDER:               | Messerleiste DIN 41612, Typ C 96, Reihen a + b + c<br>DSUB-Stecker, 9-polig, RJ45-Buchse   |
| UMGEBUNGS-<br>TEMPERATUR:     | 0 ... 50 °C  |
| LUFTFEUCHTIGKEIT:             | 85 % max.  |

## Steckerbelegung

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

## Belegung der Stiftleiste (VGA, Tastatur)





## Zeitlegramme

### Format des Meinberg Standard-Zeitlegramms

Das Meinberg Standard-Zeitlegramm besteht aus einer Folge von 32 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Das Format ist:

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

Die *kursiv* gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|          |  |
|----------|--|
| <STX>    | Startzeichen (Start-Of-Text, ASCII-Code 02h)<br>wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet   |
| tt.mm.jj | das Datum:<br><i>tt</i> Monatstag                    (01..31)<br><i>mm</i> Monat                      (01..12)<br><i>jj</i> Jahr ohne Jahrhundert      (00..99)<br><i>w</i> Wochentag                  (1..7, 1 = Montag)  |
| hh.mm.ss | die Zeit:<br><i>hh</i> Stunden                    (00..23)<br><i>mm</i> Minuten                    (00..59)<br><i>ss</i> Sekunden                   (00..59, oder 60 wenn Schaltsekunde)   |
| uv       | Status der Funkuhr: (abhängig vom Funkuhrentyp)<br><i>u</i> :    ‘#’ GPS : Uhr läuft frei (ohne genaue Zeitsynchronisation)<br>PZF: Zeitraster nicht synchronisiert<br>DCF77: Uhr hat seit dem Einschalten nicht synchr.<br>‘ ‘ (Leerzeichen, 20h)<br>GPS: Uhr läuft GPS synchron (Grundgenauig. erreicht)<br>PZF: Zeitraster synchronisiert<br>DCF77: Synchr. nach letztem Einschalten erfolgt<br><br><i>v</i> :    ‘*’ GPS: Empfänger hat die Position noch nicht überprüft<br>PZF/DCF77: Uhr läuft im Moment auf Quarzbasis<br>‘ ‘ (Leerzeichen, 20h)<br>GPS: Empfänger hat seine Position bestimmt<br>PZF/DCF77: Uhr wird vom Sender geführt |
| x        | Kennzeichen der Zeitzone:<br>‘U’    UTC    Universal Time Coordinated, früher GMT<br>‘ ‘    MEZ    Mittleuropäische Standardzeit<br>‘S’    MESZ   Mittleuropäische Sommerzeit  |
| y        | Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:<br>‘!’    Ankündigung Beginn oder Ende der Sommerzeit<br>‘A’    Ankündigung einer Schaltsekunde<br>‘ ‘    (Leerzeichen, 20h) kein Zeitsprung angekündigt  |
| <ETX>    | Ende-Zeichen (End-Of-Text, ASCII-Code 03h)   |

## Format des GPS167 Capture-Telegramms

Das Meinberg GPS167-Capturetelegramm besteht aus einer Folge von 31 ASCII-Zeichen, abgeschlossen durch eine CR/LF (Carriage Return/Line Feed) Sequenz. Das Format ist:

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

Die *kursiv* gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|                         |   |
|-------------------------|---|
| x                       | 0 oder 1, Nummer des Eingangs                 |
| _                       | ASCII space 20h                               |
| <i>tt.mm.jj</i>         | das Datum:                                    |
| <i>tt</i>               | Monatstag (01..31)                            |
| <i>mm</i>               | Monat (01..12)                                |
| <i>jj</i>               | Jahr ohne Jahrhundert (00..99)                |
| <i>hh:mm:ss.fffffff</i> | die Zeit:                                     |
| <i>hh</i>               | Stunden (00..23)                              |
| <i>mm</i>               | Minuten (00..59)                              |
| <i>ss</i>               | Sekunden (00..59, oder 60 wenn Schaltsekunde) |
| <i>fffffff</i>          | Bruchteile der Sekunden, 7 Stellen            |
| <CR>                    | Carriage Return, ASCII code 0Dh               |
| <LF>                    | Line Feed, ASCII code 0Ah                     |

## Format des SAT-Zeitlegramms

Das SAT-Zeitlegramm besteht aus einer Folge von 29 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Das Format ist:

<STX>*tt.mm.jj/w/hh:mm:ssxxxuv*<CR><LF><ETX>

Die *kursiv* gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|                 |   |
|-----------------|---|
| <STX>           | Startzeichen (Start-Of-Text, ASCII-Code 02h)<br>wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet  |
| <i>tt.mm.jj</i> | das Datum:<br><i>tt</i> Monatstag (01..31)<br><i>mm</i> Monat (01..12)<br><i>jj</i> Jahr ohne Jahrhundert (00..99)<br><i>w</i> der Wochentag (1..7, 1 = Montag)                     |
| <i>hh:mm:ss</i> | die Zeit:<br><i>hh</i> Stunden (00..23)<br><i>mm</i> Minuten (00..59)<br><i>ss</i> Sekunden (00..59, oder 60 wenn Schaltsekunde)  |
| <i>xxxx</i>     | Kennzeichen der Zeitzone:<br>UTC Universal Time Coordinated, früher GMT<br>MEZ Mitteleuropäische Standardzeit<br>MESZ Mitteleuropäische Sommerzeit                                  |
| <i>u</i>        | Status der Funkuhr:<br>'*' GPS-Empfänger hat seine Position noch nicht überprüft<br>' ' (Leerz., 20h) GPS-Empfänger hat seine Position bestimmt                                     |
| <i>v</i>        | Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:<br>'!' Ankündigung Beginn oder Ende der Sommerzeit<br>' ' (Leerzeichen, 20h) kein Zeitsprung angekündigt |
| <CR>            | Wagenrücklauf-Zeichen (Carriage-Return, ASCII-Code 0Dh)   |
| <LF>            | Zeilenvorschub-Zeichen (Line-Feed, ASCII-Code 0Ah)  |
| <ETX>           | Ende-Zeichen (End-Of-Text, ASCII-Code 03h)  |

## Format des Telegramms Uni Erlangen (NTP)

Das Zeitlegramm Uni Erlangen (NTP) einer **GPS-Funkuhr** besteht aus einer Folge von 66 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Das Format ist:

*<STX>tt.mm.jj; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn ll.lllle hhhhm<ETX>*

Die *kursiv* gedruckten Zeichen werden durch Ziffern oder Buchstaben ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|                    |  |   |   |   |  |         |   |           |                       |   |          |               |   |
|--------------------|--|---|---|---|--|---------|---|-----------|-----------------------|---|----------|---------------|---|
| <i>&lt;STX&gt;</i> | Startzeichen (Start-Of-Text, ASCII-Code 02h)<br>wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet   |   |   |   |  |         |   |           |                       |   |          |               |   |
| <i>tt.mm.jj</i>    | das Datum:<br><table><tr><td><i>tt</i></td><td>Monatstag</td><td>(01..31)</td></tr><tr><td><i>mm</i></td><td>Monat</td><td>(01..12)</td></tr><tr><td><i>jj</i></td><td>Jahr ohne Jahrhundert</td><td>(00..99)</td></tr><tr><td><i>w</i></td><td>der Wochentag</td><td>(1..7, 1 = Montag)</td></tr></table>   | <i>tt</i>   | Monatstag                                   | (01..31)  | <i>mm</i>                                      | Monat   | (01..12)  | <i>jj</i> | Jahr ohne Jahrhundert | (00..99)  | <i>w</i> | der Wochentag | (1..7, 1 = Montag)                                  |
| <i>tt</i>          | Monatstag  | (01..31)  |   |   |  |         |   |           |                       |   |          |               |   |
| <i>mm</i>          | Monat  | (01..12)  |   |   |  |         |   |           |                       |   |          |               |   |
| <i>jj</i>          | Jahr ohne Jahrhundert  | (00..99)  |   |   |  |         |   |           |                       |   |          |               |   |
| <i>w</i>           | der Wochentag  | (1..7, 1 = Montag)                                    |   |   |  |         |   |           |                       |   |          |               |   |
| <i>hh:mm:ss</i>    | die Zeit:<br><table><tr><td><i>hh</i></td><td>Stunden</td><td>(00..23)</td></tr><tr><td><i>mm</i></td><td>Minuten</td><td>(00..59)</td></tr><tr><td><i>ss</i></td><td>Sekunden</td><td>(00..59, oder 60 wenn Schaltsekunde)</td></tr></table>  | <i>hh</i>   | Stunden                                     | (00..23)  | <i>mm</i>                                      | Minuten | (00..59)  | <i>ss</i> | Sekunden              | (00..59, oder 60 wenn Schaltsekunde)                  |          |               |   |
| <i>hh</i>          | Stunden  | (00..23)  |   |   |  |         |   |           |                       |   |          |               |   |
| <i>mm</i>          | Minuten  | (00..59)  |   |   |  |         |   |           |                       |   |          |               |   |
| <i>ss</i>          | Sekunden   | (00..59, oder 60 wenn Schaltsekunde)                  |   |   |  |         |   |           |                       |   |          |               |   |
| <i>v</i>           | Vorzeichen des Offsets der lokalen Zeitzone zu UTC   |   |   |   |  |         |   |           |                       |   |          |               |   |
| <i>oo:oo</i>       | Offset der lokalen Zeitzone zu UTC in Stunden und Minuten  |   |   |   |  |         |   |           |                       |   |          |               |   |
| <i>ac</i>          | Status der Funkuhr:<br><table><tr><td><i>a:</i></td><td>'#'</td><td>Uhr hat seit dem Einschalten nicht synchronisiert</td></tr><tr><td></td><td>' '</td><td>(Leerz., 20h) Uhr hat bereits einmal synchronisiert</td></tr><tr><td><i>c:</i></td><td>'*'</td><td>GPS-Empfänger hat seine Position noch nicht überprüft</td></tr><tr><td></td><td>' '</td><td>(Leerz., 20h) Empfänger hat seine Position bestimmt</td></tr></table> | <i>a:</i>   | '#'   | Uhr hat seit dem Einschalten nicht synchronisiert |  | ' '     | (Leerz., 20h) Uhr hat bereits einmal synchronisiert | <i>c:</i> | '*'                   | GPS-Empfänger hat seine Position noch nicht überprüft |          | ' '           | (Leerz., 20h) Empfänger hat seine Position bestimmt |
| <i>a:</i>          | '#'  | Uhr hat seit dem Einschalten nicht synchronisiert     |   |   |  |         |   |           |                       |   |          |               |   |
|                    | ' '  | (Leerz., 20h) Uhr hat bereits einmal synchronisiert   |   |   |  |         |   |           |                       |   |          |               |   |
| <i>c:</i>          | '*'  | GPS-Empfänger hat seine Position noch nicht überprüft |   |   |  |         |   |           |                       |   |          |               |   |
|                    | ' '  | (Leerz., 20h) Empfänger hat seine Position bestimmt   |   |   |  |         |   |           |                       |   |          |               |   |
| <i>d</i>           | Kennzeichen der Zeitzone:<br><table><tr><td>'S'</td><td>MESZ</td><td>Mitteuropäische Sommerzeit</td></tr><tr><td>' '</td><td>MEZ</td><td>Mitteuropäische Standardzeit</td></tr></table>  | 'S'   | MESZ  | Mitteuropäische Sommerzeit                        | ' '  | MEZ     | Mitteuropäische Standardzeit                        |           |                       |   |          |               |   |
| 'S'                | MESZ   | Mitteuropäische Sommerzeit                            |   |   |  |         |   |           |                       |   |          |               |   |
| ' '                | MEZ  | Mitteuropäische Standardzeit                          |   |   |  |         |   |           |                       |   |          |               |   |
| <i>f</i>           | Ankündigung Beginn oder Ende der Sommerzeit während der letzten Stunde vor dem Ereignis:<br><table><tr><td>'!'</td><td>Ankündigung Beginn oder Ende der Sommerzeit</td></tr><tr><td>' '</td><td>(Leerzeichen, 20h) kein Zeitsprung angekündigt</td></tr></table>   | '!'   | Ankündigung Beginn oder Ende der Sommerzeit | ' '   | (Leerzeichen, 20h) kein Zeitsprung angekündigt |         |   |           |                       |   |          |               |   |
| '!'                | Ankündigung Beginn oder Ende der Sommerzeit  |   |   |   |  |         |   |           |                       |   |          |               |   |
| ' '                | (Leerzeichen, 20h) kein Zeitsprung angekündigt   |   |   |   |  |         |   |           |                       |   |          |               |   |
| <i>g</i>           | Ankündigung einer Schaltsekunde während der letzten Stunde vor dem Ereignis:<br><table><tr><td>'A'</td><td>Ankündigung einer Schaltsekunde</td></tr><tr><td>' '</td><td>(Leerzeichen, 20h) kein Zeitsprung angekündigt</td></tr></table>   | 'A'   | Ankündigung einer Schaltsekunde             | ' '   | (Leerzeichen, 20h) kein Zeitsprung angekündigt |         |   |           |                       |   |          |               |   |
| 'A'                | Ankündigung einer Schaltsekunde  |   |   |   |  |         |   |           |                       |   |          |               |   |
| ' '                | (Leerzeichen, 20h) kein Zeitsprung angekündigt   |   |   |   |  |         |   |           |                       |   |          |               |   |

|                 |  |
|-----------------|--|
| <i>i</i>        | Schaltsekunde<br>'L' Schaltsekunde wird momentan eingefügt<br>(nur in 60. sec aktiv)<br>' ' (Leerzeichen, 20h) Schaltsekunde nicht aktiv |
| <i>bbb.bbbb</i> | Geographische Breite der Empfängerposition in Grad<br>führende Stellen werden mit Leerzeichen (20h) aufgefüllt                           |
| <i>n</i>        | Geographische Breite, mögliche Zeichen sind:<br>'N' nördlich d. Äquators<br>'S' südlich d. Äquators                                      |
| <i>lll.llll</i> | Geographische Länge der Empfängerposition in Grad<br>führende Stellen werden mit Leerzeichen (20h) aufgefüllt                            |
| <i>e</i>        | Geographische Länge, mögliche Zeichen sind:<br>'E' östlich Greenwich<br>'W' westlich Greenwich   |
| <i>hhh</i>      | Höhe der Empfängerposition über Normalnull in Metern<br>führende Stellen werden mit Leerzeichen (20h) aufgefüllt                         |
| <ETX>           | Ende-Zeichen (End-Of-Text, ASCII-Code 03h)   |

## Format des NMEA Telegramms (RMC)

Das NMEA Telegramm besteht aus einer Folge von 65 ASCII-Zeichen, eingeleitet durch das Zeichen '\$' und abgeschlossen durch die Zeichen CR (Carriage Return) und LF (Line Feed). Das Format ist:

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

Die *kursiv* gedruckten Zeichen werden durch Ziffern oder Buchstaben ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|                  |   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
|------------------|---|--------------------------------------|-----------|----------|-----------|---------|----------|-----------|-----------------------|--------------------------------------|-----------|----------|----------------|
| \$               | Startzeichen (ASCII-Code 24h)<br>wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>hhmmss.ss</i> | die Zeit:<br><table> <tr> <td><i>hh</i></td> <td>Stunden</td> <td>(00..23)</td> </tr> <tr> <td><i>mm</i></td> <td>Minuten</td> <td>(00..59)</td> </tr> <tr> <td><i>ss</i></td> <td>Sekunden</td> <td>(00..59, oder 60 wenn Schaltsekunde)</td> </tr> <tr> <td><i>ss</i></td> <td>Sekunden</td> <td>(1/10 ; 1/100)</td> </tr> </table> | <i>hh</i>                            | Stunden   | (00..23) | <i>mm</i> | Minuten | (00..59) | <i>ss</i> | Sekunden              | (00..59, oder 60 wenn Schaltsekunde) | <i>ss</i> | Sekunden | (1/10 ; 1/100) |
| <i>hh</i>        | Stunden   | (00..23)                             |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>mm</i>        | Minuten   | (00..59)                             |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>ss</i>        | Sekunden  | (00..59, oder 60 wenn Schaltsekunde) |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>ss</i>        | Sekunden  | (1/10 ; 1/100)                       |           |          |           |         |          |           |                       |                                      |           |          |                |
| A                | Status (A = Zeitdaten gültig)<br>(V = Zeitdaten ungültig)   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>bbbb.bb</i>   | Geographische Breite der Empfängerposition in Grad<br>führende Stellen werden mit Leerzeichen (20h) aufgefüllt  |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>n</i>         | Geographische Breite, mögliche Zeichen sind:<br>'N' nördlich d. Äquators<br>'S' südlich d. Äquators   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>llll.ll</i>   | Geographische Länge der Empfängerposition in Grad<br>führende Stellen werden mit Leerzeichen (20h) aufgefüllt   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>e</i>         | Geographische Länge, mögliche Zeichen sind:<br>'E' östlich Greenwich<br>'W' westlich Greenwich  |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>ddmmyy</i>    | das Datum:<br><table> <tr> <td><i>dd</i></td> <td>Monatstag</td> <td>(01..31)</td> </tr> <tr> <td><i>mm</i></td> <td>Monat</td> <td>(01..12)</td> </tr> <tr> <td><i>yy</i></td> <td>Jahr ohne Jahrhundert</td> <td>(00..99)</td> </tr> </table>   | <i>dd</i>                            | Monatstag | (01..31) | <i>mm</i> | Monat   | (01..12) | <i>yy</i> | Jahr ohne Jahrhundert | (00..99)                             |           |          |                |
| <i>dd</i>        | Monatstag   | (01..31)                             |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>mm</i>        | Monat   | (01..12)                             |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>yy</i>        | Jahr ohne Jahrhundert   | (00..99)                             |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>a</i>         | magnetische Variation E/W   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <i>hh</i>        | Prüfsumme (XOR über alle Zeichen außer '\$' und '*')  |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <CR>             | Carriage-Return; ASCII-Code 0Dh   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |
| <LF>             | Line-Feed; ASCII-Code 0Ah   |                                      |           |          |           |         |          |           |                       |                                      |           |          |                |

## Format des ABB-SPA-Zeitlegramms

Das ABB-SPA-Zeitlegramm besteht aus einer Folge von 32 ASCII-Zeichen, eingeleitet durch die Zeichenfolge ">900WD:" und abgeschlossen durch das Zeichen <CR> (Carriage Return). Das Format ist:

**>900WD:*jj-mm-tt\_hh.mm;ss.fff:cc*<CR>**

Die *kursiv* gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|                     |            |   |                                      |
|---------------------|------------|---|--------------------------------------|
| <i>jj-mm-tt</i>     | das Datum: |   |                                      |
|                     | <i>jj</i>  | Jahr ohne Jahrhundert   | (00..99)                             |
|                     | <i>mm</i>  | Monat   | (01..12)                             |
|                     | <i>tt</i>  | Monatstag   | (01..31)                             |
|                     |            | Leerzeichen (ASCII-code 20h)  |                                      |
| <i>hh.mm;ss.fff</i> | die Zeit:  |   |                                      |
|                     | <i>hh</i>  | Stunden   | (00..23)                             |
|                     | <i>mm</i>  | Minuten   | (00..59)                             |
|                     | <i>ss</i>  | Sekunden  | (00..59, oder 60 wenn Schaltsekunde) |
|                     | <i>fff</i> | Millisekunden   | (000..999)                           |
| <i>cc</i>           |            | Prüfsumme. Die Berechnung erfolgt durch Exklusiv-Oder-Verknüpfung der vorhergehenden Zeichen, dargestellt wird der resultierende Byte-Wert im Hex-Format (2 ASCII-Zeichen '0' bis '9' oder 'A' bis 'F') |                                      |
| <CR>                |            | Carriage Return (ASCII-Code 0Dh)  |                                      |

## Format des Computime-Zeitlegramms

Das Computime-Zeitlegramm besteht aus einer Folge von 24 ASCII-Zeichen, eingeleitet durch das Zeichen T und abgeschlossen durch das Zeichen LF (Line-Feed, ASCII-Code 0Ah). Das Format ist:

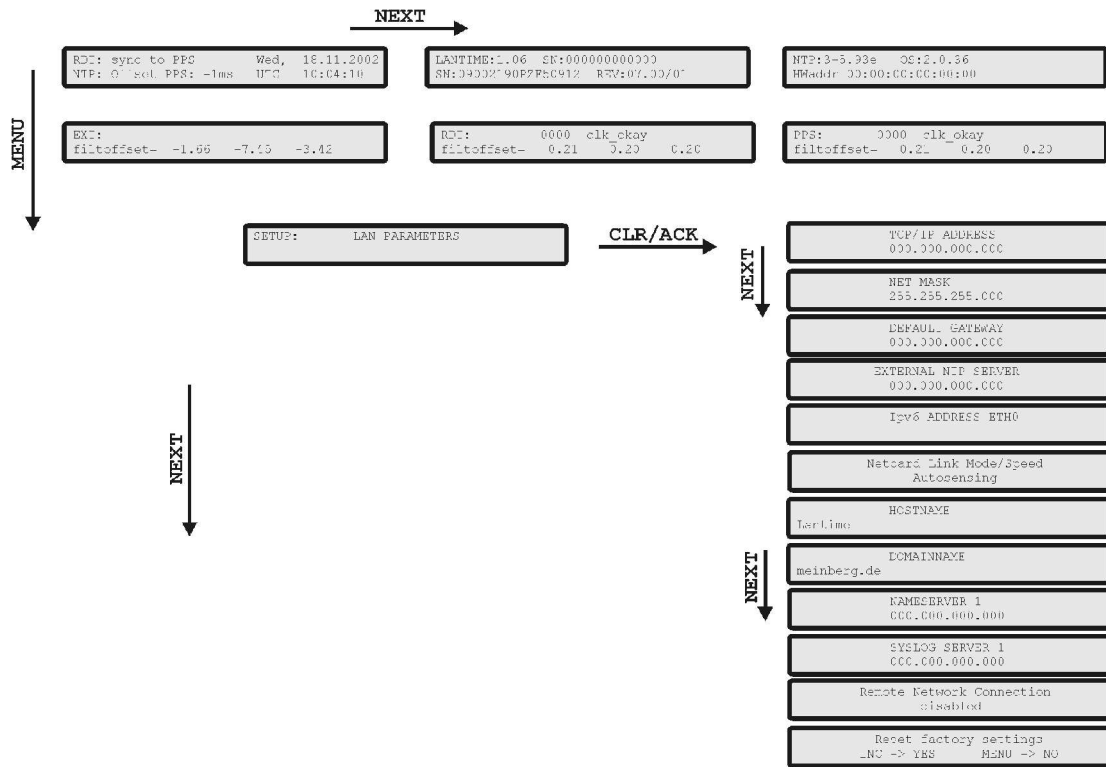
**T:jj:mm:tt:ww:hh:mm:ss<CR><LF>**

Die *kursiv* gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeitlegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

|                 |   |  |
|-----------------|---|--|
| T               | Startzeichen  | wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet |
| <i>jj:mm:tt</i> | das Datum:  |  |
| <i>jj</i>       | Jahr ohne Jahrhundert                                   | (00..99)   |
| <i>mm</i>       | Monat   | (01..12)   |
| <i>tt</i>       | Monatstag   | (01..31)   |
| <i>ww</i>       | Wochentag   | (01..07, 01 = Montag)  |
| <i>hh:mm:ss</i> | die Zeit:   |  |
| <i>hh</i>       | Stunden   | (00..23)   |
| <i>mm</i>       | Minuten   | (00..59)   |
| <i>ss</i>       | Sekunden  | (00..59, oder 60 wenn Schaltsekunde)                             |
| <CR>            | Wagenrücklauf-Zeichen (Carriage-Return, ASCII-Code 0Dh) |  |
| <LF>            | Zeilenvorschub-Zeichen (Line-Feed, ASCII-Code 0Ah)      |  |



# Kurzübersicht LANTIME Bedienung



## Konformitätserklärung

### Declaration of Conformity

Hersteller  
Manufacturer

**Meinberg Funkuhren GmbH & Co. KG**  
**Auf der Landwehr 22**  
**D-31812 Bad Pyrmont**

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

Produktbezeichnung  
Product Name

**NTP Timeserver**

Modell / Typ  
Model Designation

**Lantime/RDT**

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

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

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

Bad Pyrmont, den 08.05.2002

  
Authorized Signature

## Manuelle Displaysteuerung VP100/NET

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. Specify 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 heard 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)

## Konfigurationsdatei

In dieser Datei werden alle globalen Parameter des Zeitservers abgelegt. Diese Datei befindet sich auf der schreibgeschützten Flashdisk unter `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]:

```

## Globale Optionen Datei

In dieser Datei werden alle globalen Optionen des Zeitservers abgelegt. Diese Datei befindet sich auf der schreibgeschützten Flashdisk unter /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

```

## **Eingesetzte Software von Drittherstellern**

Der LANTIME Netzwerk Zeitserver führt eine Reihe von Software aus, die auf der Arbeit von OpenSource Projekten basieren. Sehr viele Personen haben bei der Entwicklung und Realisierung dieser Software mitgearbeitet. Wir bedanken uns ausdrücklich für diese Arbeit.

Die eingesetzte OpenSource-Software unterliegt ihren eigenen Lizenzbedingungen, die wir im Folgenden auflisten. Sollte der Einsatz einer eingesetzten Software deren Lizenzbestimmungen verletzen, werden wir nach Mitteilung unverzüglich dafür sorgen, dass diese Lizenzbestimmungen wieder eingehalten werden.

Ist für eins der eingesetzten Software-Produkte vorgeschrieben, dass der zugrundeliegende Quellcode von der Firma Meinberg zur Verfügung gestellt werden muss, senden wir Ihnen auf Anfrage entweder einen Datenträger oder eine E-Mail zu oder wir stellen Ihnen einen Link zur Verfügungen, unter dem Sie die aktuellste Version des Quellcodes im Internet beziehen können. Bitte beachten Sie, dass wir bei Zusendung eines Datenträgers die dabei anfallenden Kosten in Rechnung stellen müssen.

### **Betriebssystem GNU/Linux**

Die Weitergabe des GNU/Linux Betriebssystems unterliegt der GNU General Public License, die wir weiter unten abdrucken.

Mehr zu GNU/Linux finden Sie auf der GNU-Homepage ([www.gnu.org](http://www.gnu.org)) sowie auf der Homepage von GNU/Linux ([www.linux.org](http://www.linux.org)).

Der eingesetzte Kernel wurde mithilfe des PPSkit – Patches von Ulrich Windl für den Einsatz mit einer PPS-Referenzzeitquelle optimiert.

### **Samba**

Die Samba Software Suite ist eine Gruppe von Programmen, die das Server Message Block (abgekürzt SMB) Protokoll für UNIX Systeme implementiert. Durch den Einsatz von Samba ist das Senden von Windows Popup Meldungen sowie die Abfrage der Zeit durch Clients mithilfe des NET TIME Befehls möglich.

Die Weitergabe von Samba unterliegt – wie bei GNU/Linux – der GNU General Public License, siehe Abdruck weiter unten.

Die Website des Samba – Projekts (bzw. einen Mirror) finden Sie unter [www.samba.org](http://www.samba.org)!

## Network Time Protocol Version 4 (NTP)

Das von David L. Mills geleitete NTP-Projekt ist im Internet unter [www.ntp.org](http://www.ntp.org) erreichbar, dort finden sich eine Fülle von Informationen und Anleitungen zum Einsatz dieses Standard-Softwarepakets. Die Weitergabe und der Einsatz der NTP-Software ist erlaubt, solange der folgende Hinweis in der Dokumentation vorhanden ist:

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

## mini\_httpd

Für die webbasierende Konfigurationsoberfläche (sowohl HTTP als auch HTTPS) setzen wir den mini\_httpd von ACME Labs ein. Die Weitergabe und Nutzung dieses Programms setzt voraus, dass man folgenden Hinweis abdruckt:

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

```
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
```

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

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

Mehr zu mini\_httpd finden Sie auf der ACME Labs Homepage ([www.acme.com](http://www.acme.com)).



# GNU General Public License (GPL)

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

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

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

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

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source

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

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

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

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

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

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

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

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

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

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

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

#### NO WARRANTY

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

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

END OF TERMS AND CONDITIONS

## Timecode (optional)

### Allgemeines

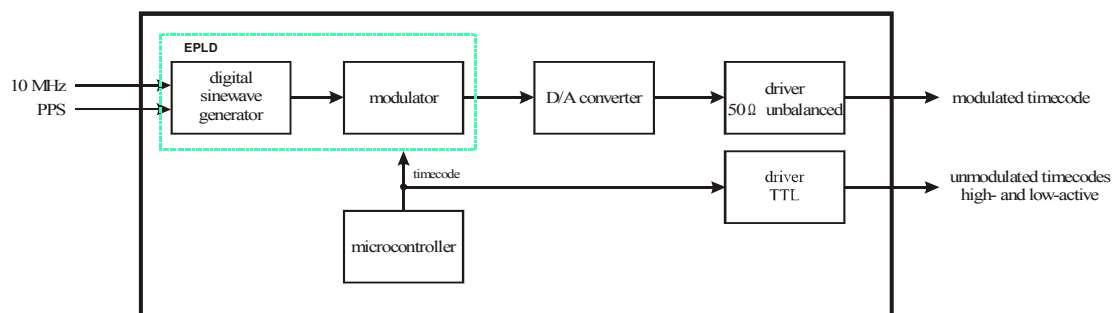
Schon zu Beginn der fünfziger Jahre erlangte die Übertragung codierter Zeitinformation allgemeine Bedeutung. Speziell das amerikanische Raumfahrtprogramm forcierte die Entwicklung dieser zur Korrelation aufgezeichneter Meßdaten verwendeten Zeitcodes. Die Festlegung von Format und Gebrauch dieser Signale war dabei willkürlich und lediglich von den Vorstellungen der jeweiligen Anwender abhängig. Es entwickelten sich hunderte unterschiedlicher Zeitcodes von denen Anfang der sechziger Jahre einige von der "Inter Range Instrumentation Group" (IRIG) standardisiert wurden, die heute als "IRIG Time Codes" bekannt sind.

Neben diesen Zeitsignalen werden jedoch weiterhin auch andere Codes, wie z.B. NASA36, XR3 oder 2137, benutzt. Die GPS167-TC beschränkt sich jedoch auf die Generierung des IRIG-B Formats, auf den in Frankreich genormten AFNOR NFS-87500 Code, sowie auf den IEEE1344 Code. IEEE1344 ist ein IRIG-B123 Code der um Informationen über Zeitzone, Schaltsekunden und Datum erweitert wurde. Auf Wunsch können auch andere Übertragungsarten realisiert werden.

### Funktionsweise

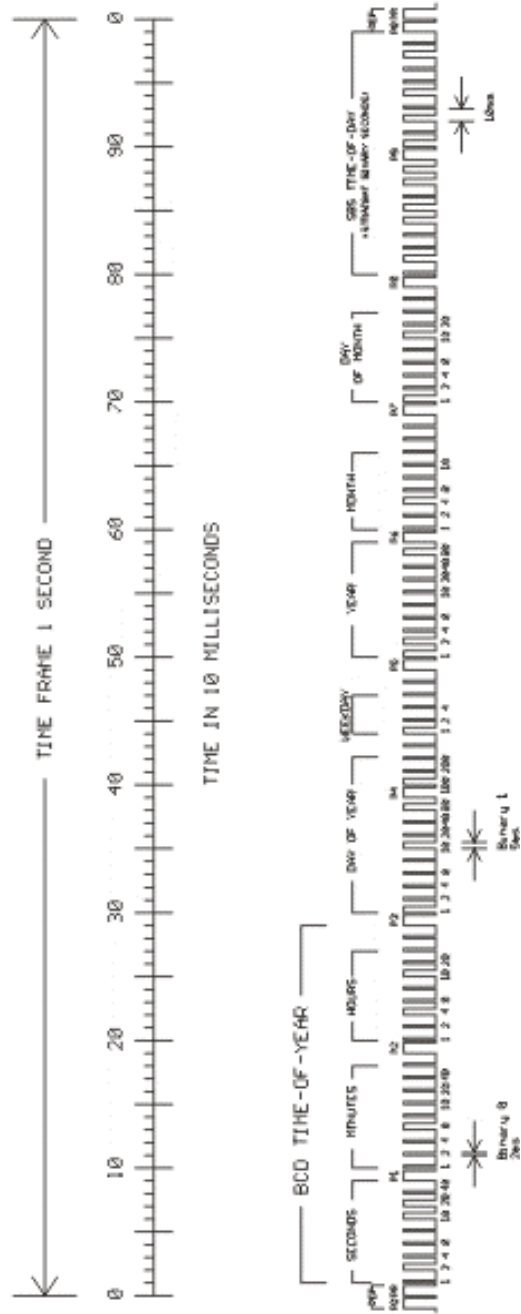
Die Europakarte GPS167-TC wurde speziell zur Erzeugung von IRIG, AFNOR und IEEE1344 Zeitcodes erweitert. Neben dem digital erzeugten amplitudenmodulierten Code wird parallel auch der unmodulierte DC-Pegel IRIG bzw. AFNOR Code bereitgestellt.

### Blockschaltbild Generierung des Timecodes





# AFNOR - Standardformat



## Belegung des CF Segmentes beim IEEE1344 Code

| Bit Nr.  | Bedeutung                     | Beschreibung   |
|--|-------------------------------|--|
| 49   | Position Identifier P5        |  |
| 50   | Year BCD encoded 1            | unteres Nibble des BCD codierten Jahres  |
| 51   | Year BCD encoded 2            |  |
| 52   | Year BCD encoded 4            |  |
| 53   | Year BCD encoded 8            |  |
| 54   | empty, always zero            |  |
| 55   | Year BCD encoded 10           | oberes Nibble des BCD codierten Jahres   |
| 56   | Year BCD encoded 20           |  |
| 57   | Year BCD encoded 40           |  |
| 58   | Year BCD encoded 80           |  |
| 59   | Position Identifier P6        |  |
| 60   | LSP - Leap Second Pending     | bis zu 59s vor Schaltsekunde gesetzt   |
| 61   | LS - Leap Second              | 0 = LS einfügen, 1 = LS löschen <sup>1)</sup>  |
| 62   | DSP - Daylight Saving Pending | bis zu 59s vor SZ/WZ Umschaltung gesetzt   |
| 63   | DST - Daylight Saving Time    | gesetzt während Sommerzeit   |
| 64   | Timezone Offset Sign          | Vorzeichen des Zeitonenoffsets 0 = '+', 1 = '-'  |
| 65   | TZ Offset binary encoded 1    | Offset der IRIG Zeit gegenüber UTC<br>IRIG Zeit PLUS Zeitonenoffset ( einschließlich Vorzeichen ) ergibt immer UTC |
| 66   | TZ Offset binary encoded 2    |  |
| 67   | TZ Offset binary encoded 4    |  |
| 68   | TZ Offset binary encoded 8    |  |
| 69   | Position Identifier P7        |  |
| 70   | TZ Offset 0.5 hour            | gesetzt bei zusätzlichem halbstündigen Offset  |
| 71   | TFOM Time figure of merit     | TFOM gibt den ungefähren Fehler der Zeitquelle an <sup>2)</sup><br>0x00 = Uhr synchron<br>0x0F = Uhr im Freilauf   |
| 72   | TFOM Time figure of merit     |  |
| 73   | TFOM Time figure of merit     |  |
| 74   | TFOM Time figure of merit     |  |
| 75   | PARITY                        | Parität aller vorangegangenen Bits   |
| <sup>1)</sup> von der Firmware werden nur eingefügte Schaltsekunden ( 59->60->00 ) unterstützt !   |                               |  |
| <sup>2)</sup> TFOM wird auf 0 gesetzt wenn die Uhr nach dem Einschalten einmal synchronisieren konnte, andere Codierungen werden von der Firmware nicht unterstützt. s.a. Auswahl des generierten Zeitcodes. |                               |  |



## Generierte Zeitcodes

Das Board verfügt neben dem amplitudenmodulierten Sinuskanal auch über einen unmodulierten TTL Ausgang zur Ausgabe des pulsweitenmodulierten DC-Signals, so dass sechs unterschiedliche Zeitcodes verfügbar sind:

- a) B002: 100 pps, PWM DC Signal, kein Träger  
BCD time-of-year
- b) B122: 100 pps, AM Sinussignal, 1 kHz Trägerfrequenz  
BCD time-of-year
- c) B003: 100 pps, PWM DC Signal, kein Träger  
BCD time-of-year, SBS time-of-day
- d) B123: 100 pps, AM Sinussignal, 1 kHz Trägerfrequenz  
BCD time-of-year, SBS time-of-day
- e) AFNOR: Code lt. NFS-87500, 100 pps, AM Sinussignal,  
1kHz Träger, BCD time-of-year, vollständiges Datum,  
SBS time-of-day, Ausgangspegel angepasst.
- f) IEEE1344: Code lt. IEEE1344-1995, 100 pps, AM Sinussignal,  
1kHz Träger, BCD time-of-year, SBS time-of-day,  
IEEE1344 Erweiterungen für Datum, Zeitzone,  
Sommer/Winterzeit und Schaltsekunde im Control  
Funktions Segment (CF)

*s.a. Tabelle Belegung des CF-Segmentes beim IEEE1344 Code*

## Auswahl des generierten Zeitcodes

Der generierte Zeitcode kann über das Menue Setup IRIG Settings oder das GPS Monitorprogramm ausgewählt werden. Die DC-Level Shift Codes B00x und modulierten Codes mit Sinusträger B12x werden immer parallel erzeugt und sind an verschiedenen Pins der VG64 Steckerleiste abnehmbar. Wird zum Beispiel der Code B122 gewählt, so ist parallel auch der Code B002 verfügbar. Gleiches gilt für die Codes IEEE1344 und AFNOR NFS 87-500.

Das TFOM Segment des IEEE1344 Codes wird in Abhängigkeit des im Zeitstring gesendeten 'already sync'ed' Zeichens ('#') gesetzt. Dieses Zeichen wird immer dann gesetzt wenn die Uhr nach dem Einschalten noch *nicht* synchronisiert hat. Für das 'time figure of merit' (TFOM) Segment des IEEE1344 Codes gilt:

Uhr hat nach dem Einschalten einmal synchronisiert : TFOM = 0000  
Uhr hat nach dem Einschalten noch nicht synchronisiert : TFOM = 1111

Zu Testzwecken lässt sich die Ausgabe des TFOM Segmentes im IEEE1344 Code abschalten. Das Segment wird dann immer auf 0000 gesetzt.

## **Ausgänge**

Die GPS167-ZTC stellt modulierte und unmodulierte Ausgänge zur Verfügung. Das Format der IRIG-Ausgänge kann den Abbildungen "IRIG-B" und "AFNOR Standardformat" entnommen werden.

### **AM - Ausgang**

Der amplitudenmodulierte Sinusträger steht an der VG-Leiste Pin 14a zur Verfügung. Die Trägerfrequenz beträgt 1 kHz (IRIG-B). Das Signal hat eine Amplitude von  $3 V_{ss}$  (MARK) bzw.  $1 V_{ss}$  (SPACE) an  $50 \Omega$ . Über die Anzahl der MARK-Amplituden bei zehn Trägerschwingungen erfolgt die Codierung. Dabei gelten folgende Vereinbarungen:

- a) binär "0":                      2 MARK-Amplituden, 8 SPACE-Amplituden
- b) binär "1":                      5 MARK-Amplituden, 5 SPACE-Amplituden
- c) position-identifizier:        8 MARK-Amplituden, 2 SPACE-Amplituden

### **PWM - Ausgänge**

Das in den Abbildungen "IRIG-" und "AFNOR Standardformat" dargestellte pulsweitenmodulierte DC-Signal wird immer parallel zum Sinussignal generiert und steht an der VG-Leiste Pin 13a als TTL-Pegel verfügbar.

### **Technische Daten**

AUSGÄNGE:            Unsymmetrisches AM-Sinussignal:  
                           $3 V_{ss}$  (MARK),  $1 V_{ss}$  (SPACE) an  $50 \Omega$   
  
                          PWM-Signal: TTL, high- und low-aktiv

## USB Stick (optional)

In der Frontblende des Lantime ist eine USB Schnittstelle herausgeführt und kann zum Anschluss eines USB Sticks benutzt werden. Der USB Stick kann für die folgenden Aufgaben benutzt werden:

- Übertragen von Konfigurationen zwischen mehreren Lantimes
- Sperren der Tasten am LCD für unbefugten Zugriff
- Sichern von Logdateien
- Aufspielen eines vollständigen oder inkrementellen Software Updates
- Überspielen von Sicherheits-Zertifikaten (SSL, SSH) und Passwörtern

Nachdem der USB Stick angeschlossen wurde, wechselt die LC Anzeige automatisch in das SETUP Menü mit dem Unterpunkt „USB MEMORYSTICK“ und es wird der Typ des USB Sticks angezeigt.

```
SETUP:          USB MEMORYSTICK
USB: 0  USB DRIVE
```

Befindet sich eine spezielle Menü-Struktur auf dem USB Stick, wird beim Drücken der NEXT Taste der nächste Menüpunkt angewählt. Dieses SETUP Menü ist nur so lange sichtbar, wie der USB Stick angeschlossen ist.

```
SETUP:          USB MEMORYSTICK
copy configuration to memory stick
```

## Menü Verzeichnisstruktur

Die einzelnen Menüpunkte mit den dazugehörigen Befehlen sind auf dem USB Stick abgelegt und werden vom Lantime entsprechend interpretiert und ausgeführt. Somit ist es möglich, dass der Benutzer eigene Menüpunkte hinzufügen kann. Auf dem USB Stick muss die folgende Verzeichnis/Datei Struktur eingerichtet werden, damit ein Menü angezeigt wird:

```
/Lantime/
  Menu/
    menu_1
    script_for_menu_1
    menu_2
    script_for_menu_2
```

## Menü Konfigurationsdateien

Die Namen der Konfigurationsdateien für die einzelnen Menü-Punkte müssen immer mit „menu\_“ beginnen. Diese Dateien können mit einem Texteditor erstellt werden und haben den folgenden Aufbau:

```
# Kommentarzeile

Menu-Name: get configuration from USB Stick
Menu-Type: default
Menu-Script: get_config_from_usb_stick
Menu-Pre-Cmd:
Menu-Post-Cmd:
```

Über den Schlüssel „Menu-Name:“ wird die Zeile angegeben, die im Display als Menü-Punkt erscheinen soll. Für den „Menu-Type:“ sollte immer default eingegeben werden. Mittels des „Menu-Script:“ wird der Name des Scripts angegeben, welches ausgeführt werden soll wenn der Benutzer diesen Punkt auswählt. Vor jedem Ausführen dieser Script Datei wird die folgende Warnmeldung ausgegeben:

```
copy configuration to memory stick
INC -> YES          MENU -> NO
```

Mit den Schlüsselworten „Menu-Pre-Cmd:“ und „Menu-Post-Cmd“ können vor und nach dem Ausführen des Scriptes spezielle Befehle an den Lantime Daemon gesendet werden. Die folgenden Befehle sind zur Zeit möglich:

```
RELOAD_CONFIG      : Konfigurationsdatei neu laden
REBOOT              : Lantime neu starten (reboot)
```

Der USB Stick wird bei Einstecken automatisch unter dem Verzeichnis „/mnt/usb\_storage“ eingebunden und kann zum Transport von Dateien (Log-Dateien, Konfigurationsdateien, Zertifikate) verwendet werden.

## Menü Script Dateien

Eine Script Datei für einen Menü-Punkt besteht aus beliebigen Befehlen, die in einer Telnet/SSH Session ausgeführt werden können. Hier ein Beispiel für das Kopieren einer Lantime-Konfigurationsdatei vom USB-Stick auf die Flash Karte des Lantimes:

```
mount -o remount, rw /mnt/flash
cp /mnt/flash/global_configuration /mnt/flash/global_configuration.old
cp /mnt/usb_storage/my_config /mnt/flash/global_configuration
mount -o remount, ro /mnt/flash
```

Dabei ist zu beachten, dass wenn auf die interne Flash Karte des Lantime geschrieben werden soll, diese erst schreibbar gemacht werden muss (mit dem Befehl „mount -o remount, rw /mnt/flash“).

## Tastatursperre

Der USB-Stick kann auch als Zugangsschlüssel für den Lantime benutzt werden. Damit ist es möglich nur dann die Tastatur am LCD zugänglich zu machen, wenn der USB-Stick eingesteckt wurde. Die Zugangsberechtigung wird über eine Datei auf dem USB-Stick „/mnt/usb\_storage/Lantime/keypad\_lock“ realisiert, indem diese Datei mit der Datei auf der Flash Disk des Lantime „/mnt/flash/keypad\_lock“ verglichen wird. So ist es möglich auch mehrere unterschiedliche USB-Sticks zu verwenden, wobei jeder Lantime seinen eigenen verwendet.

Die Tastatursperre wird über ein Untermenü auf dem USB-Stick aktiviert:

```
SETUP:          USB MEMORYSTICK
prepare front panel keypad locking
```

Dabei wird die Datei „/mnt/usb\_storage/Lantime/keypad\_lock“ auf die Flash-Disk des Lantime kopiert. Beim Deaktivieren dieser Funktion wird diese Datei wieder gelöscht.

```
SETUP:          USB MEMORYSTICK
remove front panel keypad locking
```

## Literaturverzeichnis

- [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