HANDBUCH

LANTIME M400/GPS/PTPv2

IEEE 1588 Grandmaster Clock

31. Juli 2014

Meinberg Funkuhren GmbH & Co. KG

Inhaltsverzeichnis

1 Impressum

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

Telefon: 0 52 81 / 93 09 - 0
Telefax: 0 52 81 / 93 09 - 30

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

Datum: 31.07.2014

2 Sicherheitshinweise für Geräte

Dieses Einbaugerät wurde entsprechend den Anforderungen des Standards IEC60950-1 „Sicherheit von Einrichtungen der Informationstechnik, einschließlich elektrischer Büromaschinen“ entwickelt und geprüft.

Beim Einbau des Gerätes in ein Endgerät (z.B. Gehäuseschrank) sind zusätzliche Anforderungen gem. Standard IEC60950-1 zu beachten und einzuhalten.

WICHTIG: Vor dem Anschluss an die Spannungsversorgung muss ein Erdungskabel (GND) an der Rückseite des M400/GPS angeschlossen werden!

GND

Allgemeine Sicherheitshinweise

- 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.
- Das Gerät wurde für den Einsatz bei einer maximalen Umgebungstemperatur von 40 °C geprüft.
- Die Lüftungsöffnungen dürfen nicht abgedeckt werden.
- Der Brandschutz muss im eingebauten Zustand sichergestellt sein.
- Das Gerät darf nur von Fach-/Servicepersonal geöffnet werden.

Für Spannungsversorgung 100-240VAC

- Das Gerät ist ein Gerät der Schutzklasse 1 und darf nur an eine geerdete Steckdose angeschlossen werden (TN-System).
- Zum sicheren Betrieb muss das Gerät durch eine Installationssicherung von max. 16 A abgesichert werden.
- Die Trennung des Gerätes vom Netz muss immer an der Steckdose und nicht am Gerät erfolgen.

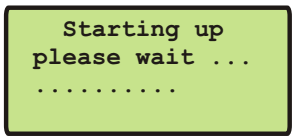
Für Spannungsversorgung 100-240VDC

- Das Gerät muss nach den Bestimmungen der EN60950 außerhalb der Baugruppe spannungslos schaltbar sein (z.B. durch den primärseitigen Leitungsschutz).
- Montage und Demontage des Steckers zur Spannungsversorgung ist nur bei spannungslos geschalteter Baugruppe erlaubt (z.B. durch den primärseitigen Leitungsschutz).
- Die Zuleitungen sind ausreichend abzusichern und zu dimensionieren.

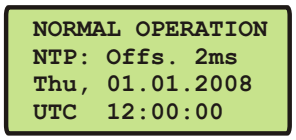
Sicherung:	T3A
Anschlussquerschnitt:	1mm^2 - 2,5mm^2 / 17AWG - 13AWG

3 Kurzanleitung zur Erstinbetriebnahme

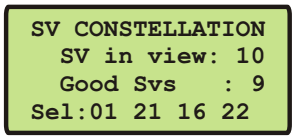
Nach dem Einschalten des Gerätes erscheint die folgende Anzeige auf dem Display, die während des Boot-Vorgangs eine Reihe von Punkten hochzählt.



Danach ist der NTP Zeitserver betriebsbereit und die Anzeige wechselt in das Hauptmenü, in dem einige wichtige Statusinformationen angezeigt werden:



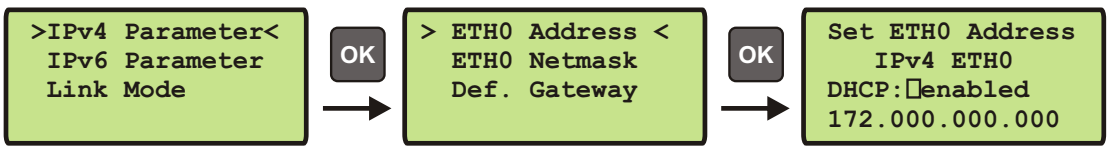
Wenn der Empfänger nicht synchronisiert hat (Refclock LED nach 12 Minuten immer noch rot), prüfen Sie die Anzahl der sichtbaren/guten Satelliten durch Tastenkombination $\downarrow, \rightarrow, \downarrow$ aus dem Hauptmenü.



Es müssen mindestens vier Satelliten gefunden werden, damit die GPS synchronisieren kann. Die Antenne muss freie Sicht zum Horizont haben.

Zur Erstinstallation muss am Gerät eine TCP/IP Adresse, Netzmaske und Default Gateway eingegeben werden. Um eine Übersicht der aktuellen Netzwerkparameter zu bekommen, drücken Sie einmal die F2 Taste. Durch nochmaliges Drücken der F2 Taste aus dieser Übersicht gelangen Sie in das SETUP Menü:

Wählen Sie dann „Interfaces“ und drücken dann 3 mal die OK Taste. Danach geben Sie mit den Pfeiltasten die TCP/IP Adresse, die Netzmaske und evt. ein Default Gateway ein.



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

Default Benutzer: root
Default Passwort: timeserver

4 Netzwerk Zeitserver mit GPS synchronisierter Zeitreferenz

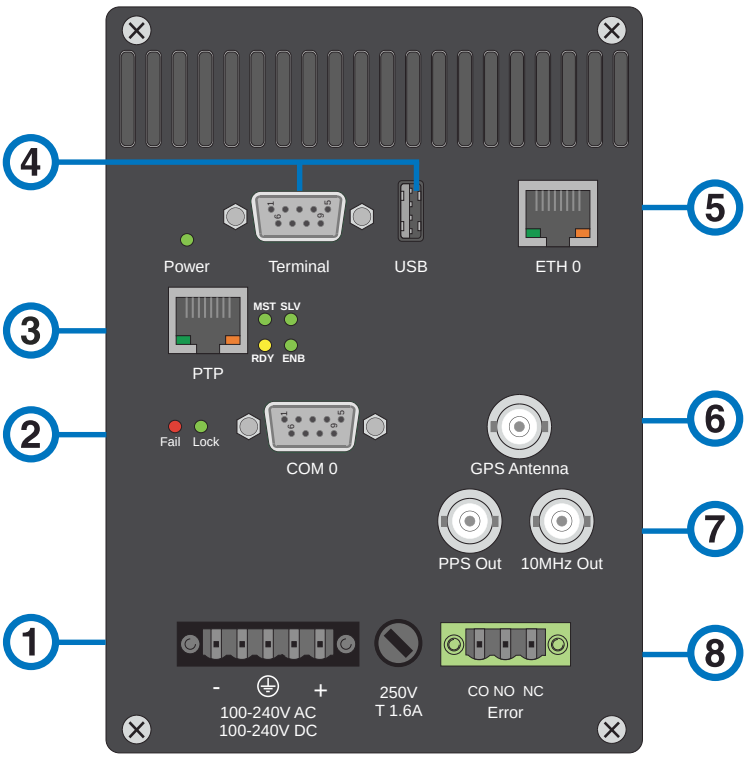
LANTIME steht für Local Area Network Timeserver. Der LANTIME stellt eine absolute und hochgenaue Zeitreferenz in einem TCP/IP Netzwerk zur Verfügung (Stratum-1-Server). Die Zeit wird mittels des NTP Protokolls (Network Time Protocol) allen NTP Clients zur Verfügung gestellt. Es soll ein möglichst einfaches 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 GPS-,GLONASS, IRIG- oder Langwellenempfänger (DCF77, MSF, WWVB), externe NTP-Server oder auch eine Empfänger-Kombination (z.B. GPS/DCF77) als Hybridempfänger eingesetzt werden. Ein LANTIME Zeitserver besteht in der Basisaustattung aus einem integrierten Empfänger, einem Einplatinenrechner mit integrierter Netzwerkkarte und einem Netzteil.

Als Betriebsystem ist ein vereinfachtes LINUX auf dem Einplatinenrechner implementiert, welches in der Boot-Phase aus einer Flash-Disk geladen wird. Alle Einstellungen können über acht Taster und einem Display vorgenommen werden. Ebenso besteht die Möglichkeit einer Fernkonfiguration über das Netzwerk mittels FTP oder TELNET. Ein integrierter Web-Server ermöglicht den Zugriff auf den LANTIME mit einem beliebigen Web-Browser.

5 Komplettsystem LANTIME

Das System LANTIME besteht aus der Satellitenfunkuhr GPS170, einem Einplatinenrechner Computer ELX800 500 MHz mit integrierter Netzwerkkarte und einem Netzteil betriebsbereit in einem Hutschienengehäuse montiert. Die Ein-/Ausgangssignale der Baugruppe LANTIME sind an der Unterseite des Systems über Steckverbinder herausgeführt. Die einzelnen Baugruppen werden nachfolgend beschrieben.



DEUTSCH

1. Spannungsversorgung
2. serielle Schnittstelle COM 0, 9pol. D-SUB
3. Option: Netzwerkanschluss, PTP IEEE1588, 10/100 Mbit Rj45
4. Terminal RS232 D-SUB, 9pol. / Power LED (grün) / USB Port
5. Netzwerk Anschluss ETH0, 10/100Mbit Rj45
6. GPS Antenne, BNC
7. PPS / 10MHz Ausgang, BNC
8. Störmelderelaisausgang

ENGLISH

1. Power supply connector
2. Serial Port COM 0, 9pin. D-SUB
3. Option: Network connector PTP IEEE1588, 10/100 Mbit Rj45
4. Terminal RS232 D-SUB, 9pin. / Power LED (green) / USB Port
5. Network connector ETH0, 10/100 Mbit RJ45
6. GPS Antenna, BNC
7. PPS / 10MHz output, BNC
8. Error, relay output

Auf dem LINUX Rechner ist ein NTPD implementiert, welcher zyklisch die Referenzzeit von der GPS Funkuhr einliest und im Netzwerk verteilt. 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.

5.1 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)

5.2 Zusatzfunktionen

- Externer NTP Zeitserver
- Freie Konfiguration des NTP: Dadurch MD5-Authentifikation und Zugriffskontrolle über Address & Mask Restriction
- Erweiterte Menüführung für Konfiguration und Monitoring über Telnet, SSH oder serielle Terminal-Schnittstelle
- 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

5.3 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

5.4 Ein- und Ausgangsoptionen

- Weitere Ethernet RJ45 Anschlüsse (bis zu acht weitere im 3HE, 4 im 1HE und 8 im HS - XL Gehäuse)
- Frequenz-/Pulsausgänge über BNC Buchsen (z.B. 10 MHz, 2.048 MHz, PPS)
- Höhere Freilaufgenauigkeit durch bessere Oszillatoren (OCXO)
- IRIG B Ausgänge
- ANZ14NET oder VP100/20NET als Nebenuhr über Netzwerk anzuschließen

5.5 Gründe für einen Netzwerk Zeitserver

Wenn die genaue Zeit im eigenen Netzwerk eine wesentliche Rolle für einen reibungslosen Betrieb spielt, sollte ein eigener Zeitserver eingesetzt werden. Prinzipiell kann man natürlich seine Rechner im Netzwerk mit Zeitservern im Internet synchronisieren. Aus den folgenden Sicherheitsaspekten und/oder Wartbarkeit sollte auf einen eigenen Zeitserver 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 Zeitservers angewiesen. Selbst die PTB (Physikalisch technisches Bundesamt) stellt auf der von ihnen angegebenen Webseite klar, dass eine dauernde Verfügbarkeit mindestens eines der PTB-Zeitserver zwar angestrebt wird, aber nicht garantiert werden kann.
- Bei einem Test von anderen frei verfügbaren Zeitservern (nicht PTB!) wurde festgestellt, dass viele eine signifikant falsche Zeit verteilt haben, 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 Zeitserver 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-Zeitserver 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-Newsgroup auf diese Tatsache hingewiesen.

6 Network Time Protocol (NTP)

NTP ist ein 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, Satelliten-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 1 ms, erreicht.

6.1 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 7/Vista/XP/NT/2000/98/95/3x, OS2 oder MAC existieren NTP Clients als Freeware oder Shareware.

Als Bezugsquelle für die neuesten Versionen wird die NTP Homepage empfohlen:
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

6.2 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 „ntpdate lantime“ 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 Logdatei 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	l	36	64	3	0.00	0.000	7885
lantime	.GPS.	0	l	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 Zeittelegramm 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“).

7 GPS Satellitenfunkuhr

Als Referenz-Zeitquelle ist eine GPS Satellitenfunkuhr in dem LANTIME integriert. Die Satellitenfunkuhr wurde mit dem Ziel entwickelt Anwendern eine hochgenaue Zeit- und Frequenzreferenz zur Verfügung zu stellen. Hohe Genauigkeit und die Möglichkeit des weltweiten Einsatzes rund um die Uhr sind die Haupteigenschaften dieses Systems, welches seine Zeitinformationen von den Satelliten des Global Positioning System empfängt.

Das Global Positioning System (GPS) ist ein satellitengestütztes System zur Radioortung, Navigation und Zeitübertragung. Dieses System wurde vom Verteidigungsministerium der USA (US Departement Of Defense) installiert und arbeitet mit zwei Genauigkeitsklassen: den Standard Positioning Services (SPS) und den Precise Positioning Services (PPS). Die Struktur der gesendeten Daten des SPS ist veröffentlicht und der Empfang zur allgemeinen Nutzung freigegeben worden, während die Zeit- und Navigationsdaten des noch genaueren PPS verschlüsselt gesendet werden und daher nur bestimmten (meist militärischen) Anwendern zugänglich sind.

Das Prinzip der Orts- und Zeitbestimmung mit Hilfe eines GPS Empfängers beruht auf einer möglichst genauen Messung der Signallaufzeit von den einzelnen Satelliten zum Empfänger. 24 aktive GPS-Satelliten und drei zusätzliche Reservesatelliten umkreisen die Erde auf sechs Orbitalbahnen in 20.000 km Höhe einmal in ca. 12 Stunden. Dadurch wird sichergestellt, dass zu jeder Zeit an jedem Punkt der Erde mindestens vier Satelliten in Sicht sind. Vier Satelliten müssen zugleich zu empfangen sein, damit der Empfänger seine Position im Raum (x, y, z) und die Abweichung seiner Uhr von der GPS-Systemzeit ermitteln kann. Kontrollstationen auf der Erde vermessen die Bahnen der Satelliten und registrieren die Abweichungen der an Bord mitgeführten Atomuhren von der GPS-Systemzeit. Die ermittelten Daten werden zu den Satelliten hinaufgefunkt und als Navigationsdaten von den Satelliten zur Erde gesendet.

Die hochpräzisen Bahndaten der Satelliten, genannt Ephemeriden, werden benötigt, damit der Empfänger zu jeder Zeit die genaue Position der Satelliten im Raum berechnen kann. Ein Satz Bahndaten mit reduzierter Genauigkeit wird Almanach genannt. Mit Hilfe der Almanachs berechnet der Empfänger bei ungefähr bekannter Position und Zeit, welche der Satelliten vom Standort aus über dem Horizont sichtbar sind. Jeder der Satelliten sendet seine eigenen Ephemeriden sowie die Almanachs aller existierender Satelliten aus.

7.1 Eigenschaften der Satellitenfunkuhr

Die eingesetzte Satellitenfunkuhr ist als Baugruppe im Europaformat (100 mm x 160mm) ausgeführt. Die maximale Kabellänge ist abhängig vom verwendeten Kabel und im Abschnitt "Antennenmontage" angegeben. Die Speisung der Antennen-/ Konvertereinheit erfolgt galvanisch getrennt über das Antennenkabel. Als Option ist ein Antennenverteiler lieferbar, der es ermöglicht, bis zu 4 Empfänger an einer einzigen Antenne zu betreiben.

Die GPS Uhr arbeitet mit dem „Standard Positioning Service". Der Datenstrom von den Satelliten wird durch den Mikroprozessor des Systems decodiert. Durch Auswertung der Daten kann die GPS-Systemzeit mit einer Abweichung kleiner als 250 nsec reproduziert werden. Unterschiedliche Laufzeiten der Signale von den Satelliten zum Empfänger werden durch Bestimmung der Empfängerposition automatisch kompensiert. Durch Nachführung des Hauptoszillators wird eine Frequenzgenauigkeit von $+-5*10^{-9}$ erreicht. Gleichzeitig wird die alterungsbedingte Drift des Quarzes kompensiert. Der aktuelle Korrekturwert für den Oszillator wird in einem nichtflüchtigen Speicher (EEPROM) des Systems abgelegt.

7.2 Zeitzone und Sommer-/Winterzeit

Die GPS-Systemzeit ist eine lineare Zeitskala, die bei Inbetriebnahme des Satellitensystems im Jahre 1980 mit der internationalen Zeitskala UTC (Universal Time Coordinated) gleichgesetzt wurde. Seit dieser Zeit wurden jedoch in der UTC-Zeit mehrfach Schaltsekunden eingefügt, um die UTC-Zeit der Änderung der Erddrehung anzupassen. Aus diesem Grund unterscheidet sich heute die GPS-Systemzeit um eine ganze Anzahl Sekunden von der UTC-Zeit. Die Anzahl der Differenzsekunden ist jedoch im Datenstrom der Satelliten enthalten, so dass der Empfänger intern synchron zur internationalen Zeitskala UTC läuft.

Der Mikroprozessor des Empfängers leitet aus der UTC-Zeit eine beliebige Zeitzone ab und kann auch für mehrere Jahre eine automatische Sommer-/Winterzeitumschaltung generieren, wenn der Anwender die entsprechenden Parameter einstellt.

8 Precision Time Protocol (PTP) / IEEE1588

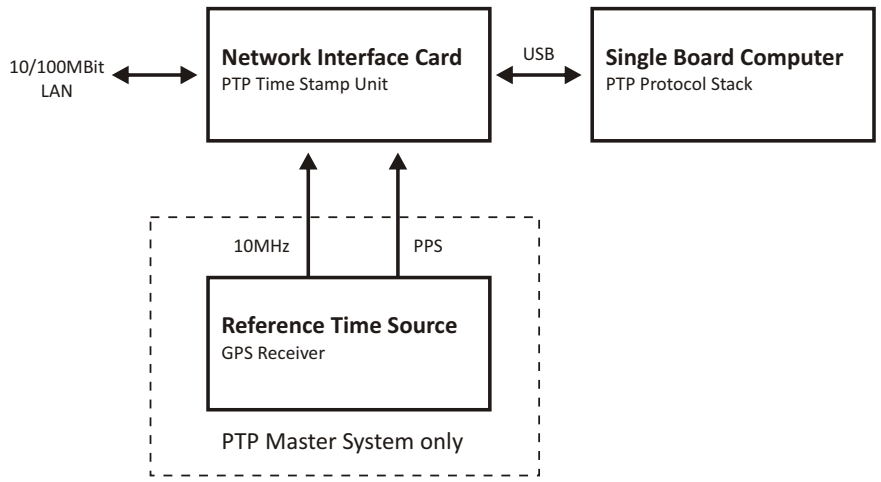
PTP/IEEE1588 ist ein Zeitsynchronisationsprotokoll, das Sub-Mikrosekunden-Genauigkeit über ein Standard-Ethernet-Kabel ermöglicht. Dieser Genauigkeitsgrad wird dadurch erreicht, dass die für PTP/IEEE1588 verwendeten Netzwerk-Ports mit einer sogenannten Hardware-Timestamping-Unit erweitert werden. Diese Komponente ermittelt sehr genau den Zeitpunkt, zu dem ein PTP Netzwerkpaket versendet bzw. empfangen wurde. Das auf Multicast- oder Unicast Paketen basierende Netzwerkprotokoll berücksichtigt diese Zeitstempel bei der Kompensation der Laufzeiten von Synchronisationspaketen und erreicht so die oben angegebene Genauigkeit.

Anders als z.B. NTP gibt es bei PTP lediglich eine Zeitquelle. Die sogenannte Grandmaster Clock ist der einzige Zeitgeber und wird von allen PTP Clients (Slave Clocks) als Zeitquelle verwendet. Sind zwei oder mehr Grandmaster Clocks in einem Netzwerk vorhanden, wird mittels eines im Standard festgelegten Algorhythmus ermittelt, wer als Grandmaster Clock verwendet wird. Dieser „Best Master Clock“ (BMC) Algorhythmus ist bei allen PTP Systemen identisch, daher werden alle PTP/IEEE1588 konformen Systeme die gleiche Grandmaster Clock auswählen. Die verbleibenden nicht ausgewählten Grandmaster Clocks gehen in den sogenannten Passiv-Modus und senden keine Synchronisationspakete, solange die aktive Grandmaster Clock diese „Sync-Messages“ versendet.

Die verwendete Netzwerk-Infrastruktur ist von entscheidender Bedeutung und nimmt großen Einfluss auf die erreichbare Genauigkeit eines PTP/IEEE1588 Netzwerks. Bei asymmetrischen Laufzeiten verschlechtert sich die Genauigkeit, daher sind Standard-Switche nicht so sehr für den Einsatz in PTP-Netzwerken geeignet. Die Store-And-Forward Technologie dieser Geräte läßt die Durchlaufzeiten der Netzwerkpakete lastabhängig teilweise dramatisch schwanken und erschwert dadurch die Laufzeit-Kompensation erheblich. Durch Einsatz des HQ-Filters (siehe entsprechendes Kapitel) können diese Schwankungen eliminiert werden. Einfache Hubs mit zumindest fixen Durchleitzeiten dagegen stellen kein Problem dar. In größeren Netzwerken helfen spezielle Switches mit PTP/IEEE1588 Funktionalität dabei, die möglichen Genauigkeitsklassen zu erreichen. Diese Komponenten fungieren als sogenannte „Boundary Clocks“ (BC) oder „Transparent Clocks“ (TC) und gleichen die internen Laufzeiten durch eigene Timestamping-Units aus, in dem sie im „Boundary Clock“-Modus gegenüber der Grandmaster Clock als Slave (Client) agieren und den angeschlossenen Slaves selbst als Grandmaster erscheinen. Im „Transparent Clock“-Modus wird dem Sync-Paket beim Durchlaufen des Switches die Verweildauer („Residence Time“) innerhalb des Switctes als Korrekturwert mitgegeben. Intern wird die Zeitskala TAI (siehe Zeitskala in Global Parameters) verwendet.

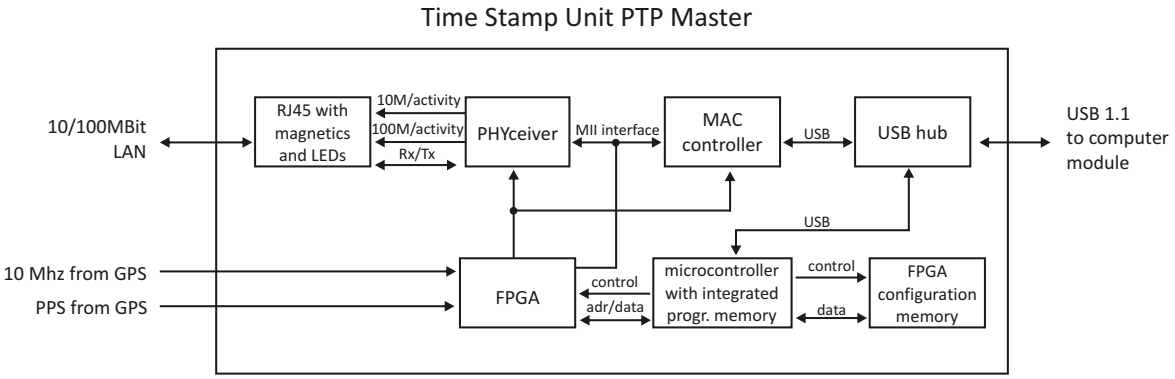
8.1 IEEE1588 PTP Time Stamp Unit

Die integrierte PTP Baugruppe (10/100 MBit) beinhaltet eine integrierte Time Stamp Unit zur Gewinnung von Zeitstempeln in IEEE1588 (PTP) kompatiblen Netzwerken. In Verbindung mit einem Single Board Computer und einer Referenzzeitquelle (nur PTP Master) bildet sie je nach Bestückungsvariante ein PTP Master- oder Slave System:



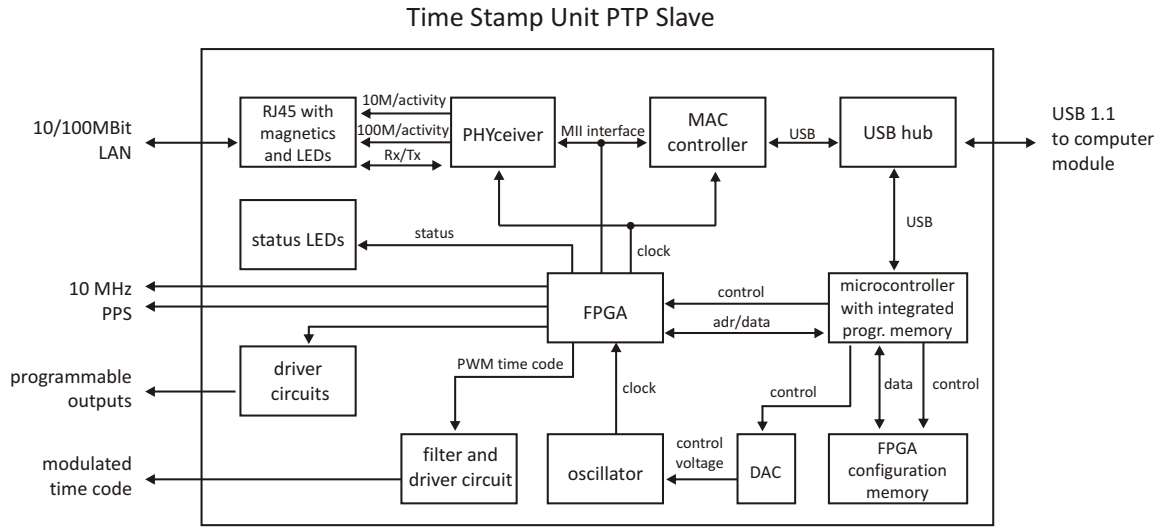
Die in einem FPGA (Field Programmable Gate Array, programmierbarer Logikschaltkreis) integrierte Time Stamp Unit überprüft den Datenverkehr auf dem MII-Interface zwischen dem PHYceiver (Baustein, welcher die physikalische Anbindung an das Netzwerk vornimmt) und dem Ethernet Controller (MAC) der Baugruppe. Wird ein gültiges PTP Paket erkannt, nimmt die Time Stamp Unit einen Zeitstempel, welcher von einem Linux-basiertem Single Board Computer ausgelesen wird und vom darauf laufenden PTP Protokollstack verarbeitet wird. Der allgemeine Datenverkehr für Status und Konfigurationsnachrichten zwischen PTP Modul und Hauptrechner erfolgt über eine USB-Verbindung.

8.2 Funktionsweise in Master-Systemen



Nach dem Systemstart übernimmt das Modul einmalig die absolute Zeit (PTP Sekunden) einer Referenzzeitquelle (z.B. GPS-Funkuhr) und der PTP Nanosekunden Anteil wird auf Null gesetzt. Ist der Oszillator der GPS-Funkuhr eingeschwungen, wird das Rücksetzen der Nanosekunden wiederholt, wodurch eine maximale Abweichung von 20 nsec zwischen dem Sekundenimpuls (PPS) der GPS-Funkuhr und dem PTP Master erreicht wird. Der Referenztakt der PTP Baugruppe (50 MHz) wird über eine PLL des FPGA aus dem Takt des GPS-disziplinierten Oszillators der Funkuhr gewonnen, wodurch eine starre Anbindung der Time Stamp Unit an das GPS-System erreicht wird.

8.3 Funktionsweise in Slave-Systemen



Nach dem Einschalten wartet das System solange, bis eine gültige Zeit von einem PTP Master empfangen wurde und setzt dann seine eigenen PTP Sekunden und Nanosekunden. Der vom PTP Treiber des Computersystems ermittelte PTP Offset wird genutzt, um den Masteroszillator der TSU-USB einzuregeln. Hierdurch wird eine hohe Genauigkeit der vom PTP Slave generierten Ausgangssignale (10 MHz/PPS/IRIG) erreicht, da diese direkt vom Oszillator der TSU-USB abgeleitet werden.

8.4 PTPv2 IEEE 1588-2008 Konfigurationsanleitung

Eine der wichtigsten Aufgaben innerhalb eines Netzwerk Zeitsynchronisationsprojekts ist die Konfiguration der Geräte innerhalb einer PTP Infrastruktur. Die Einstellungen der beteiligten PTP Grandmaster Uhren als Zeitquellen und den Endgeräten („Slaves“) müssen zueinander passen, um spätere Probleme bei der Synchronisation im produktiven Einsatz zu vermeiden. Zusätzlich dazu müssen bei der Verwendung von weiteren PTP kompatiblen Netzwerkkomponenten, wie Switche, die PTP Einstellungen ebenfalls kompatibel sein.

Es ist daher sehr wichtig im Vorfeld Entscheidungen zu treffen, wie die Kommunikation zwischen den Geräten stattfinden soll. Die wesentlichen Punkte sind hierbei Entscheidung zugunsten eines bestimmten Netzwerkkommunikationstyps wie Unicast oder Multicast oder die Entscheidung, wie oft ein Master Synchronisationsnachrichten zu den Slaves senden soll.

Dieses Kapitel vermittelt einen einleitenden Überblick über die verschiendenen Konfigurationsparameter und deren Effekte auf die Synchronisation im allgemeinen. Eine detaillierte Beschreibung der einzelnen Konfigurationsparameter, die im LANTIME Menü vorgenommen werden können, befindet sich im nächsten Kapitel innerhalb dieser Dokumentation.

8.4.1 Allgemeine Optionen

Bevor mit dem Aufbau der Infrastruktur des PTP Netzes begonnen wird, sollten die folgenden Optionen bedacht werden:

1) Layer 2 (Ethernet) oder Layer 3 (UDP/IPv4) Verbindungen
2) Multicast oder Unicast
3) Two-Step oder One-Step Betrieb
4) End-to-End (E2E) oder Peer-to-Peer (P2P) Delay Mechanismus

Diese Optionen müssen für alle beteiligten PTP Geräte definiert werden. Sollten teilnehmende Geräte abweichende Einstellungen haben oder diese nicht unterstützen, dann sind sie nicht in der Lage, eine funktionierende Synchronisation aufzubauen.

8.4.2 Netzwerk - Layer 2 oder Layer 3

PTP/IEEE 1588-2008 bietet die Möglichkeit, die PTP Nachrichten auf verscheidene Netzwerkkommunikationsebenen abzubilden. Bei allen Meinberg PTP Produkten kann man zwischen PTP über IEEE 802.3 Ethernet (Netzwerk Layer 2) oder UDP/IPv4 (Netzwerk Layer 3) wählen.

Layer 3 ist der empfohlene Modus, da er in den meisten Umbgebungen funktioniert. Im Layer 2 Betrieb muss das Netzwerk in der Lage sein, reine Ethernet Verbindungen zwischen Master und Slave Geräten herzustellen. Dies ist oft nicht der Fall, wenn das Netzwerk in verschiedene Netzwerksegmente aufgeteilt und innerhalb der Netzwerkinfrastruktur kein Layer 2 Routing vorgesehen ist.

Der einzige Vorteil bei der Verwendung im Layer 2 -Betrieb besteht in einer leichten Reduktion des Netzwerkverkehrs, da die übertragenen Netzwerkpakete nicht den UDP und IP Header beinhalten und somit 28 Bytes pro PTP Paket eingespart werden. Da PTP jedoch ein Protokoll mit wenig Datenverkehr ist, spielt dieses Argument nur eine Rolle, wenn entweder Netzwerkverbindung mit sehr geringer Bandbreite oder nach Bandbreite bezahlte Netzwerkverbindungen, z.B. über gemietete Leitungen verwendet werden müssen.

8.4.3 Multicast oder Unicast

Die erste Version von PTP (IEEE 1588-2002, auch bekannt als PTPv1) unterstützte nur die Übermittlung über Multicast-Nachrichten. Multicast hat den großen Vorteil, dass der Master nur ein Sync Paket an eine Multicast Adresse schicken muss, welches dann von allen Geräten empfangen wird, die auf dieser Multicast Adresse lauschen.

In der Version 2 des PTP Standards (IEEE 1588-2008) wurde zusätzlich der Betrieb über Unicast eingeführt. Die Unicast Kommunikation basiert auf einer Punkt-zu-Punkt Verbindung, bei welcher der Master ein Sync Paket zu jedem Slave Gerät schicken muss, was wesentlich mehr CPU Performance auf dem Master und eine erhöhte Netzwerklast zur Folge hat.

Unicast Kommunikation wird in bestimmten Netzwerkumgebungen verwendet, in denen Multicast Pakete durch Switche und Router geblockt werden (müssen).

8.4.4 Two-Step oder One-Step

PTP erfordert, das der Master periodisch SYNC Pakete zu den Slave Geräten schickt. Der Hardware-Zeitstempel-Ansatz von PTP erfordert ebenso, das der Master den Moment exakt bestimmt, bei welchem das SYNC Paket auf das Netzwerkkabel geht und diesen Zeitpunkt an die Slaves weiter gibt. Dies kann entweder durch das Aussenden einer separaten Nachricht geschehen (das so genannte „FOLLOWUP Paket“, auch Two-Step Verfahren genannt) oder durch direkte Manipulation des SYNC Pakets (im One-Step Verfahren) kurz bevor das Paket den Netzwerkport verlässt. Bei dieser Manipulation wird der Zeitstempel von der Hardware Zeitstempeleinheit direkt in das SYNC Paket geschrieben, kurz bevor es auf das Netzwerkkabel geht.

8.4.5 End-To-End (E2E) oder Peer-To-Peer (P2P) Delay Messungen

Zusätzlich zum Empfang der SYNC/FOLLOWUP Pakete, muss ein Slave auch in der Lage sein, die Paketlaufzeit vom Master zum Slave zu bestimmen, um den Offset zur Masteruhr korrekt berechnen zu können. Dieses „Delay Measurement“ wird vom Slave in einem bestimmten Interval durchgeführt. Eine Laufzeitmessung wird durchgeführt, indem der Slave ein sogenanntes DELAY_REQUEST Paket zum Master sendet und sich die Zeit der Aussendung dieses Pakets merkt. Der Master nimmt dann einen Zeitstempel beim Empfang dieses Pakets und sendet diesen Zeitstempel in einem DELAY_RESPONSE Paket an den Slave zurück.

IEEE 1588-2008 bietet zwei verschiedene Mechanismen zur Durchführung der Laufzeitmessung an.
Ein Slave kann entweder die Gesamtlaufzeit zum Master bestimmten, dies wird dann **End-to-End** Mechanismus (oder kurz E2E) genannt. Alternativ kann ein PTP Gerät nur die Laufzeit zu seinem direkten Nachbarknoten im Netzwerk messen, wobei der Nachbarknoten sowohl ein PTP Endgerät wie auch ein Switch darstellen kann. Dieses Verfahren wird **Peer-to-Peer** Mechanismus (oder kurz P2P) genannt. Beim P2P Verfahren werden die einzelnen Laufzeiten zwischen den Netzwerkknoten akkumuliert und dem durchlaufenden Sync Paket vom Master als Korrekturwert mitgegeben, so dass am Ende der Slave die Gesamtlaufzeit ermitteln kann.

Der Vorteil des P2P Verfahrens ist die deutliche Reduktion von möglichen Synchronisationsungenauigkeiten aufgrund von plötzlichen Topologieänderungen innerhalb des Netzwerks.

Beispiel: In einer Ringtopologie wird die Paketlaufzeit verändert, wenn der Ring an einer Stelle aufbricht, da der Netzwerkverkehr unter Umständen in eine andere Richtung umgeleitet wird. Ein PTP Slave, der die Paketlaufzeit mit Hilfe des E2E Verfahrens ermittelt, würde in diesem Fall von einer falschen Paketlaufzeit ausgehen bis er die nächste Laufzeitmessung durchführt. Dieses Problem würde in einer P2P Infrastruktur nicht passieren, da zum Zeitpunkt der Topologieänderung bereits alle Laufzeiten zwischen den Links bekannt sind und ein Sync Paket vom Master bereits beim ersten Durchlauf über den neuen Netzwerkpfad mit den entsprechenden Korrekturwerten versehen wird.

Der Nachteil des P2P Verfahrens besteht darin, das alle beteiligten Netzwerkknoten, inklusive aller Switche zwischen Master und Slave, das P2P Verfahren beherrschen müssen. Ein Switch/Hub ohne P2P Unterstützung würde entweder alle empfangenen PDELAY_REQUEST Pakete an alle Ports weiterleiten und die Genauigkeit dadurch erheblich verschlechtern bzw. unbrauchbar machen oder im schlechtesten Fall alle PDELAY Pakete blocken und überhaupt keine Laufzeitmessung ermöglichen.

Daher bleibt das E2E Verfahren die einzige Wahl für die Verwendung von PTP über nicht PTPv2-kompatible Switche.

8.4.6 Einstellungsempfehlungen

Meinberg empfiehlt als Standardeinstellung die Einstellungen Layer 3, Multicast, Two-Step und End-to-End Verfahren, falls dies in der geplanten Netzwerkumgebung möglich ist. Diese Einstellungen ermöglichen die bestmögliche Kompatibilität und reduzieren die Wahrscheinlichkeit das Probleme bei der Interoperabilität zwischen Geräten verschiedener Hersteller auftreten können.

8.4.7 Nachrichtenintervalle

Die Entscheidung zwischen den verschiedenen oben beschriebenen Modi ist hauptsächlich durch die verwendetete Netzwerkumgebung vorgegeben in welcher die PTP Geräte installiert werden. Zusätzlich zu den einzustellenden Modi müssen eine Reihe von Intervallen für bestimmte PTP Nachrichtentypen definiert werden, falls nicht die Standardeinstellungen verwendet werden sollen, die in den meisten Fällen jedoch nicht verändert werden müssen.

Es gibt jedoch Anwendungen, bei denen die Intervalle angepasst werden müssen. Dies ist beispielsweise der Fall, wenn durch hohe Netzwerklast Schwankungen bei den Paketlaufzeiten auftreten können (PDV - „Packet Delay Variation"). Probleme bei der Client Synchronisation können dann durch die Erhöhung der Frequenz der ausgesendeten SYNC Pakete vermieden werden, da in diesem Fall Messfehler schneller korrigiert werden.

Die Intervalle für die folgenden PTP Nachrichten können editiert werden:
1) ANNOUNCE Messages
2) SYNC/FOLLOWUP Messages
3) (P)DELAY_REQUEST Messages

8.4.8 ANNOUNCE Messages

Diese PTP Nachricht transportiert den Zustand und die Qualitätsinfomationen über den aktuell aktiven Master im PTP Netzwerk. Der Vorgang der zur Entscheidung führt, welcher Grandmaster im Netzwerk aktiv werden soll, wird „Best Master Clock Algorithm" (BMCA) genannt. Die notwendigen Parameter zur Ausführung des BMCA werden alle in der ANNOUNCE Message übertragen, die von einem Master periodisch ausgesendet wird.

Das Intervall mit welchem diese Nachricht gesendet wird, beeinflusst direkt die Umschaltzeit, die benötigt wird, um einen Wechsel des Masters durchzuführen, falls der aktuell aktive Master ausfällt oder ein „besserer" im Netz aktiv wird.

In der Zeit in der noch kein Master bestimmt wurde, ist es möglich, das mehrere potentielle (Grand-)Master Announce Messages aussenden. Dies geschieht u.a., wenn die Geräte innerhalb des PTP Netzwerks gleichzeitig gestartet werden. Ein PTP Gerät, welches grundsätzlich Master werden kann, empfängt gleichzeitig zur Aussendung der „eigenen" Announce Message die Announce Messages der anderen PTP Master Geräte. Sobald festgestellt wird, das ein anderer Master im Netzwerk existiert, welcher bessere Werte aufweist als die eigenen, wird der Master die weitere Aussendung von ANNOUNCE Messages einstellen. Auf diese Weise bleibt nach kurzer Zeit nur noch der „beste" Master übrig.

Ein Grandmaster, der nicht die Aufgabe des aktiven Masters übernimmt, wechselt in den „PASSIVE" Modus und wartet darauf, im Fall eines Fehlers des aktiven Masters die Master-Rolle wieder zu übernehmen.

Um einen Master auszuwählen, ist es erforderlich, dass mindestens zwei aufeinander folgende ANNOUNCE Messages empfangen werden. Der Empfang einer ersten ANNOUNCE Message muss innerhalb einer Wartezeit von mindestens 3 ANNOUNCE Message Intervallen erfolgen. Legt man beispielsweise ein ANNOUNCE Intervall von 2 Sekunden zugrunde (dies ist der Standardwert), so würde beim Ausfall eines Masters nach 6 Sekunden festgestellt werden, dass der Master einen Fehler hat und nach weiteren 4 Sekunden der neue Master feststeht.

Ein ANNOUNCE Intervall von 2 Sekunden hat demzufolge eine Umschaltzeit von mindestens 10 Sekunden zur Folge. Ein kürzeres ANNOUNCE Intervall ermöglicht daher im Fehlerfall prinzipiell eine schnellere Umschaltzeit. Ein zu kurzes Intervall kann jedoch in bestimmten Umgebungen kurzfristig zu Fehlentscheidungen führen. Es wird daher empfohlen die Standardeinstellung beizubehalten.

8.4.9 SYNC/FOLLOWUP Messages

Der aktive MASTER sendet SYNC Nachrichten (und im Two-Step Verfahren zugehörige FOLLOWUP Nachrichten) in einem konfigurierten Intervall aus. Dieses Intervall (Standard ist 1 SYNC/FOLLOWUP Paket einmal pro Sekunde) bestimmt, wie oft die SLAVES Synchronisationsinformationen erhalten um die eigene Uhr gegenüber der Masteruhr abzugleichen und nachzuführen.

Zwischen dem Empfang zweier Sync Nachrichten läuft die Slave Uhr frei auf der eigenen Zeitbasis, zum Beispiel dem Quarzoszillator. Ein wichtiger Faktor bei der Entscheidung welches SYNC Intervall zu wählen ist, ist die Stabilität des Oszillators. Ein sehr guter Oszillator benötigt eine geringere SYNC Rate, um die Stabilität zu halten als ein weniger guter Oszillator. Auf der anderen Seite wird die erforderliche Netzwerkbandbreite direkt beeinflusst, wenn das SYNC Intervall geändert wird.

Für Meinberg Slave Geräte ist die Standardeinstellung (einmal pro Sekunde) ausreichend um die bestmögliche Synchronisiationsgenauigkeit zu erreichen.

8.4.10 (P)DELAY_REQUEST Messages

Wie bereits bei der Erläuterung der Mechanismen für die Laufzeitmessungen („End-To-End“ oder „Peer-to-Peer“) erwähnt wurde, sind die Delay Messungen ein wichtiger Faktor bei der Realisierung der erforderlichen Genauigkeit.

Im End-to-End Modus werden vom Slave standardmäßig alle 8 Sekunden Delay Messungen durchgeführt, in dem ein DELAY_REQUEST Paket an den Master gesendet wird, welcher dann in einem DELAY_RESPONSE Paket den Zeitstempel zum Zeitpunkt des Eintreffens des DELAY_REQUEST Pakets an den Slave zurückschickt. In Umgebungen, wo das Netzwerkdelay stark variiert, kann die Messrate erhöht werden, um schneller auf Fehlmessungen zu reagieren, die durch Verzögerungen innerhalb des Netzwerks entstanden sein können.

Meinberg Slave Geräte sind in der Lage den Effekt einer veralteten Delay Messung durch den Einsatz eines Filters und einer optimierten Oszillator-Regelung zu begrenzen. Dies verhindert, das eine Slave Uhr große Sprünge durchführt selbst wenn durch hohe Netzwerklast „Ausreißer“ bei den Messungen vorkommen. Die Masteruhr wird über einen gewissen Zeitraum beobachtet, bevor eine Regelung des eigenen Oszillators durchgeführt wird. Mit einem „low cost“ Oszillator wäre dies nicht möglich, da vor allem die temperaturabhängige Drift und Alterungseffekte des Oszillators eine größere Abweichung zur Folge haben.

Slave Geräte dürfen einen Master nicht öfter anfragen als der Master in seinen DELAY_RESPONSE Messages vorgibt. Meinberg Grandmaster geben standardmäßig eine Delay Request Rate von 8 Sekunden vor. Im „Peer-to-Peer“ Modus ist eine Änderung des Intervalls nicht so kritisch, da nur die Laufzeit zum nächsten „Hop“ gemessen wird (Port-zu-Port) und eine Änderung der Laufzeit auf dieser kurzen Strecke sehr unwahrscheinlich ist.

8.4.11 HQ Filter

Falls im angeschlossenen PTP Netzwerk keine PTP Switches verwendet werden, sind die zu erwartenden Genauigkeiten abhängig von der Charakteristik der Switches. Netzwerk Switches ohne PTP Unterstützung haben die Eigenschaft die PTP Pakete nicht deterministisch zu verzögern und damit die Zeitgenauigkeit der PTP Messung zu verschlechtern (zeitlicher Jitter durch Variation der Paketlaufzeiten). Unter Jitter wird im folgenden die Varianz der gemessenen Offsets um einen bestimmten Mittelwert verstanden, der im betrachten Zeitrahmen ermittelt wird.

Dieser zeitliche Jitter kann zwischen 100ns und 10000ns (bisher getestete Switches) liegen. Bei Routern liegt dieser Jitter noch wesentlich höher. Um diesen zeitlichen Netzwerk Jitter zu reduzieren kann der HQ-Filter aktiviert werden. Mit Layer2 Switchen können dann Genauigkeiten im Submicrosekundenbereich erreicht werden. Ebenso werden Schwankungen durch Netzwerklast und Fehlmessungen eliminiert.

Funktionsweise
Wenn der HQ-Filter eingeschaltet ist, werden in der Startphase zuerst nur PTP Messungen durchgeführt ohne die eigene Zeit zu regeln. Dieses wird im Status mit dem Zusatz „init“ angezeigt. In dieser Phase werden einige statistische Parameter der Eingangswerte berechnet: Zum einen der maximale Jitter von PTP Offset und PathDelay und zum anderen die aktuelle Drift des internen Oszillators. Der Filter Parameter **estimated accuracy** gibt den betragsmäßig maximal zu erwartenden Jitter an, d.h., alle gemessenen Werte, die außerhalb dieses Bereichs liegen, werden verworfen. Ist der gemessene maximale Jitter kleiner als dieser Parameter, wird der gemessene Wert als maximale Grenze verwendet. Der maximale Jitter wird kontinuierlich immer neu berechnet. Als Default wird **estimated Accuracy** auf 1s eingestellt, damit die Grenzen automatisch gefunden werden.

PDSC
PDSC ist die Abkürzung für „Path Delay Step Compensation“. PDSC versucht Sprünge im PTP Path Delay zu eliminieren, die durch eine Änderung des Asymmetrie Delays entstehen. Ein solcher Sprung im PTP Path Delay kann durch einen Wechsel der Netzwerk Route (Topology Change) entstehen, wie es beispielsweise in SDH Netzwerken der Fall ist. Es werden nur Sprünge erkannt, die größer als der gemessene Jitter sind. Diese Funktion ist nur in Verbindung mit dem HQ-Filter zu verwenden.

8.4.12 Option: PTP Client Management

Ab Lantime Firmware Version 5.34l
Mit diesem Menü können die PTP Clients im Netzwerk überwacht werden. Im Menü ***PTP Setup*** -> ***PTP Parameters*** -> ***PTP Client Management*** geben Sie das Request Intervall in Sekunden an, d.h. in welchem Intervall die PTP Clients überprüft werden sollen. Bei 0 wird das PTP Client Management abgeschaltet. Ein Wert von 60s sollte ein guter Wert sein.

```
PTP Client Management
Request Interval [s]: 10
Set Request Interval to 0 to
disable PTP Client Management
```

Dann kann über das Front-Panel eine Übersicht über alle zur Zeit vorhandenen PTP Nodes in dem Netzwerk angezeigt werden:

```
PTP Client Management:found 5  PTP Nodes
EC4670FFFE003335 MASTER
0050C2FFFED287DE SLAVE  -89.0ns +20.82us
EC4670FFFE000801 PASSIVE
0050C2FFFEB717EA SLAVE  -99.0ns +20.68us
EC4670FFFE002435 PASSIVE
```

Es können maximal 7 PTP Nodes angezeigt werden. Die vollständige Liste von maximal 100 PTP Nodes kann über das WEB Interface ausgegeben werden.

9 GPS Antennenmontage

Die GPS-Satelliten sind nicht geostationär positioniert, sondern bewegen sich in circa 12 Stunden einmal um die Erde. Satelliten können nur dann empfangen werden, wenn sich kein Hindernis in der Sichtlinie von der Antenne zu dem jeweiligen Satelliten befindet. Aus diesem Grund muss die Antennen-/Konvertereinheit an einem Ort angebracht werden, von dem aus möglichst viel Himmel sichtbar ist. Für einen optimalen Betrieb sollte die Antenne eine freie Sicht von 8° über dem Horizont haben. Ist dies nicht möglich, sollte die Antenne so montiert werden, dass sie eine freie Sicht Richtung Äquator hat. Die Satellitenbahnen verlaufen zwischen dem 55. südlichen und 55. nördlichen Breitenkreis. Ist auch diese Sicht ziemlich eingeschränkt, dürften vor allem Probleme entstehen, wenn vier Satelliten für eine neue Positionsberechnung gefunden werden müssen.

Die Montage kann entweder an einem stehenden Mastrohr mit bis zu 60 mm Außendurchmesser oder direkt an einer Wand erfolgen. Ein passendes, 50 cm langes Kunststoffrohr mit 50 mm Außendurchmesser und zwei Wand- bzw. Masthalterungen gehören zum Lieferumfang. Als Antennenzuleitung kann ein handelsübliches 50 Ohm Koaxialkabel verwendet werden. Die maximale Leitungslänge zwischen Antenne und Empfänger ist vom Dämpfungsfaktor des verwendeten Koaxialkabels abhängig.

Bei Einsatz des optional lieferbaren Antennenverteilers können mehrere Empfänger an einer Antenne angeschlossen werden. Die Gesamtlänge eines Stranges von der Antenne bis zum Empfänger darf die maximale Kabellänge nicht überschreiten. Der Antennenverteiler darf sich an einer beliebigen Position dazwischen befinden.

Bei der Antennenmontage mit einem Überspannungsschutz ist zu beachten, dass dieser direkt nach Gebäudeeintritt des Antennenkabels montiert wird. Der verwendete Überspannungsschutz ist nicht zur Außenmontage geeignet.

9.1 Beispiel:

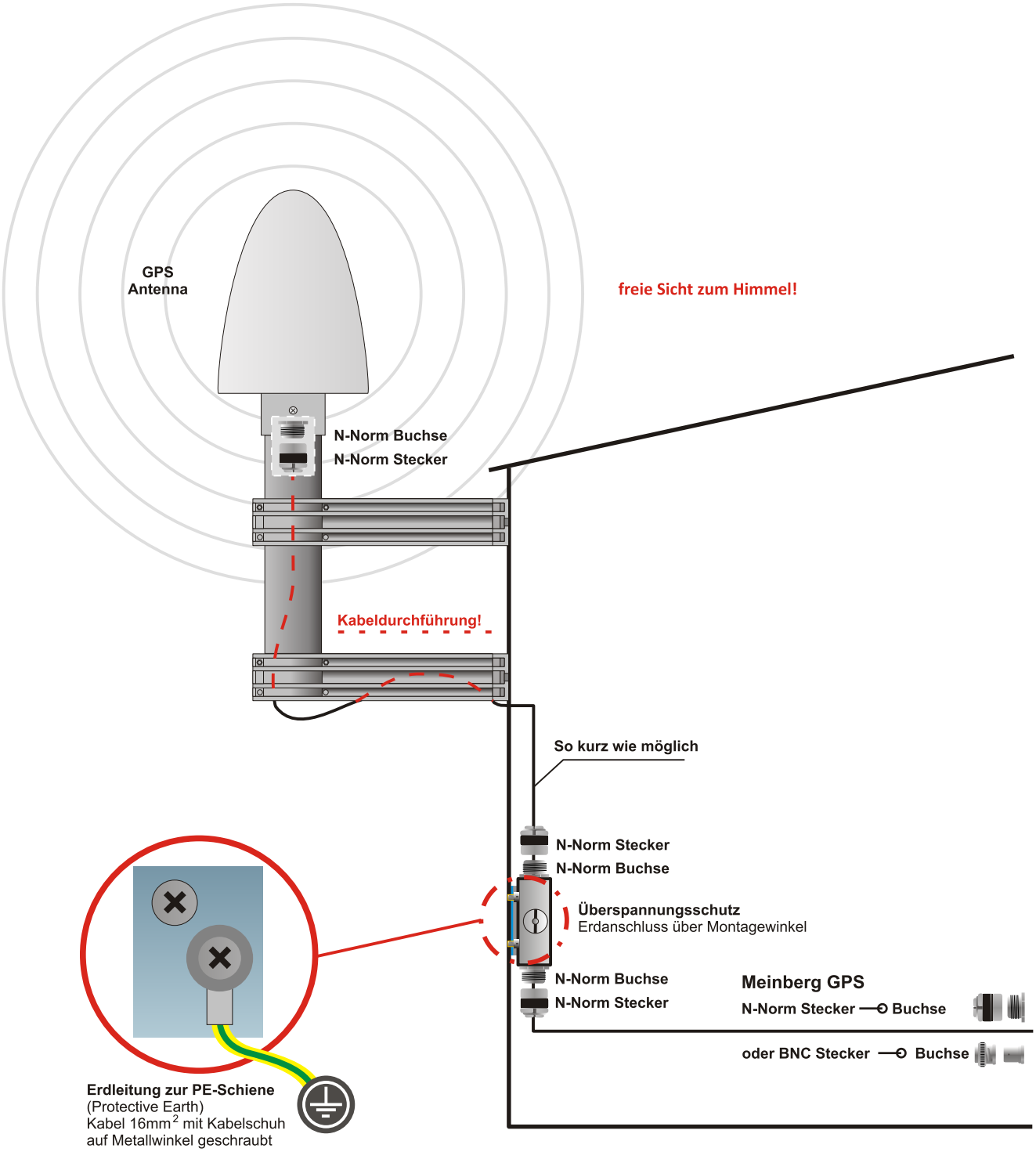
Kabeltyp	Kabel-Ø [mm]	Dämpfung bei 100MHz [dB]/100m	Max. Kabellänge [m]
RG58/CU	5mm	17	300 (1)
RG213	10,5mm	7	700 (1)

(1) Die Angaben sind für Geräte mit Antennen ab Baujahr Januar 2005.

Bei den angegebenen Daten handelt es sich um typische Werte. Die genauen Werte sind im Datenblatt des eingesetzten Kabels nachzuschlagen.

9.2 Antennenmontage mit Überspannungsschutz

Ein Überspannungsschutz für koaxiale Leitungen ist optional verfügbar. Der Erdanschluss ist auf möglichst kurzem Wege über den mitgelieferten Montagewinkel zu realisieren. Der Überspannungsschutz ist mit zwei N-Norm Buchsen ausgestattet. Im Normalfall wird die Antenne über das Antennenkabel direkt an das System angeschlossen.



9.3 Kurzschluss auf der Antennenleitung

(Optional für Baugruppen mit Display)
Sollte auf der Antennenleitung ein Kurzschluss auftreten, wird dieser durch eine Warnmeldung im Display angezeigt:

In diesem Fall muss die Uhr ausgeschaltet, der Fehler behoben und danach die Uhr wieder eingeschaltet werden. Die Versorgungsspannung für die Antennen/Konvertereinheit beträgt im Leerlauf ca.18.5V_{DC} und bei angeschlossener GPS Antenne ca.16V_{DC} .

10 Bootphase des GPS170 Empfängers

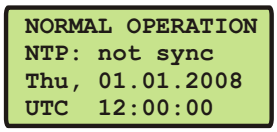
Nachdem die Antenne und die Stromversorgung angeschlossen wurden, ist das Gerät betriebsbereit. Etwa 2 Minuten nach dem Einschalten hat der Oszillator seine Betriebstemperatur und damit seine Grundgenauigkeit erreicht, die zum Empfang der Satellitensignale erforderlich ist. Wenn im batteriegepufferten Speicher des Empfängers gültige Almanach- und Ephemeriden vorliegen und sich die Empfängerposition seit dem letzten Betrieb nicht geändert hat, kann der Mikroprozessor des Geräts berechnen, welche Satelliten gerade zu empfangen sind. Unter diesen Bedingungen muss nur ein einziger Satellit empfangen werden, um den Empfänger synchronisieren zu lassen.

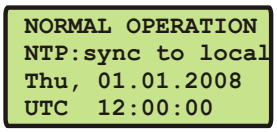
Wenn sich der Standort des Empfängers seit dem letzten Betrieb um einige hundert Kilometer geändert hat, stimmen Elevation und Doppler der Satelliten nicht mit den berechneten Werten überein. Das Gerät geht dann in die Betriebsart **Warm Boot** und sucht systematisch nach Satelliten, die zu empfangen sind. Aus den gültigen Almanachs kann der Empfänger die Identifikationsnummern existierender Satelliten erkennen. Wenn vier Satelliten empfangen werden können, kann die neue Empfängerposition bestimmt werden und das Gerät geht über zur Betriebsart **Normal Operation**. Sind keine Almanachs verfügbar, z.B. weil die Batteriepufferung unterbrochen war, startet die GPS170 in der Betriebsart **Cold Boot**. Der Empfänger sucht einen Satelliten und liest von diesem das komplette Almanach ein. Nach etwa 12 Minuten ist der Vorgang beendet und die Betriebsart wechselt zu Warm Boot.

11 Bootphase des Linux Rechners

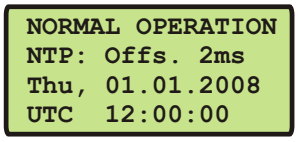
Das Linux Betriebssystem wird aus einer gepackten Datei von der Flash-Disk des Einplatinenrechners in eine RAM-Disk geladen. Das gesamte Dateisystem befindet sich nach dem Booten in der RAM-Disk. Dadurch wird gewährleistet, dass bei jedem Neustart ein initialer Zustand des Dateisystems zur Verfügung steht; nur einige Parameter-Dateien werden zusätzlich auf der Flashdisk gespeichert. Dieser Bootvorgang dauert ca. 1 Minute. Nachdem das LINUX System hochgefahren ist, wird automatisch die Netzwerkfunktion initialisiert, das Programm zur Kommunikation mit der Funkuhr und 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 und die verwendete integrierte Funkuhr des Systems sind. Solange der NTPD nicht synchron mit der Funkuhr ist wird eine der folgenden Meldungen auf dem LC-Display angezeigt:





Damit der NTPD sich auf die Referenzuhr synchronisieren kann, muss ein ausreichender Empfang gegeben sein, d.h. die Status-LED der Referenzuhr (Ref. Time) muss grün leuchten. Ist dies der Fall, wird im LC-Display folgende Meldung angezeigt:



Die zweite Zeile des LC-Displays bedeutet, dass der NTPD sich auf die Referenzuhr synchronisiert hat - mit einem Offset von 2ms (Abbildung oben). D.h., die Abweichung von der internen NTP Referenzzeit zum Empfänger beträgt aktuell 2ms. Da es sich bei der internen Referenzzeit des NTP um PLL (Phase Locked Loop) handelt, braucht es eine gewisse Zeit, bis der Offset zur Funkuhr 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.

12 Benutzerschnittstellen zur Konfiguration

12.1 Einleitung Konfiguration LANTIME

Das LANTIME bietet mehrere Möglichkeiten zur Konfiguration der Parameter:

Command Line Interface (CLI) über TELNET
Command Line Interface über SSH
Command Line Interface: serielles Terminal im Frontpanel (38400/8N1/VT100)
HTTP Interface
Secure HTTP Interface (HTTPS)
Frontpanel LCD/VFD Interface
SNMP Management

Zur ersten Inbetriebnahme des LANTIME muss das Frontpanel LCD/VFD Interface benutzt werden, um einmalig eine IP Adresse dem Gerät zu vergeben (siehe auch DHCP IPv4 oder AUTOCONF IPv6). Bei einem LANTIME mit seriellem Terminal Interface („Term“ oder „Terminal“) kann die Inbetriebnahme mit Hilfe eines Terminal Programms (Einstellungen: 38400Baud, 8N1, VT100), 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

12.2 Hauptmenü

Das Hauptmenü wird angezeigt, wenn nach Einschalten des Geräts die Initialisierungsphase abgeschlossen ist. Über das Tastenfeld mit den 4 Pfeilen und den Tasten „OK“, „ESC“, „F1“ und „F2“ kann in der Anzeige durch die einzelnen Menüs navigiert werden. Das Hauptmenü kann immer durch mehrmaliges Drücken der „ESC“ Taste erreicht werden. Im Hauptmenü werden die wichtigsten Statusinformationen des Gerätes angezeigt. In der obersten Zeile wird der momentane Betriebsstatus, der Offset zur internen Uhr sowie Zeit und Datum angezeigt.

Bei einem GPS Empfänger kann hier auch „GPS: COLD BOOT“, „GPS: WARM BOOT“ oder „GPS: UPDATE ALMANAC“ erscheinen. Wenn die Antennenleitung unterbrochen ist, kommt hier die Meldung „GPS: ANTENNA FAULTY“.

Unten werden das aktuelle Datum, Name der Zeitzone (bei NTP immer UTC; für die seriellen Schnittstellen kann eine andere Zeitzone eingestellt werden) und die aktuelle Zeit angezeigt. Hinter der Uhrzeit kann ein „*“ erscheinen, wenn die Einstellung „Ignore Lock“ (Simulationsmodus) aktiviert wurde.

Mittels der mehrfarbigen LEDs werden Zustände des Zeitserver angezeigt:

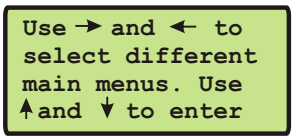
„Ref. Time“
grün: die Referenzuhr (z.B. eingebaute GPS) liefert eine gültige Zeit.
rot: die Referenzuhr liefert keine gültige Zeit (z.B. nicht synchron)

„Time Service“
grün: NTP ist synchron zur Referenzuhr (z.B. eingebaute GPS).
rot: NTP ist nicht synchron oder auf die „local clock“ geschaltet

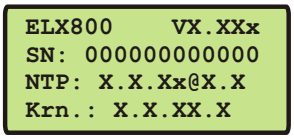
„Network“
grün: alle überwachten Netzwerkanschlüsse sind angeschlossen (Link up)
rot: mindestens einer der überwachten Netzwerkanschlüsse (siehe „Setup Device Parameter / Check Network Linkup“) ist nicht angeschlossen (kein Link)

„Alarm“
aus: kein Fehler
rot: allgemeiner Fehler – weitere Informationen auf dem Display.

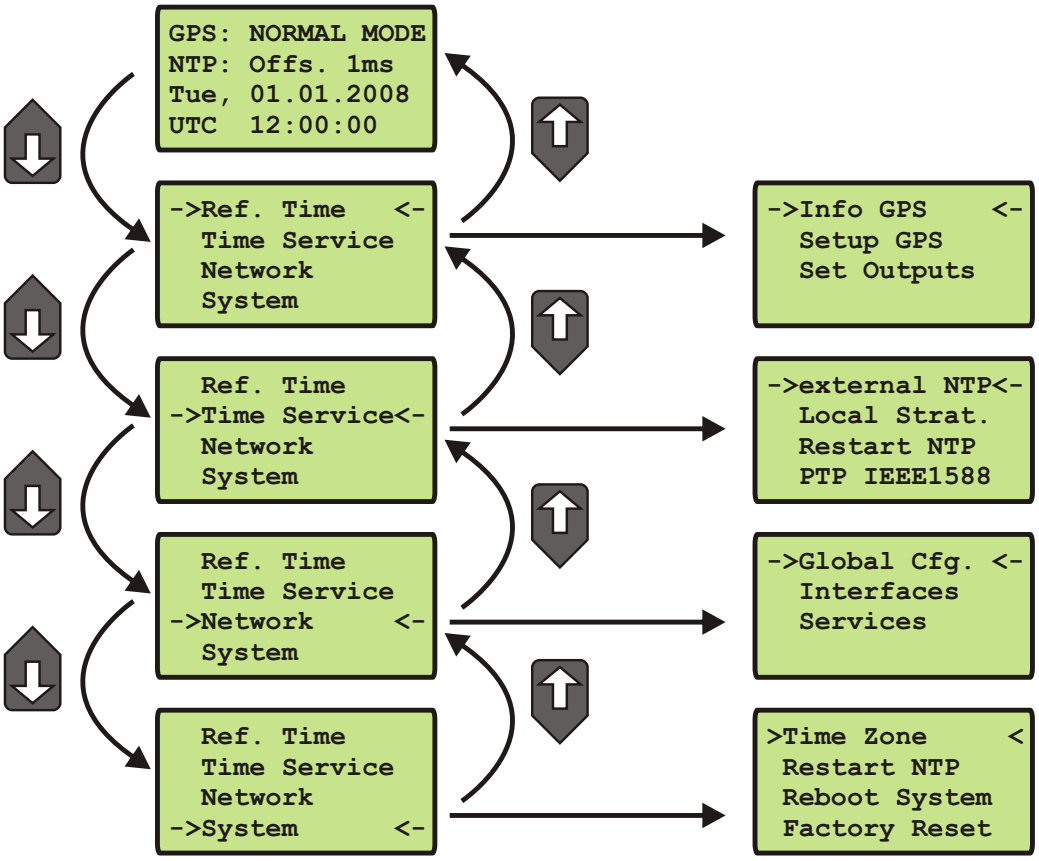
Mit „F1“ aus dem Hauptmenü wird eine kurze Beschreibung zur Navigation mit den Tasten durch die Menüs angezeigt.



Durch Drücken der „OK“ Taste im Hauptmenü wird eine Seite mit den Software Versionen für den LANTIME, NTP und das Betriebssystem angezeigt.



Mit den Pfeiltasten „UP“ und „DOWN“ kann durch die einzelnen Hauptmenüs navigiert werden. Folgende Hauptmenüs stehen zur Verfügung (die PTP Seite wird nur mit entsprechender Option angezeigt):

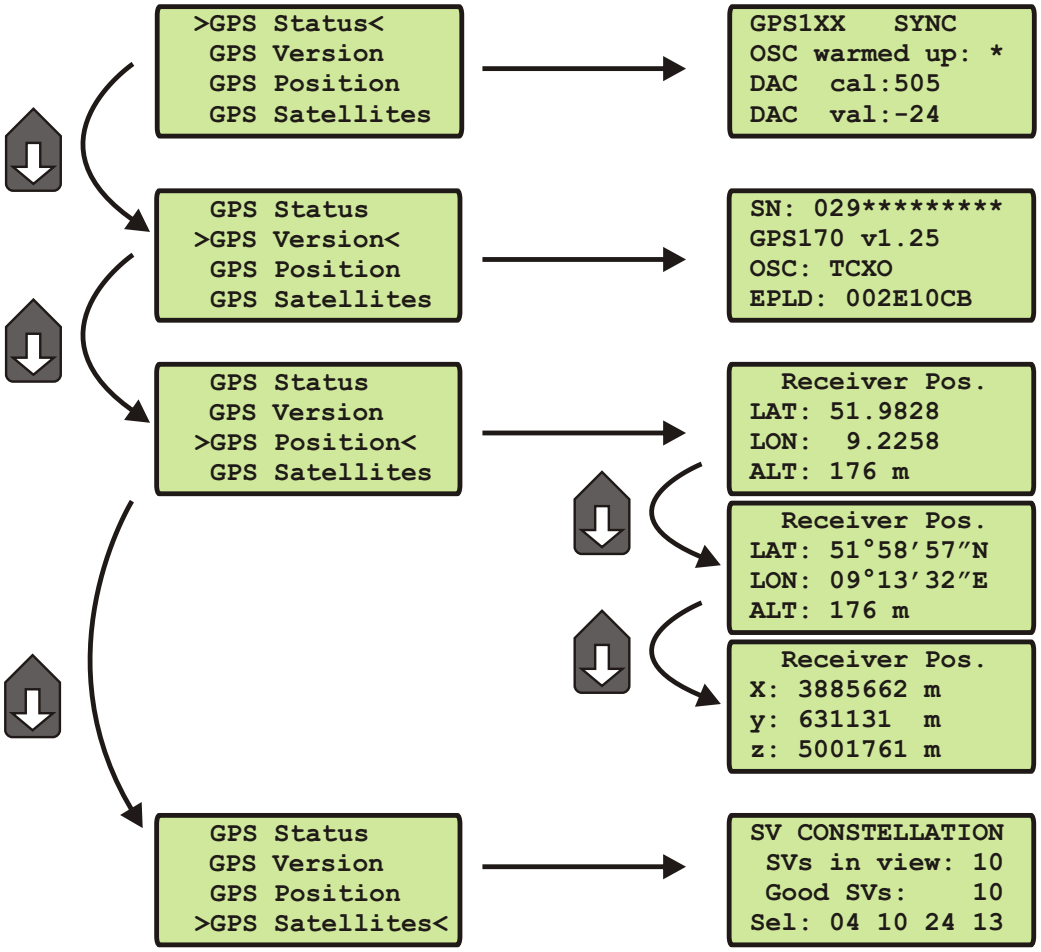


12.3 Menü: Reference Time

Alle Statusinformationen und Einstellungen zur Referenzuhr werden über dieses Menü vorgenommen.

Mit der „OK“ oder Pfeil-Rechts Taste werden die Untermenüs geöffnet.

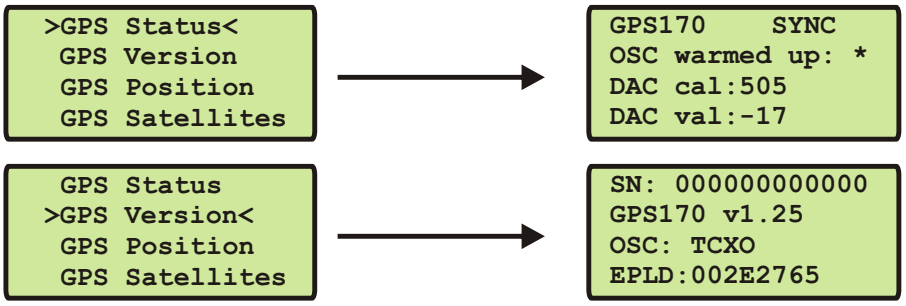
12.3.1 Menü: Info Receiver



In diesem Menü werden alle wichtigen Informationen zur GPS Funkuhr, des internen Oszillators und der GPS Satelliten angezeigt.

GPS170 Status und Version

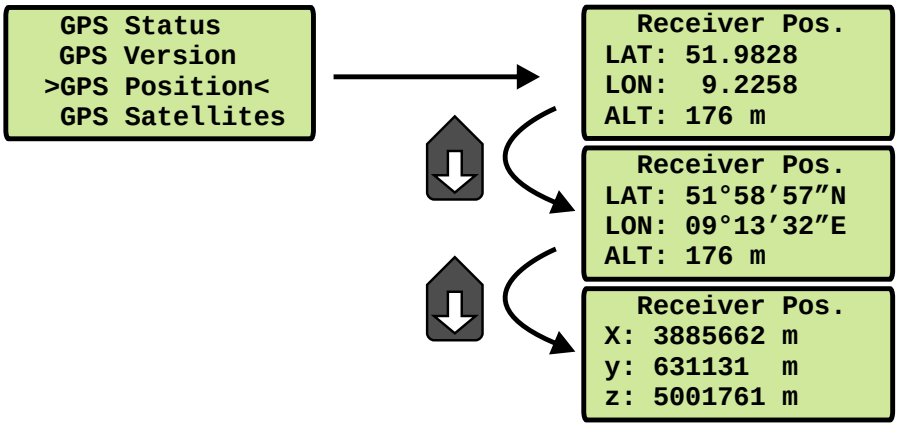
Alle Statusinformationen und Einstellungen zur Referenzuhr werden über diese Menüs vorgenommen.



In der ersten Zeile wird der Typ der Referenzuhr (hier GPS) mit dem aktuellen Status der Funkuhr angezeigt. Unter „GPS Version“ werden die Versionsnummer der Firmware, die Seriennummer der Referenzuhr und der eingebaute Typ des Oszillators angezeigt.

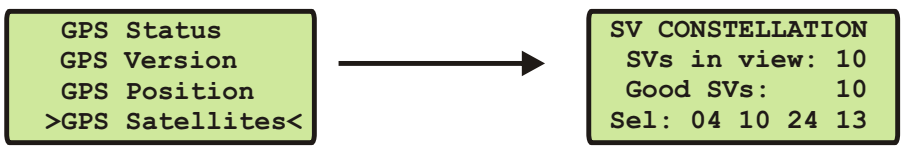
GPS170 - Receiver Position

Dieses Menü zeigt die aktuelle Empfängerposition an. Mit Hilfe des Tasters OK kann zwischen drei Formaten gewählt werden: Das Standardformat zeigt geographische Breite (Latitude), geographische Länge (Longitude) und Höhe über Normal Null (Altitude); wobei Breite und Länge in Grad, Minuten und Sekunden sowie die Höhe in Metern angegeben werden. Das nächste Format ist auch geographisch, jedoch werden Breite und Länge in Grad mit Nachkommastellen angezeigt. Das dritte Format gibt die Position in kartesischen Koordinaten (Earth Centered, Earth Fixed; ECEF) an, wobei der Nullpunkt mit dem Mittelpunkt der Erde zusammenfällt und die x-Richtung in der Äquatorebene zum Null-Meridian weist.

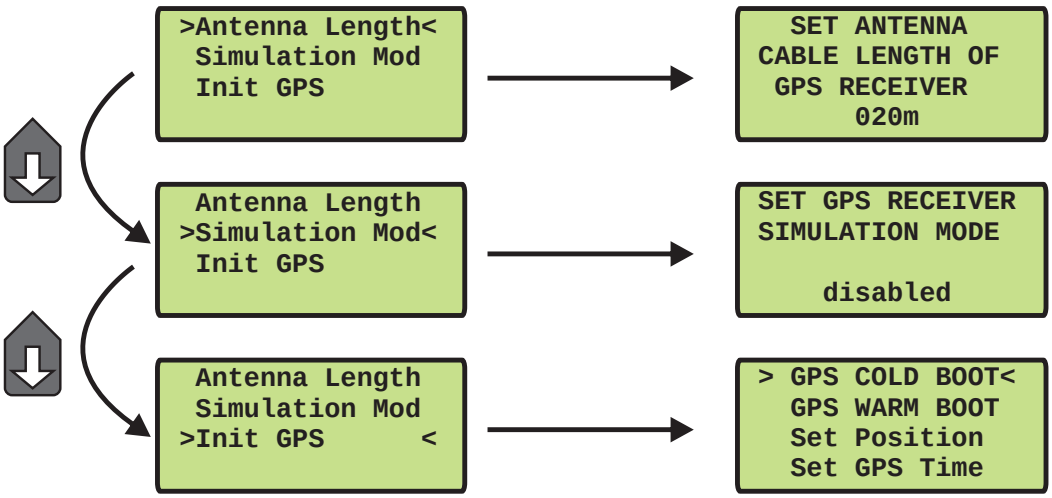


GPS170 - Satellite Constellation

Das Menü Satellitenkonstellation (Satellite Constellation) gibt einen Überblick, wie viele Satelliten nach den Berechnungen des Empfängers gerade in Sicht sind, d.h., eine Elevation von mindestens 5° über dem Horizont haben. Der zweite Wert gibt die Anzahl der Satelliten an, die empfangen und zur Positionsbestimmung genutzt werden können und der letzte Wert zeigt die Nummern der momentan zur Positionsbestimmung benutzten vier Satelliten.

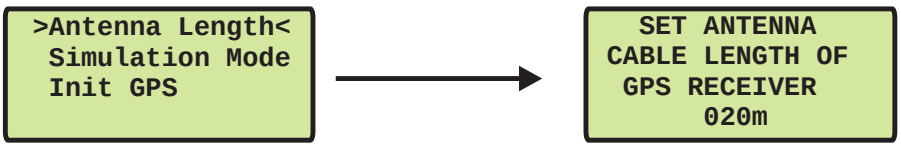


12.3.2 Menü: Setup GPS170



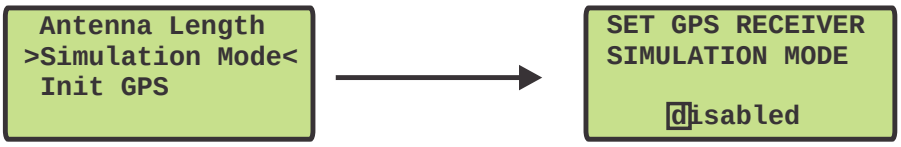
12.3.3 Set Antenna Cable Length

Dieses Menü erlaubt es dem Benutzer, die Signallaufzeit des Antennenkabels zu kompensieren. Das empfangene Zeitraster wird um ca. 5ns/m Antennenkabel verzögert. Durch Eingabe der Kabellänge wird dieser Zeitfehler automatisch ausgeglichen. Als Defaultwert wird bei Auslieferung 20m eingestellt. Die maximale Eingabemöglichkeit ist auf 500m begrenzt (Spezialkabel).

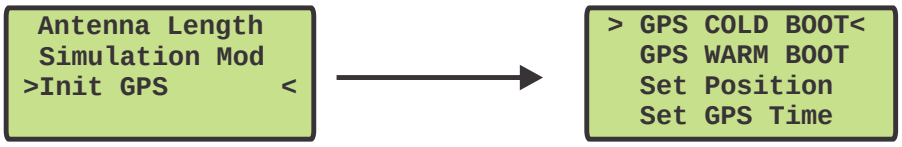


12.3.4 Set GPS Receiver Simulation Mode

Dieses Menü erlaubt es dem Benutzer, das LANTIME auch ohne Antenne zu betreiben. Normalerweise verliert der NTPD die Synchronisation zur GPS wenn die Antenne abgezogen ist oder nicht genügend Satelliten empfangen werden (rote FAIL LED leuchtet). Über die Aktivierung des Simulation Mode werden die entsprechenden Statusinformationen für den NTPD fest auf SYNC gesetzt. Dadurch ist es auch möglich andere Uhrzeiten, welche über das SETUP Menü eingetragen wurden, an den NTPD zu übermitteln. Im Normalfall sollte dieser Punkt disabled sein. Ist diese Einstellung aktiviert, wird im Hauptmenü ein „*“ hinter der Uhrzeit angezeigt.



12.3.5 Menü: Init GPS



Initiate Cold Boot of GPS Receiver

Dieses Menü erlaubt es dem Benutzer alle GPS-Systemwerte zu initialisieren, d.h. alle gespeicherten Satellitendaten werden gelöscht. Bevor die Initialisierung erfolgt, wird nochmals eine Bestätigung des Bedieners erwartet. Anschließend geht das System in die Betriebsart COLD BOOT, um nach einem Satelliten zu suchen und von diesem die aktuellen Parameter einzulesen.

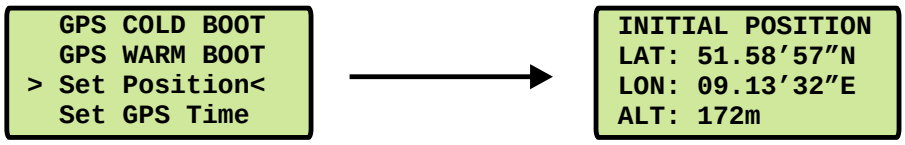
Hinweis:
Bitte beachten Sie, dass der Receiver ungefähr 15 Minuten benötigt, um die Informationen der Satelliten neu einzulesen und den COLD BOOT abzuschließen!

Initiate Warm Boot of GPS Receiver

Dieses Menü erlaubt es dem Benutzer, den Empfänger in den BOOT MODE zu schalten. Das kann erforderlich sein, wenn die Satellitendaten im batteriegepufferten Speicher zu alt sind oder wenn das Gerät an einem Ort in Betrieb genommen wird, der mehrere hundert Kilometer vom letzten Betriebsstandort entfernt ist, da dann die Berechnung der Sichtbarkeit der Satelliten falsche Ergebnisse liefert. Wenn der Benutzer in einem solchen Fall manuell in den BOOT MODE schaltet, kann die Zeitspanne bis zur Synchronisation wesentlich verringert werden, obwohl der Empfänger dieses nach einer Weile selbst tun würde, wenn keine Satelliten empfangen werden können. Nach Bestätigung der Auswahl geht das Gerät in die Betriebsart WARM BOOT, wenn sich noch gültige Satellitendaten im Speicher befinden, ansonsten werden diese im COLD BOOT neu eingelesen.

Init Receiver Position

Wenn der Empfänger zum ersten Mal an einem neuen Standort in Betrieb genommen wird, der weit vom letzten Standort entfernt ist, muss die GPS im Warm Boot nach Satelliten suchen, da die berechneten Werte für Elevation und Doppler zu sehr von den tatsächlichen abweichen. Durch Eingabe der ungefähren neuen Position kann dies vermieden werden, wodurch die Zeit bis zur Synchronisation verkürzt wird.



Init Receiver Time

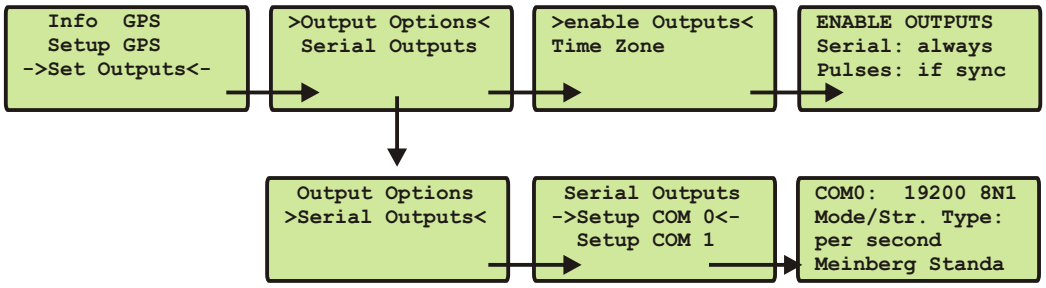
Wenn die Hardware-Uhr des Systems falsch geht, berechnet der Empfänger ungültige Werte für Elevation und Doppler und muss im Warm Boot nach Satelliten suchen. Durch Eingabe der richtigen Zeit kann dies vermieden werden, wodurch die Zeit bis zur Synchronisation verkürzt wird.

Wenn das LANTIME ohne Antenne betrieben wird, können zu Testzwecken auch andere Zeiten eingestellt werden. Dabei ist zu beachten, dass zum einen der NTPD sich nicht mehr auf die GPS Referenzuhr synchronisiert, wenn diese keinen Empfang hat und zum anderen sich der NTP automatisch beendet, wenn die Abweichung zwischen Systemzeit und Referenzuhr größer als 1024 Sekunden ist. Für einen solchen Test sollte der Punkt „Simulation Mode“ aktiviert sein (siehe unten). Nach dem manuellen Setzen der Zeit wird die Systemzeit des Rechners auch gesetzt und der NTP neu gestartet.

12.3.6 Menü Set Outputs

Mit Hilfe dieses Untermenüs können die Optionen und Zeitzone der Ausgänge sowie die Übertragungsgeschwindigkeit und Datenformat der seriellen Schnittstelle eingestellt werden.

Standardwerte für serielle Ausgänge:
Defaulteinstellung: COM: 19200 baud, 8N1, pro Sekunde, Meinberg Standard Time String



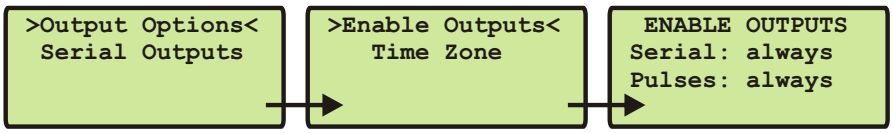
Baudrate: 300 bis 9600
Datenformat: 7E2, 8N1, 8E1, 8O1

COM gibt ein Zeittelegramm sekündlich, minütlich oder auf Anfrage aus. Auf Anfrage bedeutet, dass ein angeschlossener Client ein „?“ senden muss, um als Antwort das Zeittelegramm zu erhalten.Es kann zwischen folgenden Zeittelegrammen gewählt werden. Die genaue Definition dieser Zeittelegramme ist im Anhang beschrieben.

- Standard Meinberg-Telegramm
- GPS Capture-Telegramm
- SAT-Telegramm
- UNI-Erlangen-Telegramm
- NMEA-Telegramm (RMC)
- SPA-Telegramm
- Computime-Telegramm
- Sysplex1-Telegramm
- RACAL-Telegramm

12.3.7 Enable Outputs

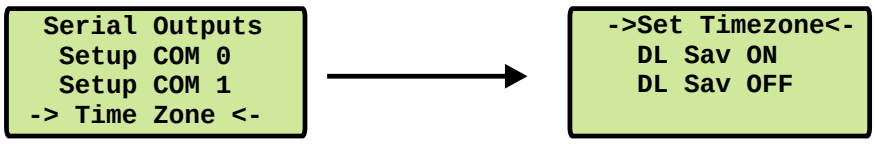
Über dieses Menü können die Puls-Ausgänge (Sekundenimpuls, Minutenimpuls und 10 MHz) und die seriellen Ausgänge an der Anschlussseite des Gerätes abhängig vom Zustand des GPS Empfängers parametriert werden. Die Ausgänge können so eingestellt werden, dass diese erst aktiv werden, wenn der GPS Empfänger synchronisiert hat (if sync) oder permanent aktiviert werden (always).



12.3.8 Setup Time Zone

Die Zeitzone der seriellen Ausgänge kann entsprechend eingestellt werden. Diese Einstellungen wirken sich auf die seriellen Schnittstellen und die Timecode Ausgänge aus. Die interne Zeit des Zeitservers und die NTP Zeit bezieht sich immer auf UTC und ist unabhängig von diesen Einstellungen der Zeitzone. Die Anzeige im Display wird über ein anderes Menü eingestellt (Haptmenü: System->Set time zone).

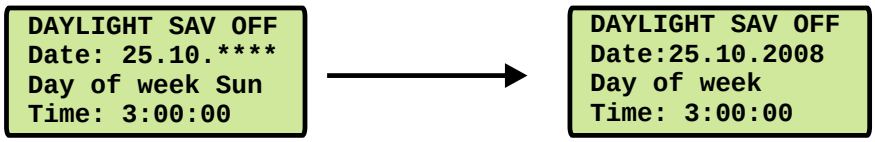
Im ersten Untermenü (Daylight Saving OFF) werden die Einstellungen für die normale Ortszeit (Winterzeit) vorgenommen. Im zweiten Untermenü (Daylight Saving ON) wird hingegen die Sommerzeit konfiguriert.



Nach der Auswahl einer von beiden Menüpunkten gelangt man hier zu den Einstellmöglichkeiten der Winter- bzw. Sommerzeit. Exemplarisch wird in der oben angegebenen Abbildung die Konfiguration der Winterzeit aufgezeigt.

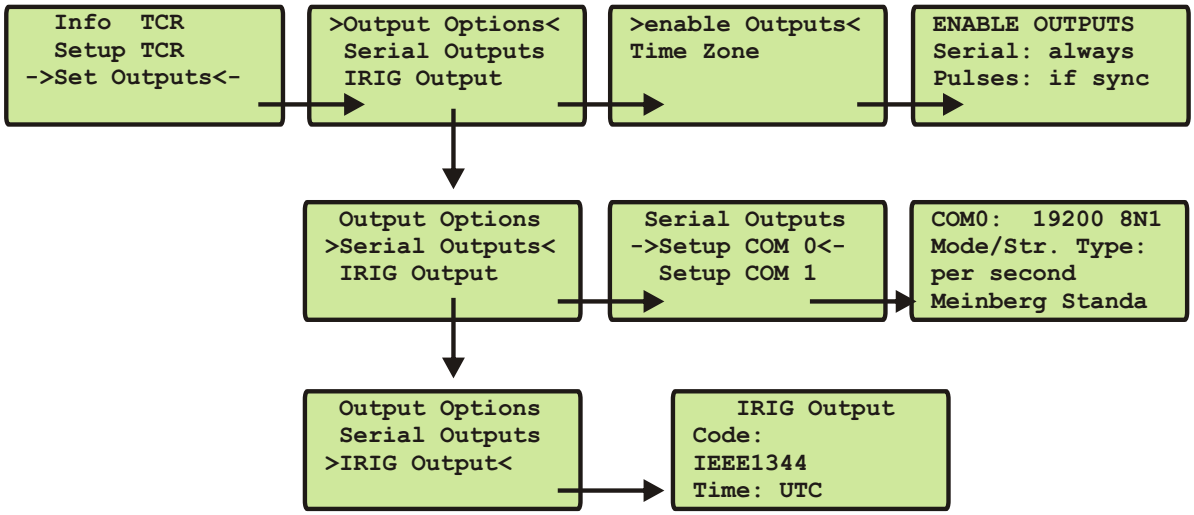
In der ersten editierbaren Zeile werden Name und Abweichung für die normale Ortszeit angegeben (z.B.: MEZ = UTC + 1h).

Die beiden folgenden Zeilen dienen der Eingabe des Umschaltzeitpunktes, in dem die Winterzeit aktiviert wird. GPS bietet zwei Möglichkeiten zur Eingabe von Sommer-/Winterzeit: Entweder werden Datum und Uhrzeit der Umschaltpunkte für ein Jahr exakt definiert oder es werden Randbedingungen gesetzt, mit deren Hilfe das Gerät automatisch für mehrere Jahre den Tag der Umschaltung bestimmen kann. Die Abbildungen unten zeigen beide Varianten: Wird die Jahreszahl als ´*´ angezeigt, muss ein Wochentag eingegeben werden; dann ist der Tag der Umschaltung der erste Tag ab dem eingegebenen Datum, der mit dem eingegebenen Wochentag übereinstimmt. In der Abbildung unten ist z.B. der 25.10. im Jahr 2008 ein Samstag, am darauf folgenden Sonntag, den 26.10., zur angegebenen Uhrzeit, findet die Umschaltung auf Winterzeit statt. Wird eine bestimmte Jahreszahl eingegeben, ist der Tag der Umschaltung genau festgelegt und der Wochentag wird als ´*´ angezeigt.



Für den Fall, dass keine Sommerzeitumstellung benötigt wird, sind unter beiden Menüpunkten (DAYlight SAVING ON / OFF) beliebige aber exakt gleiche Daten, Zeiten und Offsets zu setzen. Nach Eingabe dieser Werte sollte ein Restart des Gerätes erfolgen.

12.3.9 Option: Menü Set IRIG Output (Bei vorhandenem Display)

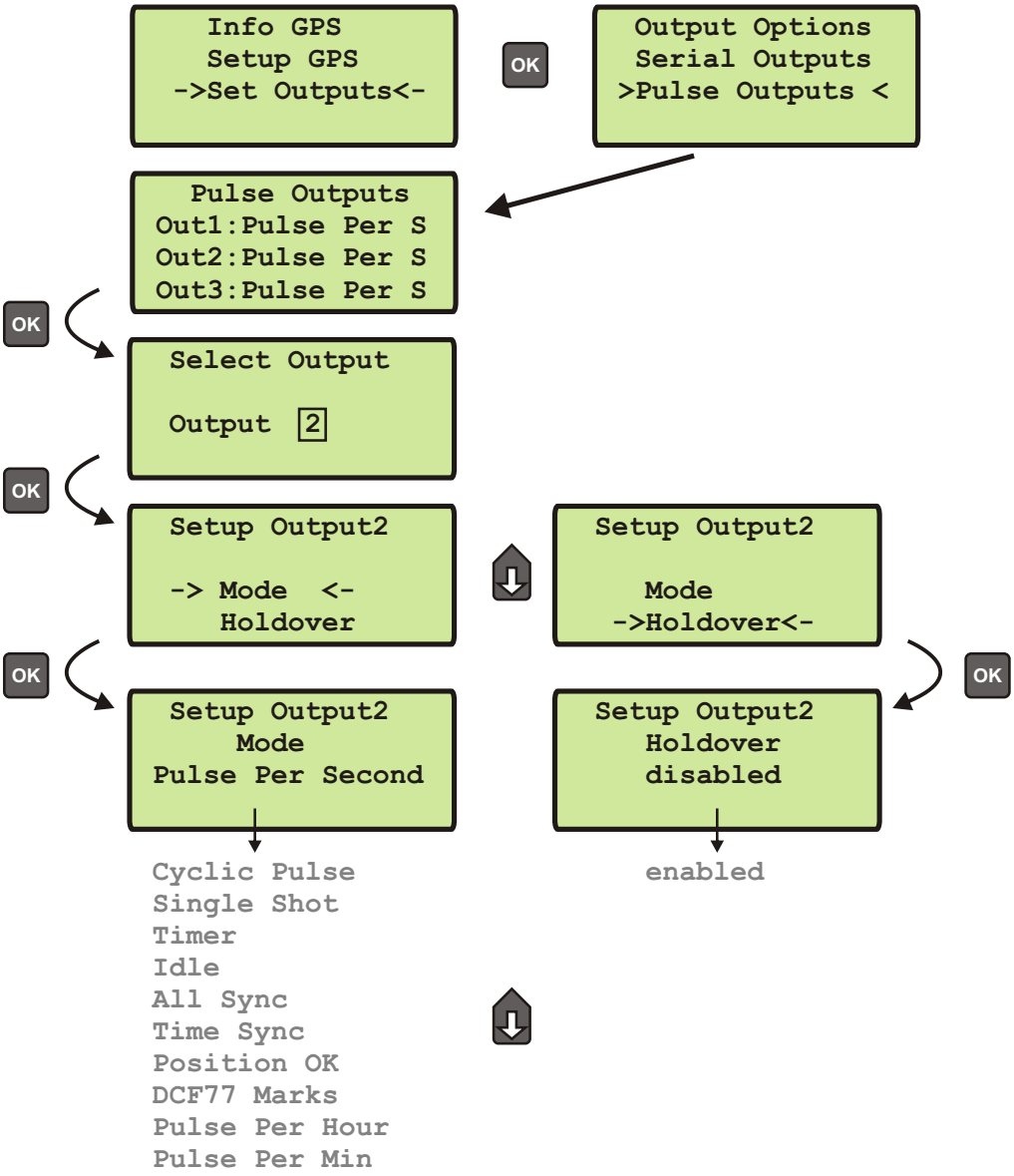


In diesem Untermenü können die optional vorhandenen IRIG Ausgänge eingestellt werden.
Folgende Werte sind möglich:

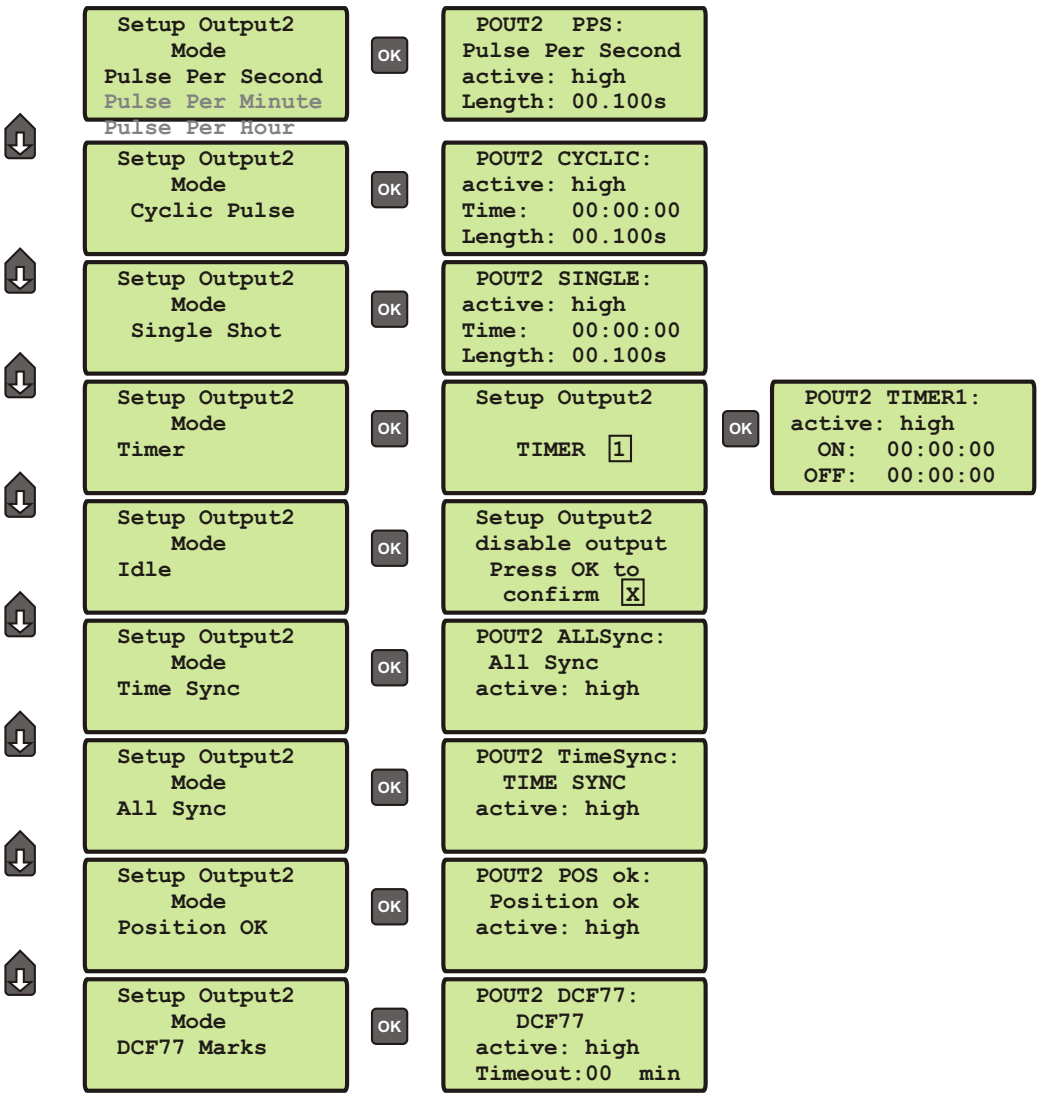
IRIG Code	B002+B122 B003+B123 B006+B126 B007+B127 AFNOR NFS-87500 IEEE1344
Time	local UTC

12.3.10 Option: Menü Setup Progr. Pulses

Stellt die angeschlossene Funkuhr programmierbare Impuls/Schaltausgänge zur Verfügung, so können deren Einstellungen hier verändert werden. Der Menüpunkt erscheint nicht im Menü Outputs, wenn von der angeschlossenen Funkuhr keine programmierbaren Ausgänge zur Verfügung gestellt werden.



Im Untermenü „Mode“ wird der Betriebsmodus des jeweiligen Ausgangs festgelegt. Verfügbare Betriebsmodi sind: Timer, Single Shot, Cyclic Pulse, Pulse Per Second, Pulse Per Min, Pulse Per Hour, DCF77 Marks, Position OK, Time Sync, All Sync und Idle. Je nach gewähltem Modus und Bestätigung durch „OK“ werden unterschiedliche Steuerelemente im Display dargestellt.



Timer Modus
Im Timer Modus simuliert der Ausgang eine Schaltuhr mit Tagesprogramm. Auf jedem Ausgang der Funkuhr sind je drei Ein- und drei Ausschaltzeiten am Tag programmierbar. Soll eine Schaltzeit programmiert werden, so muss die Einschaltzeit „On“ und die zugehörige Ausschaltzeit „OFF“ eingetragen werden. Liegt der Einschaltzeitpunkt später als der Ausschaltzeitpunkt, so wird das Schaltprogramm derart interpretiert, dass der Auschaltzeitpunkt am darauffolgenden Tag liegt.

Ein Programm On Time 23.45.00, Off Time 0.30.00 würde demnach bewirken, dass am Tag n um 23.45 Uhr der Ausgang z.B. PORT1 aktiviert, und am Tag n+1 um 0.30 Uhr deaktiviert wird. Sollen eines oder mehrere der drei Programme ungenutzt bleiben, so müssen in die Felder On und Off nur gleiche Schaltzeiten eingetragen werden. Mit „active“ wird der Aktiv Zustand für die Schaltzeiten angegeben. Ist „active: high“ angewählt, liegt am entsprechenden Ausgang im inaktiven Zustand (außerhalb einer Schaltzeit) ein low - Pegel, und im aktiven Zustand ein high - Pegel an.

Cyclic Pulse - Erzeugung zyklisch wiederholter Impulse
Im Modus Cycle wird die Zeit zwischen zwei Impulsen eingegeben. Diese Zykluszeit muss immer in Stunden, Minuten und Sekunden eingegeben werden. Zu beachten ist, dass die Impulsfolge immer mit dem Übergang 0.00.00 Uhr Ortszeit synchronisiert wird. Dies bedeutet, dass der erste Impuls an einem Tag immer um Mitternacht ausgegeben wird, und ab hier mit der gewählten Zykluszeit wiederholt wird. Eine Zykluszeit von 2sek würde also Impulse um 0.00.00Uhr, 0.00.02 Uhr, 0.00.04 Uhr etc. hervorrufen. Grundsätzlich ist es möglich jede beliebige Zykluszeit zwischen 0 und 24 Stunden einzustellen, jedoch machen meistens nur Impulszyklen Sinn, die immer gleiche zeitliche Abstände zwischen zwei Impulsen ergeben. So würden zum Beispiel bei einer Zykluszeit von 1Stunde 45min Impulse im Abstand von 6300 Sekunden ausgegeben. Zwischen dem letzten Impuls eines Tages und dem 0.00Uhr Impuls würden jedoch nur 4500 Sekunden liegen.

DCF77 Marks
Im Betriebsmodus DCF77 Marks wird der gewählte Ausgang in den DCF77 Simulationsmodus geschaltet, der Ausgang wird im Takt der für den DCF77 Code typischen 100 und 200 ms Impulse (logisch 0/1) aktiviert.

Im Feld 'Timeout' kann eingegeben werden, nach wieviel Minuten im Falle eines Freilaufes der Funkuhr der DCF-Simulationsausgang abgeschaltet werden soll. Wird hier der Wert Null eingegeben, ist die Timeout Funktion inaktiv.

Single Shot Modus
Der Single Shot Modus erzeugt pro Tag einen einmaligen Impuls definierter Länge.
Im Feld Time wird die Uhrzeit eingegeben, zu der ein Impuls erzeugt werden soll. Der Wert „Length" erlaubt die Einstellung der Impulsdauer in 10ms Schritten zwischen 10ms und 10sek. Eingaben, die nicht im 10ms Raster liegen werden abgerundet.

Pulse Per Second, Per Min, Per Hour Modus
Diese Modi erzeugen Impulse definierter Länge pro Sekunde, pro Minute oder pro Stunde. Das angezeigte Menü ist für alle drei Betriebsarten gleich. Der Wert „Length" bestimmt die Impulsdauer in 10ms Schritten zwischen 10ms und 10sek.

Position OK, Time Sync und All Sync
Zur Ausgabe des Synchronisationsstatus der Funkuhr sind drei verschiedene Modi auswählbar. Im Modus 'Position OK' wird der Ausgang aktiviert, wenn der GPS Empfänger genügend Satelliten empfängt um seine Position zu berechnen.

Der Modus 'Time Sync' aktiviert den Ausgang immer dann, wenn die interne Zeitbasis der Funkuhr mit dem Timing des GPS Systems synchronisiert wurde. Der Modus 'All Sync' führt eine UND Verknüpfung beider Zustände durch, d.H. der entsprechende Ausgang wird immer dann aktiviert, wenn die Position berechnet werden kann UND die interne Zeitbasis synchronisiert wurde.

Idle Modus
Über den Modus 'IDLE' können die programmierbaren Impulsausgänge einzeln deaktiviert werden.

Holdover
In der Betriebsart „enabled" bleibt der Ausgang eingeschaltet, im „disabled" Betrieb wird der Ausgang bei Verlust der Synchronisation abgeschaltet.

12.4 Menü: Time Service

Alle Statusinformationen und Einstellungen zum NTP werden über dieses Menü vorgenommen.

12.4.1 Menü: External NTP

Zu den internen Referenzuhren (Local Clock, GPS, PPS) können zusätzlich externe NTP Server mit berücksichtigt werden. Die interne Referenzuhr hat immer Vorrang vor den externen NTP Servern. Wenn die interne Referenzuhr nicht synchron oder ausgefallen ist, schaltet der NTP automatisch auf eine der externen NTP Server um. Über diesen Menüpunkt können noch weitere NTP Server konfiguriert werden.

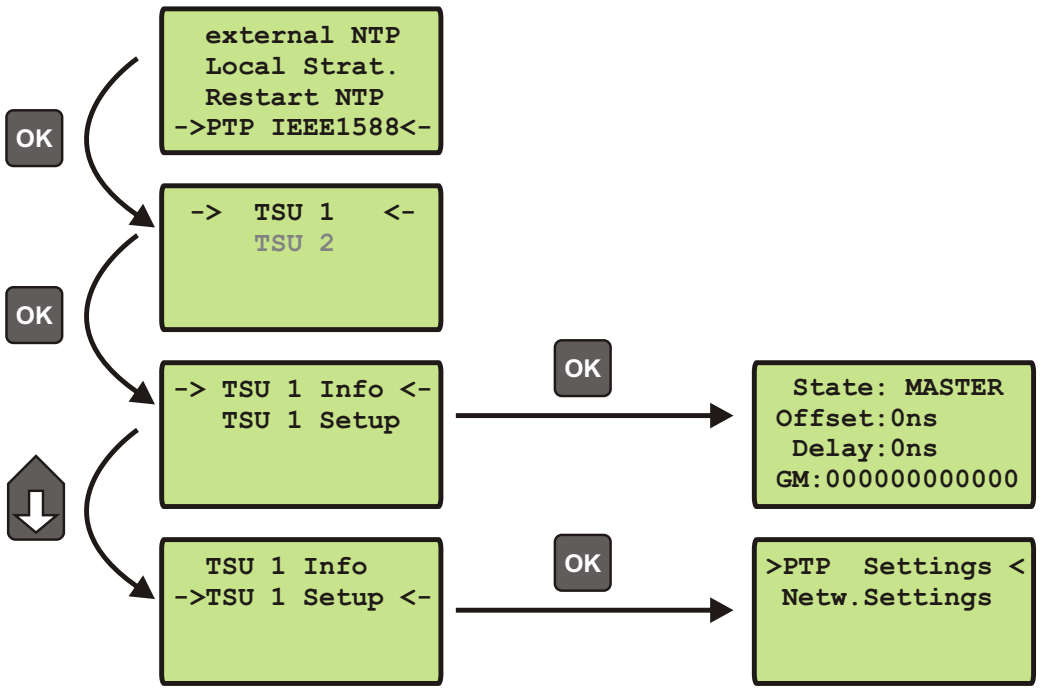
12.4.2 Menü: Stratum of local clock

Die „Local Clock“ wird vom NTP als eine Referenzuhr benutzt. Diese entspricht der Hardwareuhr des Rechners. Wenn keine Referenzuhr (GPS oder externe NTP Server) mehr zur Verfügung steht, schaltet der NTP auf diese „Local Clock“ zurück. Der Stratum-Wert der „Local Clock“ kann über dieses Menü eingestellt werden. Der Stratum-Wert unter NTP entspricht der Güte der Referenzuhr oder dem Abstand zur nächsten Referenzuhr.

12.4.3 Menü: Restart NTP

Mit diesem Menüpunkt wird die Systemzeit einmalig mit der Referenzuhr gesetzt und der NTP neu gestartet.

12.4.4 Option: Menü PTP v2 - IEEE 1588-2008



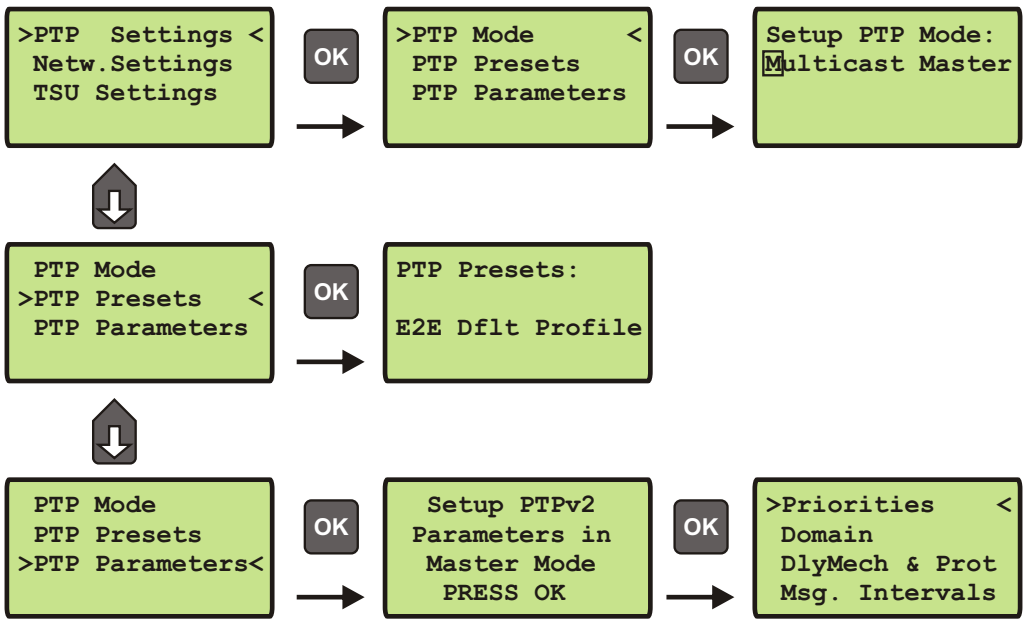
Das Menü für die PTP IEEE 1588 Konfiguration befindet sich unter der Hauptmenükategorie „Time Service“ und ist in die Abschnitte „TSU x Info“ und „TSU x Setup“ unterteilt. In einem Gerät mit mehr als einer PTPv2 Karte (auch TSU, Time Stamp Unit genannt), werden die Untermenüs für alle PTP Karten aufgelistet.

Menü TSU Info

Die Seite „TSU x Info“ vermittelt einen Überblick über den Status der wichtigsten Parameter des PTP Subsystems. Die Zusammenstellung der Parameter ist abhängig vom eingestellten Modus. In der Betriebsart „Grandmaster“ wird hier der „MASTER“ Zustand dargestellt. Die Werte für Offset und Delay sind im Master-Modus auf 0 gesetzt. Darüber hinaus wird die MAC-Adresse des Grandmasters eingeblendet.

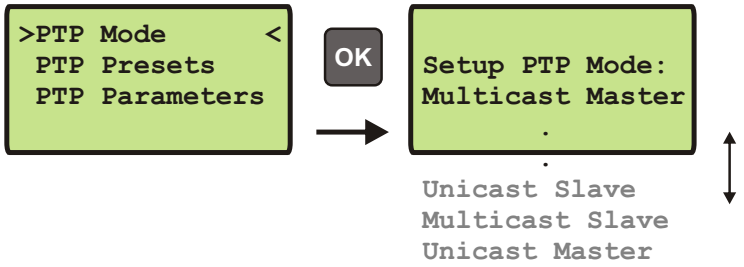
Bei MRS (Multi Reference Source) Geräten erscheint hier alternativ der Zustand der Betriebsart „Slave“.

Menü TSU Setup



In diesem Menu können die Einstellungen für alle PTP Parameter für die ausgewählte PTP Schnittstelle vorgenommen werden.

Menü PTP Mode



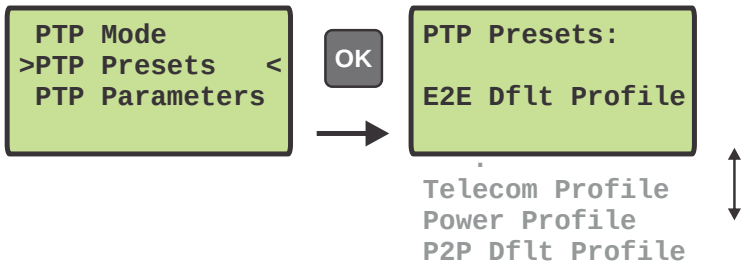
Die Anzahl der möglichen PTP Modi hängt von den Features des Gerätes ab.

Unterstütze Modi auf einem reinen GPS System:
- PTPv2 Multicast Master
- PTPv2 Unicast Master

Unterstützte Modi auf einem MRS (Multi Reference Source) System:
- PTPv2 Multicast Slave
- PTPv2 Multicast Master
- PTPv2 Unicast Slave
- PTPv2 Unicast Master

PTP Presets laden

Jedes „PTP Preset“ stellt einen Satz von PTP Parametern dar, mit dem man die PTP Einheit in einem Schritt auf ein bestimmtes PTP Profil umschalten kann. Nachdem ein bestimmtes Preset eingestellt wurde, besteht aber immer noch die Möglichkeit die einzelnen Parameter zu verändern.



Hinweis: Sobald ein PTP Preset ausgewählt ist, werden die vorher eingestellten PTP Parameter überschrieben!

Es werden drei verschiedene Presets unterstützt:

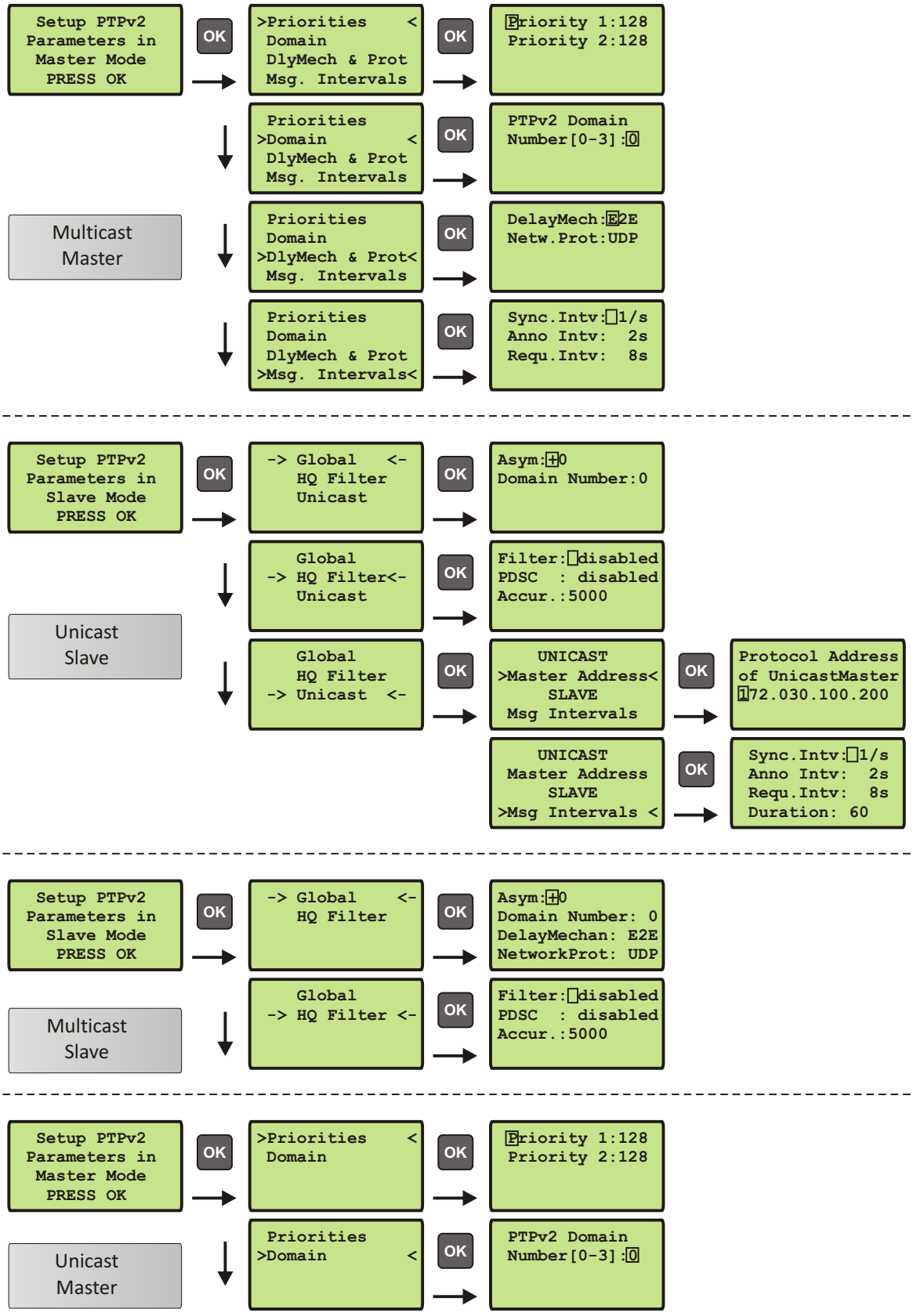
Delay Request-Response Default Profile
- Sync Msg. Rate: 1/sec
- Ann. Msg. Rate: 2 sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech.: „E2E“

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

Telecom Systems Profile (nach ITU-T G.8265.1)
- Mode: Unicast
- Priority 1: 128
- Priority 2: 128
- Delay Mech.: „E2E“
- Default Domain: 4
- Clock Class Mapping nach G.8265.1

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

PTP Parameters



In Abhängigkeit vom eingestellten PTP Mode werden im Untermenu „PTP Parameters“ verschiedene Untermenüs dargestellt.

Parameter für alle PTP Modes:

Priorities:
Priority1 (nur Master):
Das Attribut wird bei der Ausführung des Best-Master-Clock-Algorithmus (BMCA) verwendet.
Geräte mit niedrigeren priority1 Werten haben bei der Wahl des besten Masters Vorrang gegenüber Geräten mit höheren priority1 Werten.
Konfigurierbarer Bereich: 0 .. 255.

Priority2 (nur Master):
Das Attribut wird bei der Ausführung des Best-Master-Clock-Algorithmus (BMCA) verwendet.
Für den Fall, dass der Best-Master-Clock-Algorithmus auch nach Auswertung der PTP Parameter priority1 und der Qualitätsparameter clockClass, clockAccuracy und scaledOffsetLogVariance keinen Master ermitteln konnte, ermöglicht das priority2 Attribut eine Bevorzugung von einem Gerät bevor der so genannte Tie-Break durchgeführt wird. Der Tie-Break basiert auf der clockIdentity (der MAC-Adresse des PTP Ports) und führt schließlich eine endgültige Entscheidung für einen Master herbei. Die Werte clockClass, clockAccuracy und scaledOffsetLogVariance sind vom Status des Grandmasters abhängig und können nicht konfiguriert werden.
Konfigurierbarer Bereich: 0 .. 255.

Domain Number:
Eine PTP Domain ist eine logische Gruppierung von PTP Geräten innerhalb eines physikalischen PTP Netzwerks. PTP Slaves, die sich mit einem bestimmten Master verbinden sollen, müssen alle die Domain Nummer des Masters konfiguriert haben.

Delay Mechanismus:
E2E - End-to-End (Delay Request-Response)
P2P - Peer-to-Peer (Pdelay Request-Response) - wird nur im Multicast Mode unterstützt

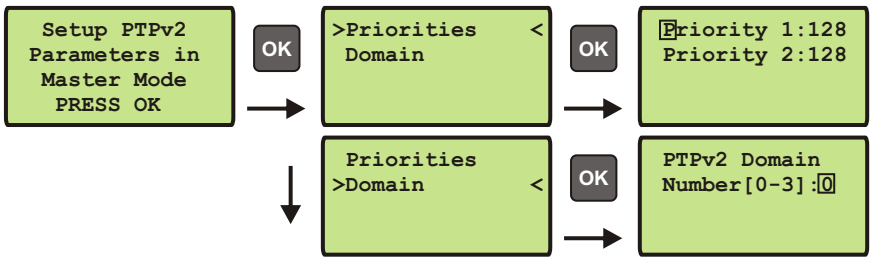
Netzwerkprotokoll:
UDP - UDP/IPv4 (Layer 3)
ETH - IEEE 802.3/Ethernet (Layer 2) - wird nur im Multicast Mode unterstützt

Nur für MRS:
Globale Parameter im PTP Slave Mode:

Asym: (Default Asymmetry Offset)
Falls innerhalb des Netzwerks ein konstanter Asymmetrieoffset bekannt ist, kann dieser Offset zur Kompensation dieses Asymmetrieoffsets eingetragen werden um einen potentiellen Zeitfehler zu korrigieren.
Hinweis: Nur in Umgebungen mit bekanntem Asymmterieoffset verwenden.

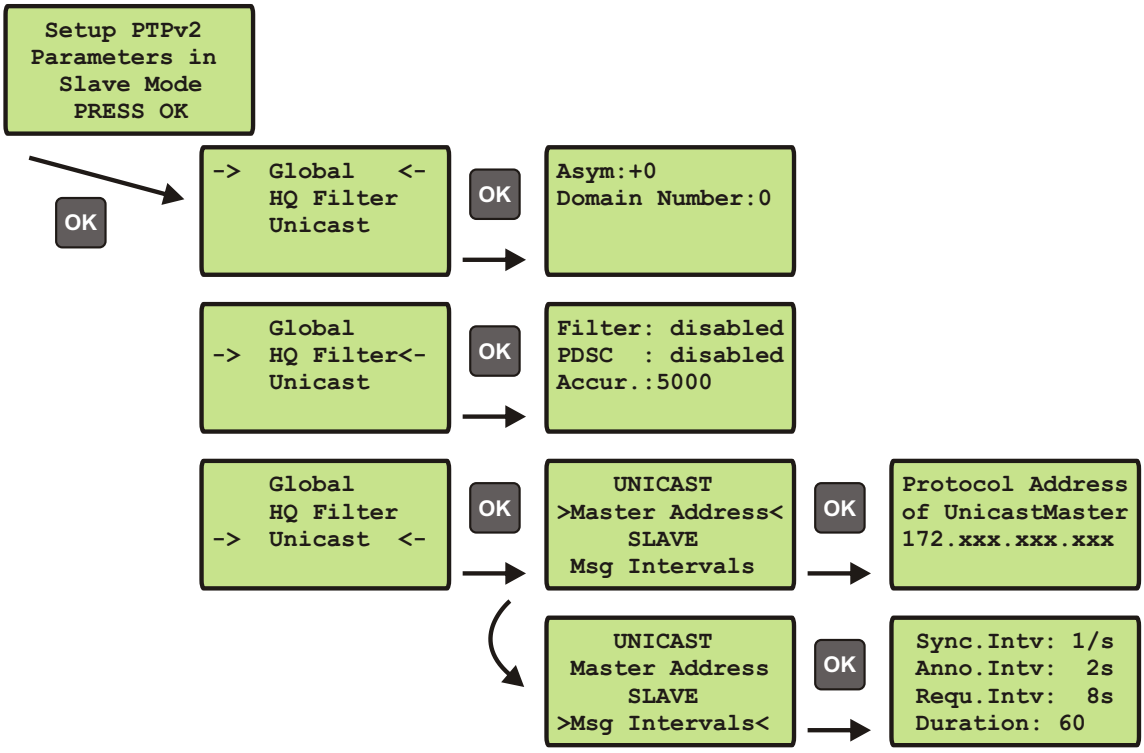
HQ Filter:
Im Slave Modus kann in stark belasteten Netzen bei Verwendung von nicht PTP-fähigen Switchen der „HQ Filter“ zur Verringerung des Jitters eingeschaltet werden. Anwendungsgebiete und Konfigurationsmöglichkeiten sind im Kapitel 8.4.11 beschrieben.

Unicast Master



Falls „Unicast Master“ eingestellt ist, sind ausschließlich Einstellungen bezüglich der Priorities und der Domain Number möglich. Die notwendigen Einstellungen für die zu versendenden Nachrichten müssen im Rahmen des „Unicast Negotiation“ Verfahrens auf den Slaves vorgenommen werden.

Unicast Slave (nur MRS Geräte)



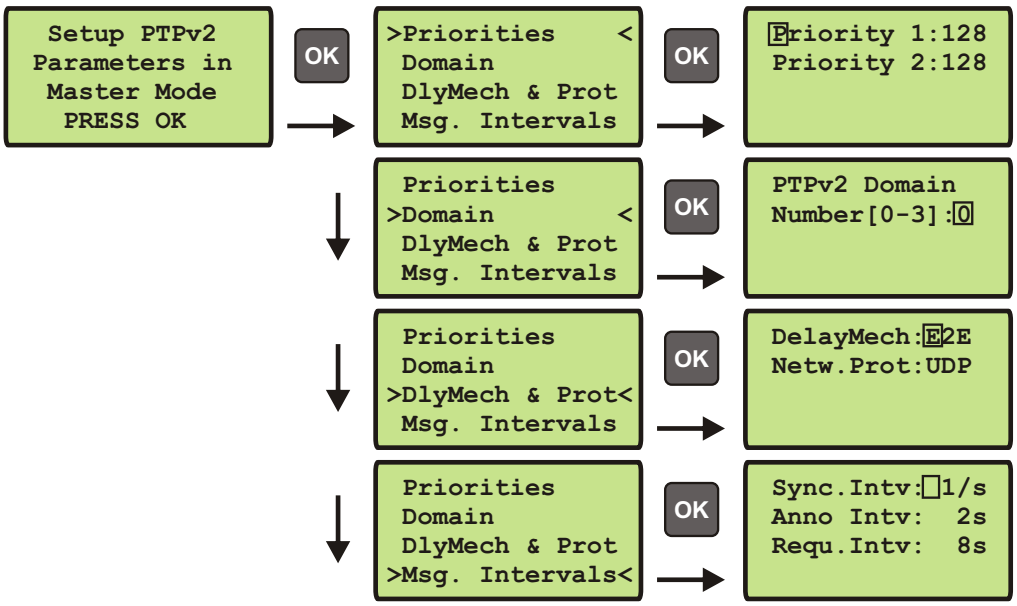
Zusätzlich zu den im Kaptitel „PTP Parameters“ beschriebenen Parametern können im „Unicast Slave“ Betrieb die folgenden Parameter eingestellt werden.

Unter **„Master Address“** muss die IP Adresse des PTP Ports des verwendeten PTP Grandmasters eingestellt sein.

Msg Intervals: Rate und Sendedauer für Sync, Announce und Delay Response Nachrichten
In diesen Untermenüs wird eingestellt, welche Nachrichten bei welcher Rate und mit welcher Dauer von einem Grandmaster angefordert werden sollen. Dies geschieht im Rahmen des „Unicast Negotiation“ Protokolls.

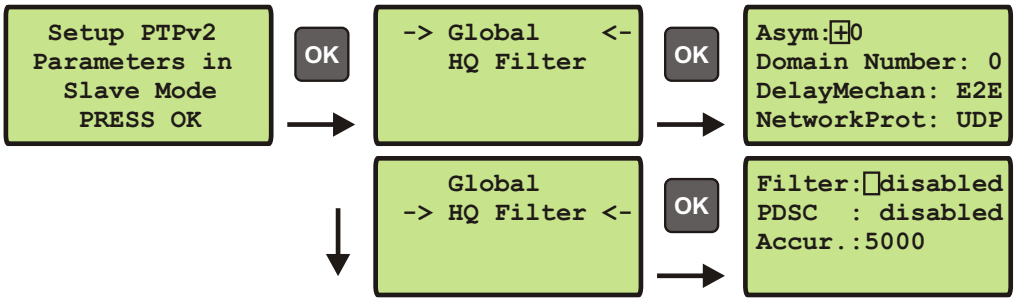
Mit **„Sync. Intv“, „Anno Intv“ und „Requ. Intv“** wird die Rate der Sync-, Announce und DelayRequest Messages eingestellt, mit welcher die jeweilige Nachricht vom Grandmaster zum Slave gesendet wird. Über die **„Duration“** wird bestimmt, wie lange der Master eine bestimmte Nachricht zum Slave senden soll. Um einen kontinuierlichen Empfang eines Nachrichtentyps sicher zu stellen, erneuert der Slave kurz vor Ablauf der „Duration“ seine Anfrage für einen bestimmten Nachrichtentyp. Dieser Vorgang wird im Rahmen des „Unicast Negotiation“ Protokolls automatisch sichergestellt.

Multicast Master



Für den Betrieb im Multicast Master Modus können zusätzlich zu den bereits beschriebenen Parametern aus dem Kapitel PTP Parameters die Paketrate der Sync, Announce und Delay Request Messages eingestellt werden (64/sec...64 sec).

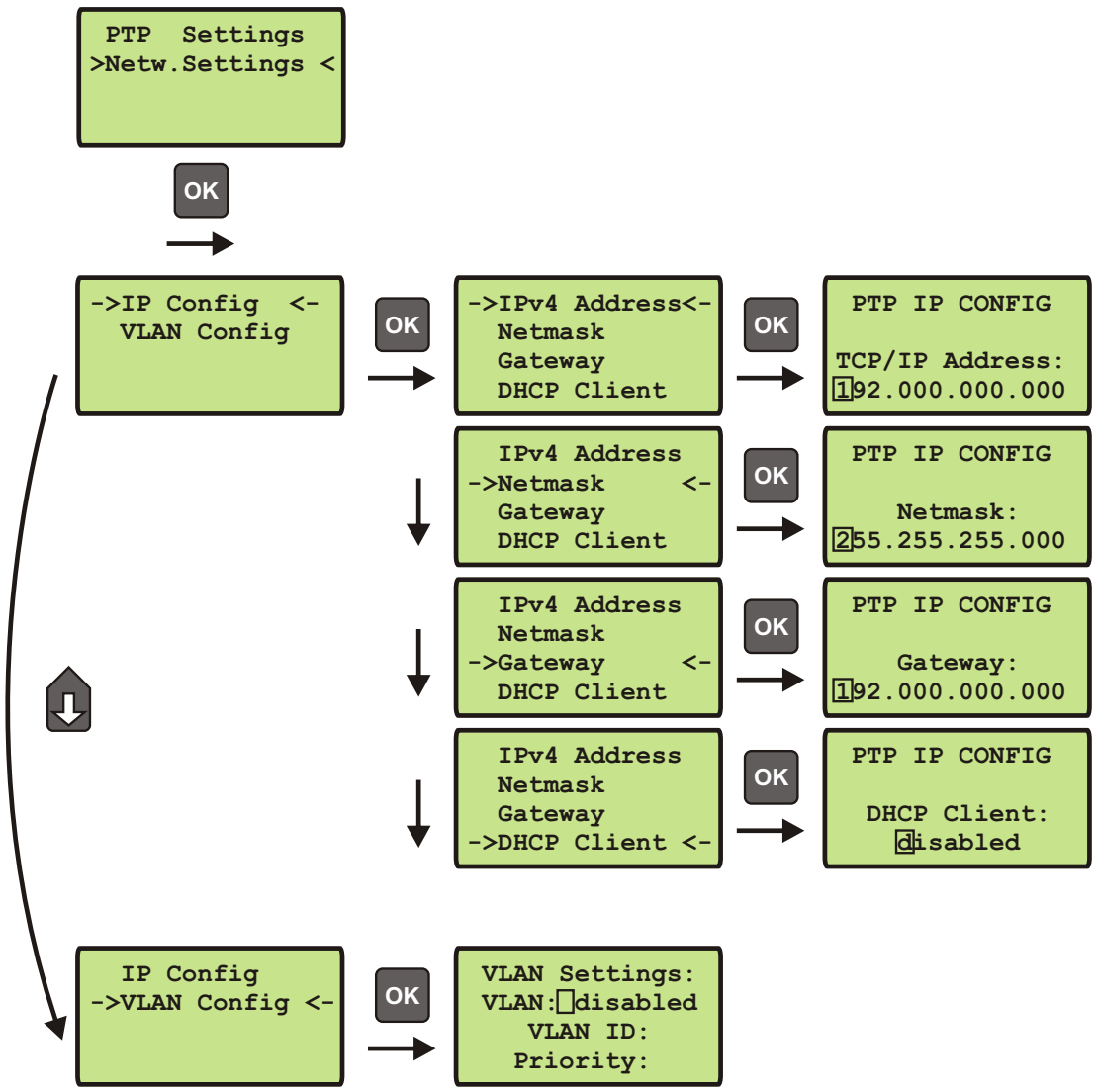
Multicast Slave (nur MRS Geräte)



Für den Betrieb im Multicast Slave Modus können zusätzlich zu den bereits beschriebenen Parametern aus dem Kapitel „PTP Parameters“ die Einstellungen für den „HQ Filter“ vorgenommen werden. Die Funktionsweise ist im Kapitel 8.4.11 erläutert.

Menü Network Settings

Konfigurationseinstllungen für die PTPx Netzwerkschnittstelle

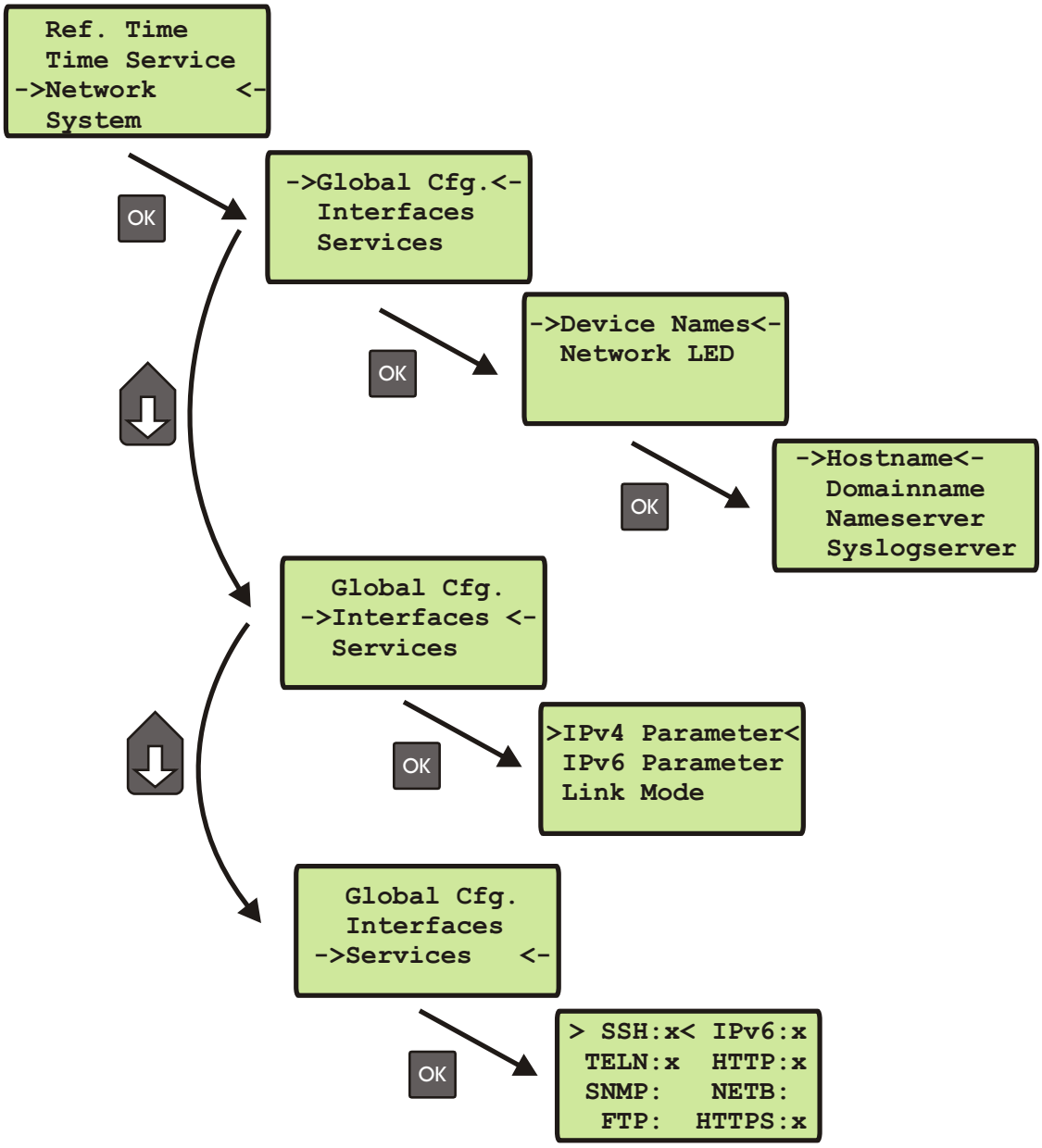


Hier kann die statische IP Konfiguration des PTPx Interfaces vorgenommen werden. Alternativ lässt sich für die PTPx Schnittstelle der DHCP Dienst aktivieren.

VLAN Config:
Virtual LAN (IEEE 802.1Q) Konfiguration für das PTPx Interface:

- VLAN ID: Ein 12-bit Wert (0..4096), der die Zugehörigkeit zu einem VLAN spezifiziert.
- Priority: Die Priorität gibt den „Frame Priority Level“ von 0 (niedrigster) bis 7 (höchster) an, der dazu verwendet wird bestimmte Klassen (Protokolle) des Netzwerkverkehrs zu priorisieren.

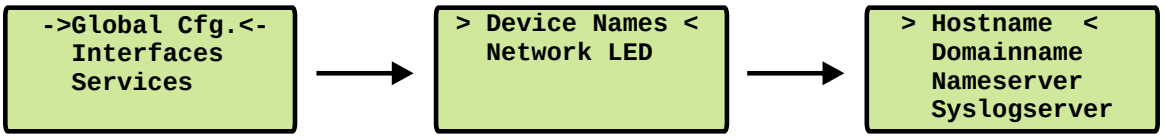
12.5 Menü: Network



In diesem Untermenü werden die Netzwerkparameter festgelegt. Bei der Erstinstallation des LANTIME müssen diese Parameter an das vorhandene Netzwerk angepasst werden.

Differenzierte Einstellungen können dann später über den Netzwerkzugang mit TELNET, SSH oder das WEB Interface 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. Alle Parameter für die Konfiguration des Zeitservers werden in der Datei „/mnt/flash/config/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 Auslieferzustand abgebildet.

12.5.1 Menü: Global Configuration

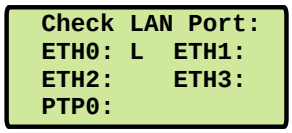


In diesem Untermenü werden Hostname, Domainname, Nameserver und Syslogserver eingestellt

Ein Nameserver und ein Syslogserver können eingetragen werden. Bei den Nameservern und Syslogservern sind nur IPv4 Adressen möglich. Jeweils ein weiterer Nameserver bzw. Syslogserver kann dann später über das WEB-Interface konfiguriert werden. Sind beide Adressen auf 0.0.0.0 gesetzt wird der REMOTE SYSLOG-Dienst nicht verwendet.

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.

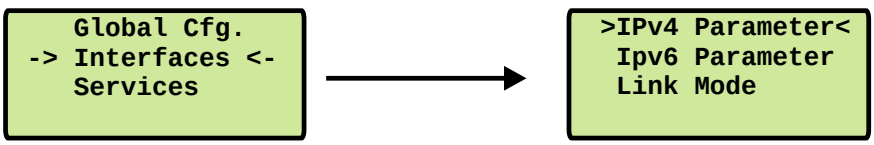
Beachten Sie, dass alle SYSLOG Ausgaben auf dem Zeitserver unter „/var/log/messages“ gespeichert werden und somit nach einem Neustart des Systems gelöscht sind. Ein täglich ausgeführtes Programm (CRON Job) prüft die Größe der Log-Dateien und löscht diese, wenn sie zu groß werden.



Über das Menü „Check Network Linkup“ kann eingestellt werden, welche Netzwerk Ports auf „LINK UP“ überprüft werden sollen. Wenn eine der ausgewählten Schnittstellen keinen LINK hat, wird die rote LED „Network“ an der Vorderseite des Gerätes eingeschaltet.

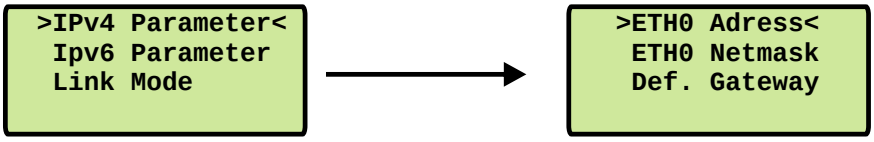
12.5.2 Menü: Network Interfaces

In diesem Untermenü werden die Netzwerkparameter festgelegt. Bei der Erstinstallation des LANTIME müssen diese Parameter an das vorhandene Netzwerk angepasst werden. Es können die folgenden Parameter eingestellt werden:



Differenzierte Einstellungen können dann später über den Netzwerkzugang mit TELNET, SSH oder das WEB Interface 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.

12.5.3 Menü: Setup IPv4 LAN Parameter



Für jeden physikalischen Netzwerkanschluss (RJ45 Buchse) steht ein separater Abschnitt zur Verfügung. 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.

Falls sich ein DHCP Server (Dynamik Host Configuration Protocol) im Netz befindet, kann die Netzwerkeinstellung auch automatisch vorgenommen werden. Die Netzwerkeinstellungen werden dann automatisch von einem DHCP-Server (muss sich bereits im Netzwerk befinden) vorgenommen. Der DHCP-Client vom LANTIME ist nur für das IPv4 Netzwerk Protokoll einsetzbar.

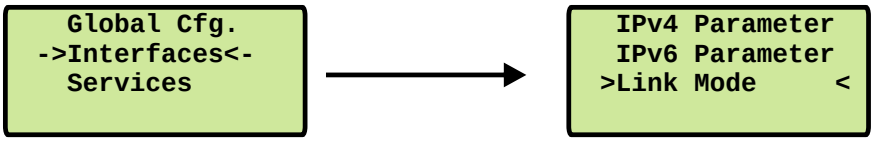
Im Menü werden die möglichen Dienste angezeigt, die der LANTIME zur Verfügung stellt: TELNET, FTP, SSH, HTTP, HTTPS, SNMP und NETBIOS. Die einzelnen Dienste können über die Checkboxen aktiviert oder deaktiviert und werden direkt nach dem Abspeichern entsprechend gestartet oder beendet.

12.5.4 Menü: Setup IPv6 Parameter

Über das Frontpanel können die Parameter für IPv6 nur für die erste Schnittstelle eingestellt werden. Dabei sind drei globale IPv6 Adressen möglich, zwei davon sind über das Front Panel einstellbar, eine weitere dritte über das WEB-Interface. 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.

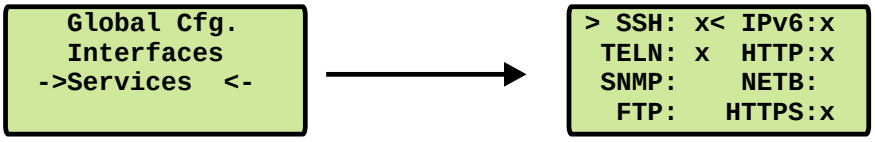
Ist das IPv6-Netzwerkprotokoll aktiviert, wird dem LANTIME automatisch immer eine Link-Local IPv6-Adresse in der Form „FE80::...“ zugewiesen, die die eigene Hardware-Adresse der Netzwerkkarte enthält. Befindet sich in dem IPv6 Netzwerk ein Router-Advertiser werden zusätzlich noch eine oder mehrere Link-Global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

12.5.5 Menü: Link Mode



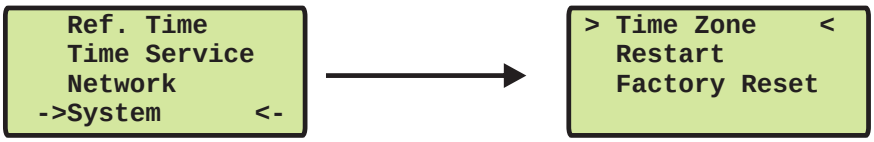
Über das Link Mode Untermenü können die Parameter für Geschwindigkeit und Duplex der ersten Netzwerkschnittstelle eingestellt werden. Es stehen 5 Modi zur Verfügung: Autosensing, 10 MBit/Halb-Duplex, 100 MBit/Halb-Duplex, 10MBit/Voll-Duplex, 100 MBit/Voll-Duplex. Standardmäßig werden die Schnittstellen auf Autosensing eingestellt.

12.5.6 Menü: Network Services



Im Menü werden die möglichen Dienste angezeigt, die der LANTIME zur Verfügung stellt: SSH, TELNET, SNMP, FTP, IPv6, HTTP, HTTPS und NETBIOS. Die einzelnen Dienste können über die Auf/Ab Tasten aktiviert oder deaktiviert werden. Die Navigation durch die Liste erfolgt mit Hilfe der Rechts/Links Tasten. Die Dienste werden direkt nach dem Abspeichern mit OK entsprechend gestartet oder beendet.

12.6 Menü: System



In diesem Untermenü werden System spezifische Parameter festgelegt.

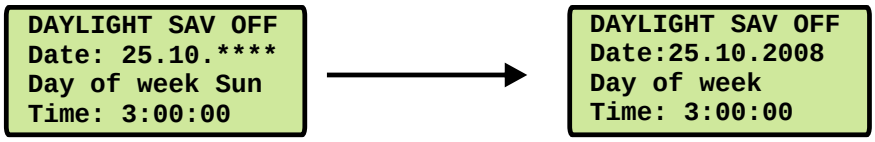
12.6.1 Menü: Set time zone

In diesem Menü wird die Zeitzone für die Anzeige im Display eingestellt. Diese Einstellungen wirken sich nicht auf die seriellen Schnittstellen und die Timecode Ausgänge aus. Die interne Zeit des Zeitservers und die NTP Zeit bezieht sich immer auf UTC und ist unabhängig von diesen Einstellungen der Zeitzone. Die Zeitzone für die seriellen Schnittstellen wird über ein anderes Menü eingestellt - **(Reference Time->Serial Outputs)**.

Im ersten Untermenü (Daylight Saving OFF) werden die Einstellungen für die normale Ortszeit (Winterzeit) vorgenommen. Im zweiten Untermenü (Daylight Saving ON) wird hingegen die Sommerzeit konfiguriert.

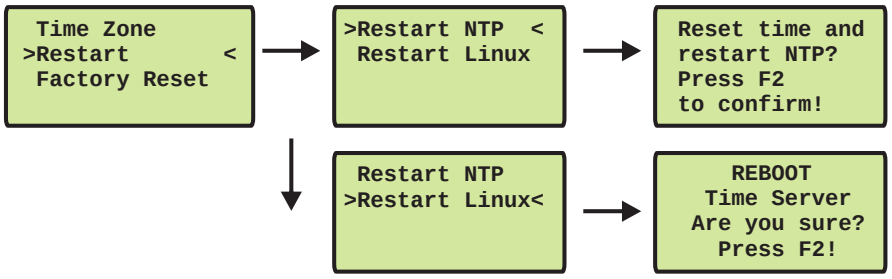
Nach der Auswahl einer von beiden Menüpunkten gelangt man hier zu den Einstellmöglichkeiten der Winter- bzw. Sommerzeit. Exemplarisch wird in der oben angegebenen Abbildung die Konfiguration der Winterzeit aufgezeigt.

In der ersten editierbaren Zeile werden Name und Abweichung für die normale Ortszeit angegeben (z.B.: MEZ = UTC + 1h).
Die beiden folgenden Zeilen dienen der Eingabe des Umschaltzeitpunktes, in dem die Winterzeit aktiviert wird. GPS bietet zwei Möglichkeiten zur Eingabe von Sommer-/Winterzeit: Entweder werden Datum und Uhrzeit der Umschaltpunkte für ein Jahr exakt definiert oder es werden Randbedingungen gesetzt, mit deren Hilfe das Gerät automatisch für mehrere Jahre den Tag der Umschaltung bestimmen kann. Die Abbildungen unten zeigen beide Varianten: Wird die Jahreszahl als ´*´ angezeigt, muss ein Wochentag eingegeben werden; dann ist der Tag der Umschaltung der erste Tag ab dem eingegebenen Datum, der mit dem eingegebenen Wochentag übereinstimmt. In der Abbildung unten ist z.B. der 25.10. im Jahr 2008 ein Samstag, am darauf folgenden Sonntag, den 26.10., zur angegebenen Uhrzeit, findet die Umschaltung auf Winterzeit statt. Wird eine bestimmte Jahreszahl eingegeben, ist der Tag der Umschaltung genau festgelegt und der Wochentag wird als ´*´ angezeigt.



Für den Fall, dass keine Sommerzeitumstellung benötigt wird, sind unter beiden Menüpunkten (DAYlight SAVING ON / OFF) beliebige aber exakt gleiche Daten, Zeiten und Offsets zu setzen.

12.6.2 Menü: Restart



Restart NTP
Wenn zu Testzwecken die Uhrzeit der internen Uhr verstellt wurde, muss die Uhrzeit des Systems ebenfalls gesetzt werden. Der NTP beendet sich, wenn die Zeitabweichung zwischen der Referenzuhr (GPS170) und der Systemzeit mehr als 1000 Sekunden abweicht. Mit diesem Menüpunkt wird die Systemzeit einmalig mit der Referenzuhr gesetzt und der NTP neu gestartet.

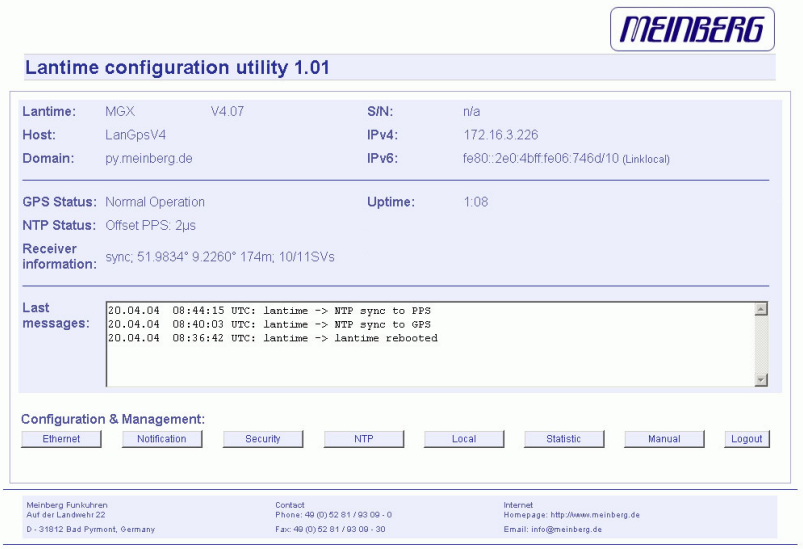
Restart Linux
Über den Punkt **Restart Linux** wird das Betriebssystem neu gestartet – die eingebaute Referenz Uhr wird nicht neu gestartet.

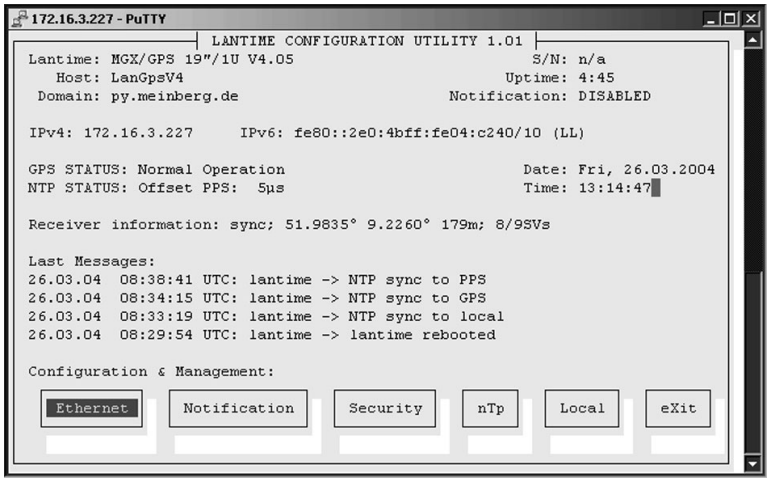
12.6.3 Menü Factory Reset

Wird der Menüpunkt **Reset to Factory Defaults** aufgerufen und bestätigt, werden alle Netzwerk Parameter und Systemparameter auf die Werkseinstellung zurückgesetzt.

13 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.





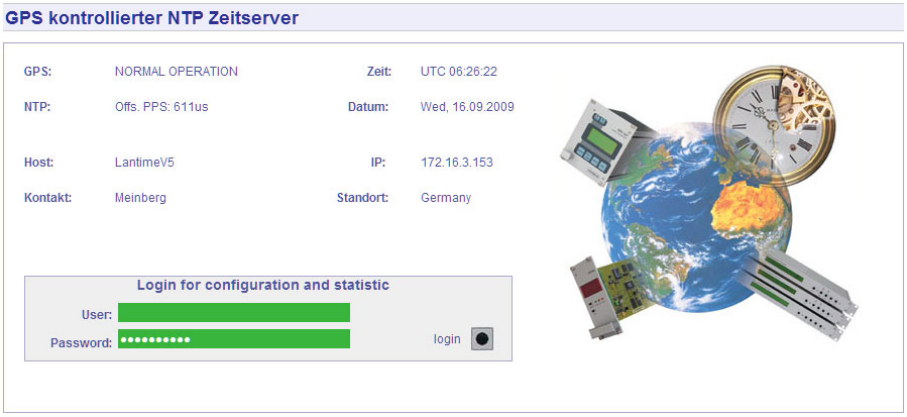
Zum anderen kann über eine TELNET oder SSH Verbindung ein Comand-Line-Interface (CLI) geöffnet werden, wo mit Hilfe des Programms „setup“ eine textbasierte Benutzerschnittstelle gestartet wird. Bis auf wenige Ausnahmen sind das WEB-Interface und das CLI von den Möglichkeiten zur Konfiguration identisch (das CLI hat keine Statistikfunktion).

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.

14 Das HTTP Interface

Um eine HTTP Verbindung zu dem LANTIME aufzubauen, geben Sie die IP Adresse Ihres LANTIME in das Adressfeld des Webbrowsers ein:

Es erscheint bei HTTP und HTTPS das gleiche Interface:



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 Empfängers 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 dem Empfänger (für ca. 5 min nach dem Einschalten) erscheint „NTP: not sync“. Dieser Status wird auch angegeben, wenn der Empfänger nicht synchron ist und der NTPD dann auf seine „LOCAL-CLOCK“ zurückgeschaltet hat.

Der verwendete Empfänger wird zum einen über die serielle Schnittstelle und zum anderen über den Sekundenimpuls an den NTP angebunden. Es sind also 2 Referenzen in der Konfiguration des NTP eingetragen: einmal der Empfänger und zum anderen der PPS (Pulse Per Second). Dieses ist entsprechend im Status des NTP sichtbar - es wird entweder der Offset zur seriellen Anbindung zur Referenzzeitquelle oder zum Sekundenimpuls (PPS) angezeigt: „NTP: Offset GPS [PZF,WWV,MSF,TCR]: 2ms“ oder „NTP: Offset PPS: 1ms“. Im zweiten Abschnitt werden Informationen zu den Netzwerk Parametern wie Hostname, IP Adresse und die Angaben zum Kontakt und dem Standort des Gerätes. Weiter unten kann ein Benutzername 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 Benutzername und das Passwort eingegeben wird.

Login bei Erstinstallation:
Benutzer: *root*
Passwort: *timeserver*

14.1 Konfiguration: Hauptmenü

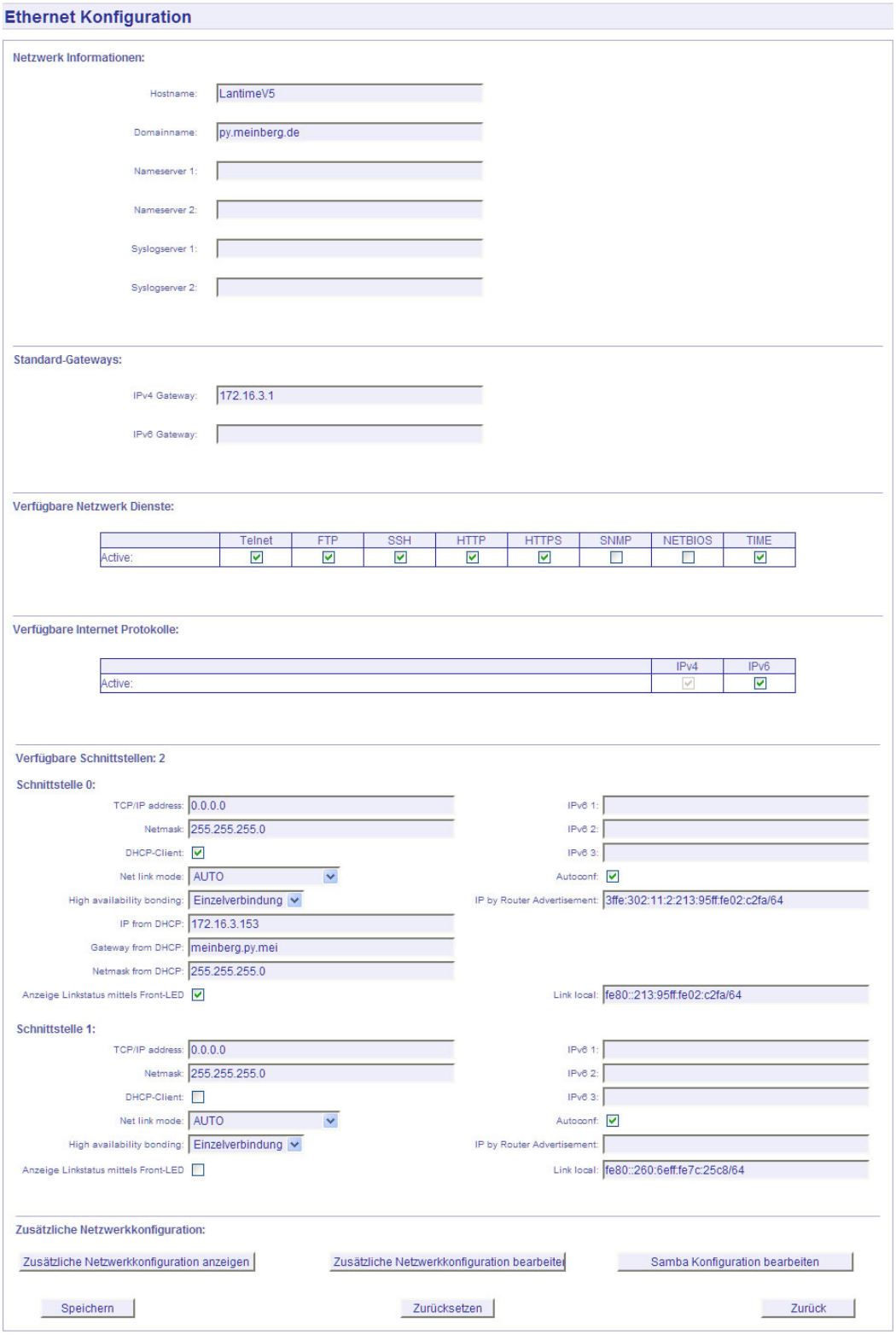
Nachdem das Passwort erfolgreich eingegeben wurde, gelangt man zur Hauptseite des Konfigurations- und Verwaltungsprogramms. Diese Seite gibt einen kurzen Überblick über die wichtigsten Einstellungen und Laufzeitparameter des Gesamtsystems. Oben links steht die LANTIME Variante mit der Versionsnummer für die LANTIME Software, wobei es sich um einen übergeordneten Softwarestand aller enthaltenen Module und Software Pakete handelt. Darunter wird die Seriennummer, der Kontakt und der Standort angezeigt. Rechts wird der aktuelle Hostname, Domainname und die IPv4 sowie die IPv6 Adressen des ersten Ethernet Anschlusses geschrieben.

Im zweiten Abschnitt wird der Status der GPS und des NTP wie oben schon beschrieben angezeigt, sowie zusätzliche Informationen zum GPS Empfänger mit Position und Anzahl der sichtbaren und guten Satelliten. 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.

14.2 Konfiguration: Ethernet



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.

14.2.1 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.

14.3 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 Checkboxen 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 DHCPC 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.

14.3.1 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 Netzwerk-einstellungen 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.

14.3.2 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

127.0.0.1bei 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.

14.3.3 High availability bonding

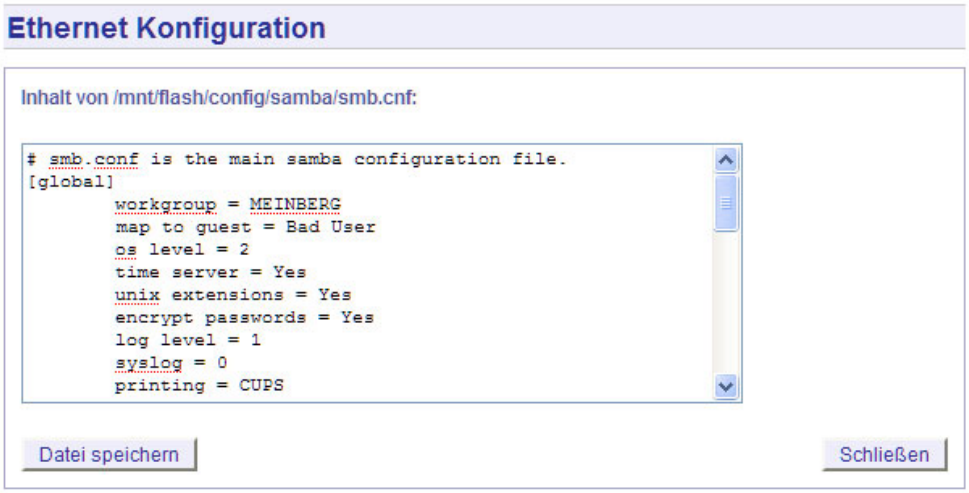
Nach IEEE802.3 ist es möglich, eine logische Netzwerkverbindung auf mehrere physikalische Verbindungen zu verschiedenen Switches aufzuteilen. Nur eine physikalische Verbindung wird zur gleichen Zeit verwendet. Offiziell als Bonding for High Availability bezeichnet, bieten es mehrere Hersteller unter 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. Bei dem hier implementierten Bonding wird nicht die MAC Adresse der Netzwerkschnittstellen, sondern nur die IP Adresse abhängig von dem Link-Status auf den nächsten möglichen ETH-Port umgeschaltet. Dabei werden alle Dienste neu gestartet.

14.3.4 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.

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



14.4 Konfiguration: Notification

14.4.1 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 unter anderem Aktionen EMAIL, SNMP-TRAP, WINDOWS POPUP MESSAGE, die Anzeige der Nachricht über das Großdisplay VP100/NET, das benutzerdefinierte Script und das integrierte Relais (siehe Anhang) zur Verfügung. Jede Bedingung kann mit jeder Aktion beliebig verknüpft werden.

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

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

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.

14.4.2 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. Über den Button CC-Empfänger können zusätzliche EMAIL Adressen eingestellt werden, zu denen diese Nachricht gesendet werden soll. Die EMAIL 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

14.4.3 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 Netwerke“ 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:

14.4.4 Alarm SNMP-TRAP

In den Einstellungen für die SNMP TRAPs als Benachrichtigung und Alarmmeldung können vier 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.

14.4.5 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).

14.4.6 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/config/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.

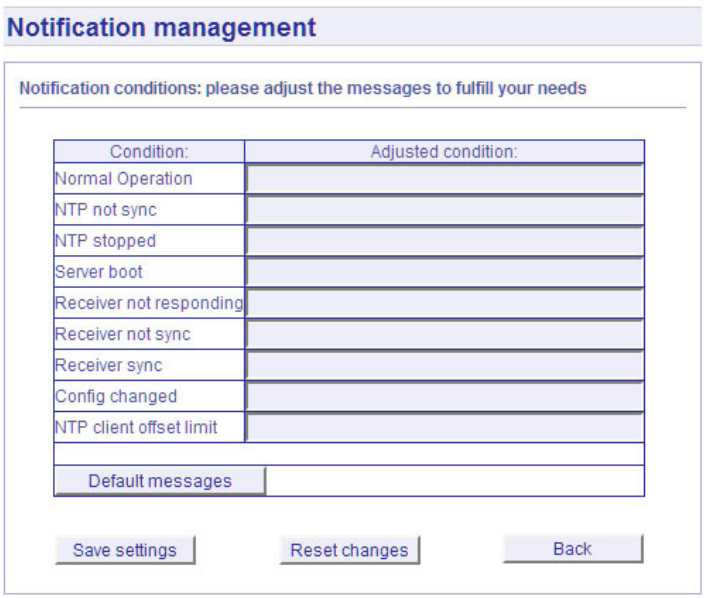
14.4.7 NTP Client Überwachung

Mit Hilfe der NTP Client Überwachung kann eine Gruppe von externen NTP Clients überwacht werden. Über den Schalter „Client Liste bearbeiten“ können alle NTP Clients, die überwacht werden sollen, zeilenweise als TCP/IP Adresse oder Hostname eingetragen werden.

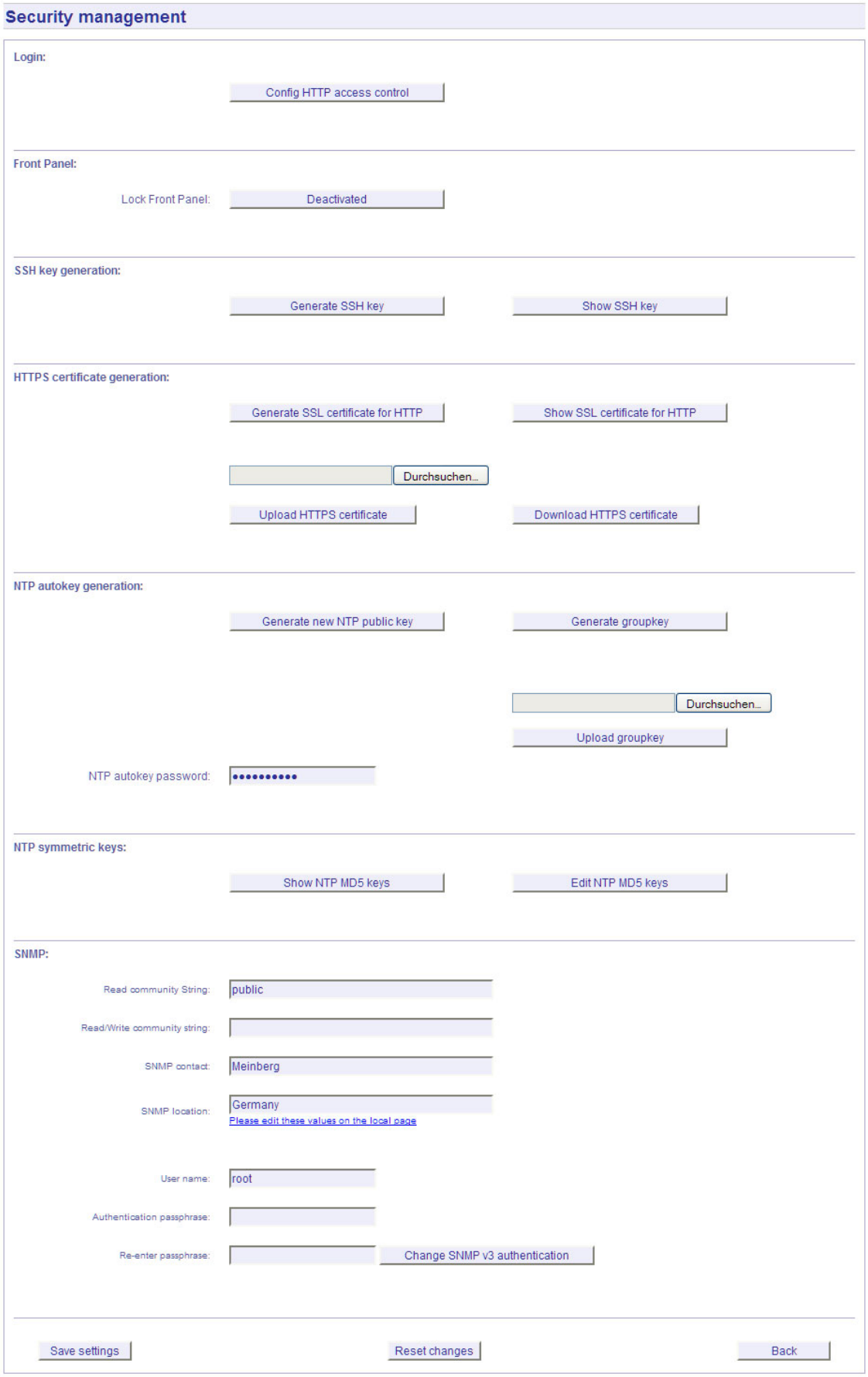
Drei Kriterien liegen der Client Überwachung zu Grunde: Zeit der Abweichung des NTP Clients zum Zeitserver, der Stratum des Clients und die Erreichbarkeit. Trifft eines dieser Bedingungen zu, wird die entsprechend konfigurierte Aktion ausgeführt. Über den Button „Client Status anzeigen“ wird der Status von allen NTP Clients in der Liste angezeigt:

14.4.8 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.



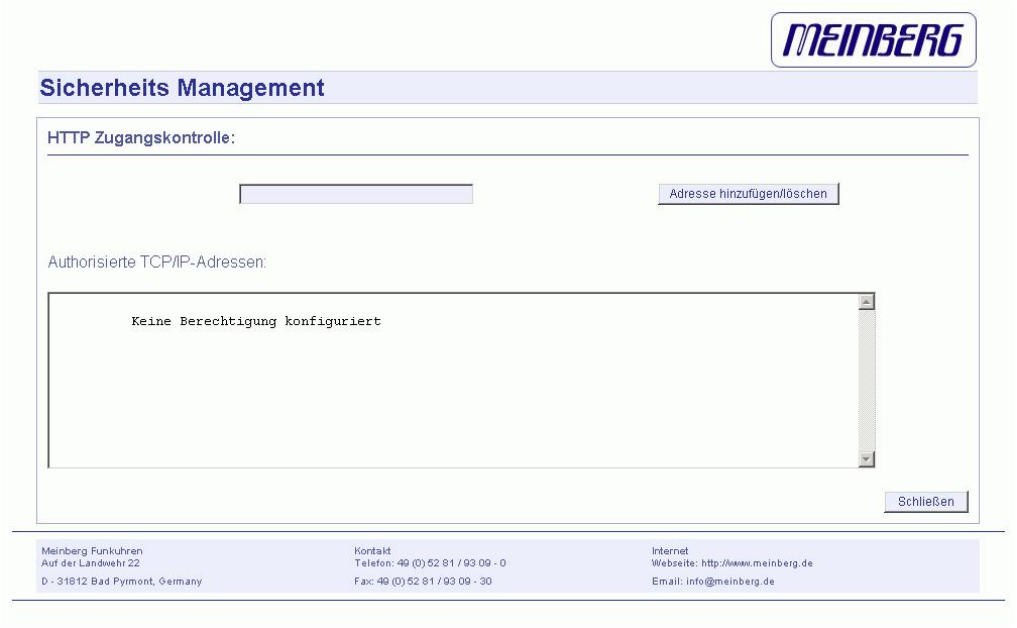
14.5 Konfiguration: Sicherheit



14.5.1 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).

14.5.2 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:

14.5.3 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:

ssh root @ 192.168.16.111

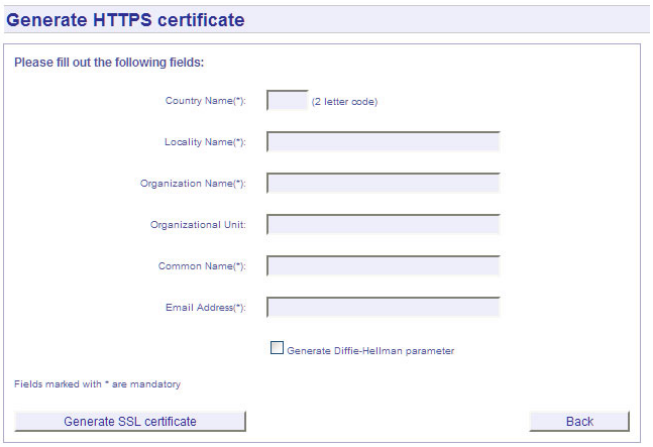
Beim ersten Zugriff muss das neue Zertifikat bestätigt werden und dann wird man nach dem Passwort **timeserver** gefragt.

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.

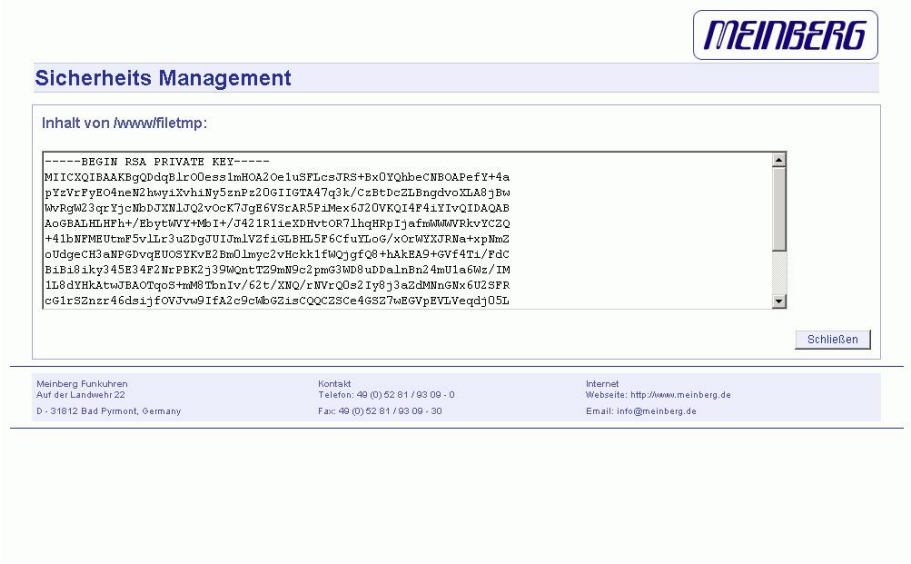
14.5.4 SSL Zertifikat für HTTPS erstellen

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.



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



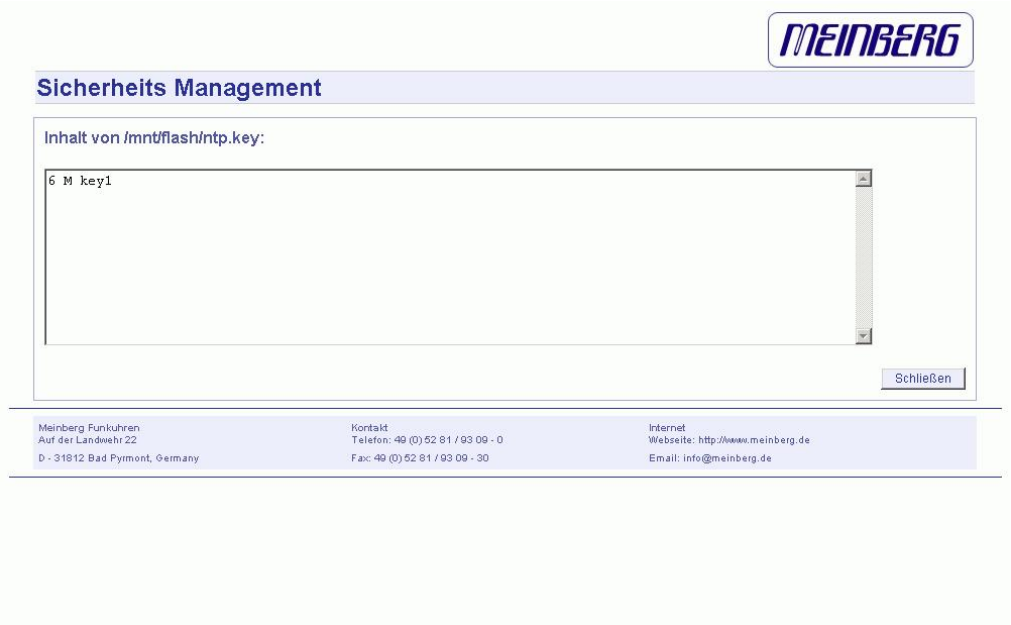
Zusätzlich kann ein eigenes Zertifikat mittels des Buttons „HTTPS-Zertifikat importieren“ eingespielt werden.

14.5.5 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.

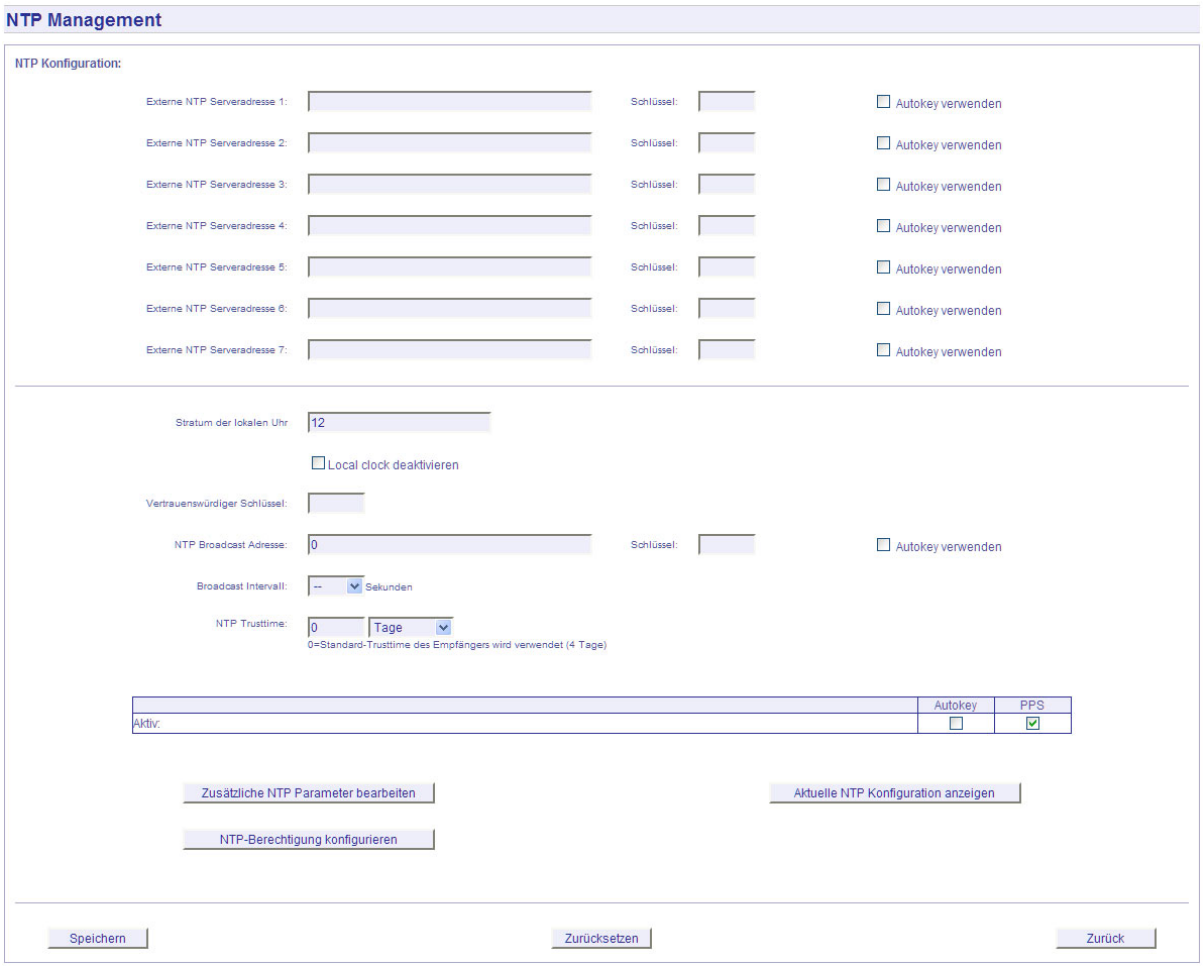
Über die beiden Punkte „NTP MD5 Schlüssel anzeigen“ und „NTP MD5 Schlüssel erzeugen“ können die symmetrischen NTP Keys verwaltet werden. Bitte lesen Sie hierzu auch das Kapitel über die symmetrischen Keys.



14.5.6 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.

14.6 Konfiguration: NTP



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 GPS 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  # GPS 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
```

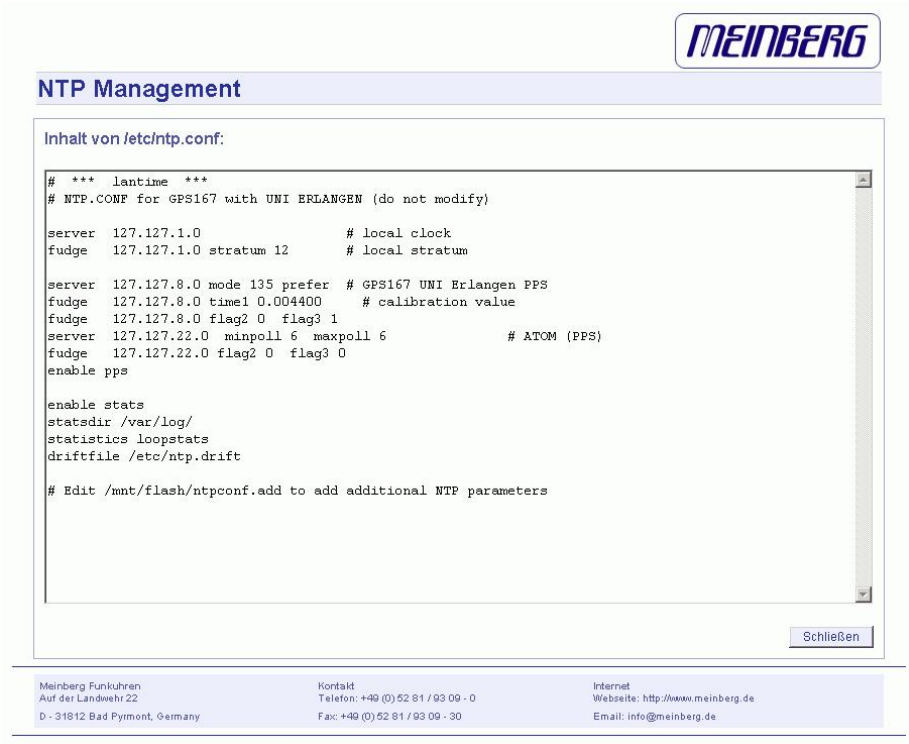
Die NTP Trusttime gibt die Zeit an, wie lange der NTP die GPS Referenzzeit noch akzeptiert, wenn diese in den Freilauf Zustand (nicht mehr synchron) wechselt. Die Freilauf-Genauigkeit der Referenzuhr hängt direkt mit dem eingebauten Quarz zusammen. Standardmäßig ist ein TCXO Quarz im LANTIME GPS eingebaut. 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

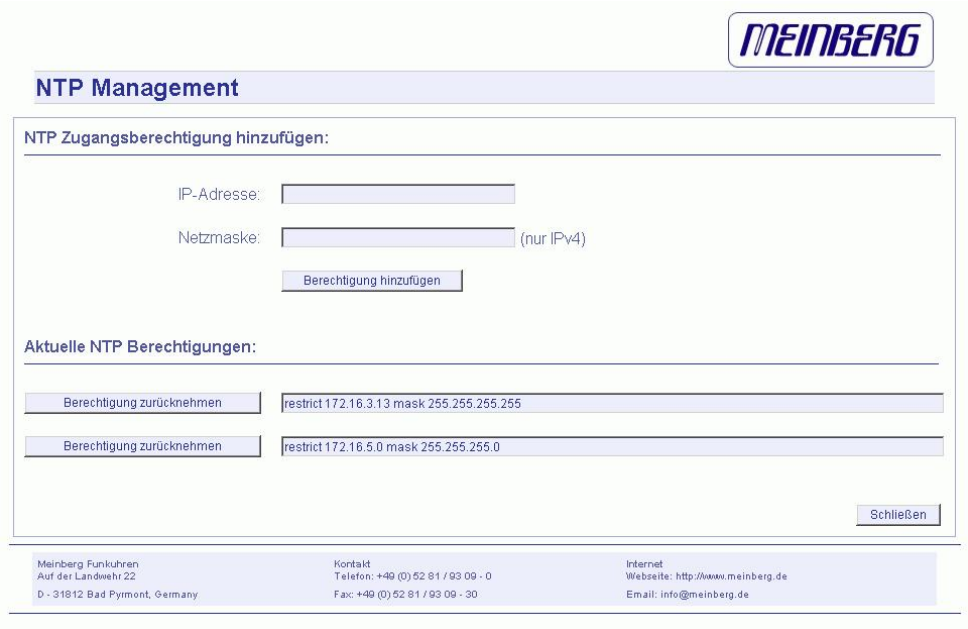
Im nächsten Punkt können die beiden Optionen AUTOKEY und PPS für den Zeitserver aktiviert werden, wobei PPS sich auf die zusätzliche Referenzuhr über den Sekundenimpuls bezieht.

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.

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.



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 ausgebelendet, d.h. nur die Benutzer aus dieser Liste haben NTP-Zugriff (dürfen die Zeit anfragen) auf den Zeitserver.



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.

14.6.1 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 unauthentisierte Pakete, authentisierte Pakete die nicht entschlüsselt werden können oder authentisierte 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 authentisierte 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** gekennzeichneter Key ist wiederum als Hex Ziffer geschrieben, jedoch im NTP Standard Format mit dem höchswertigen Bit (HSB) jedes Octets als das ungerade Parity Bit.
- Ein mit **M** gekennzeichneter 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.

14.6.2 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 Zertifkat 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:

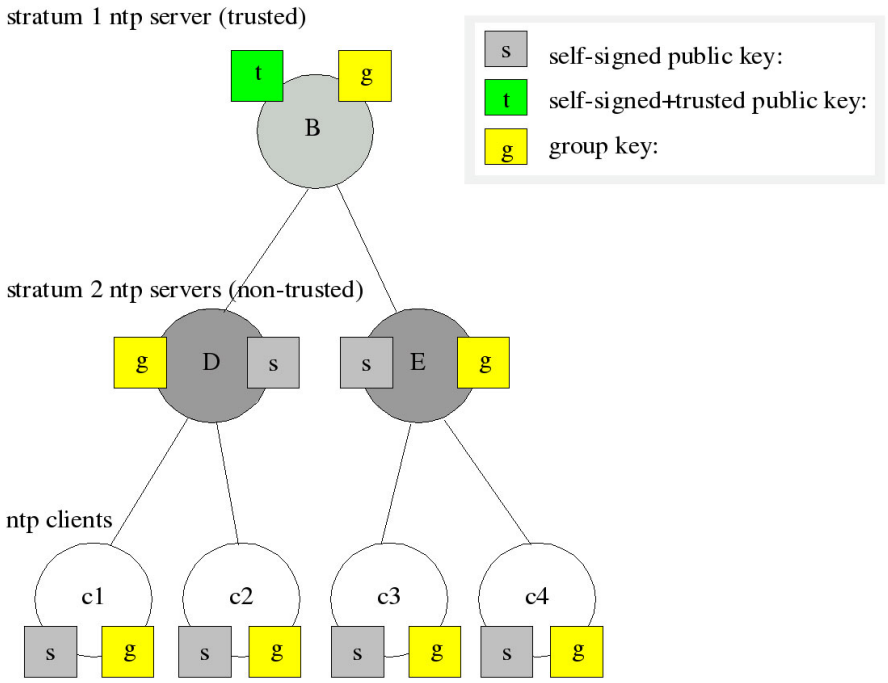
```
cp /etc/ntp/ntpkey_*  /mnt/flash/config/ntp/uploaded_groupkeys
```

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.

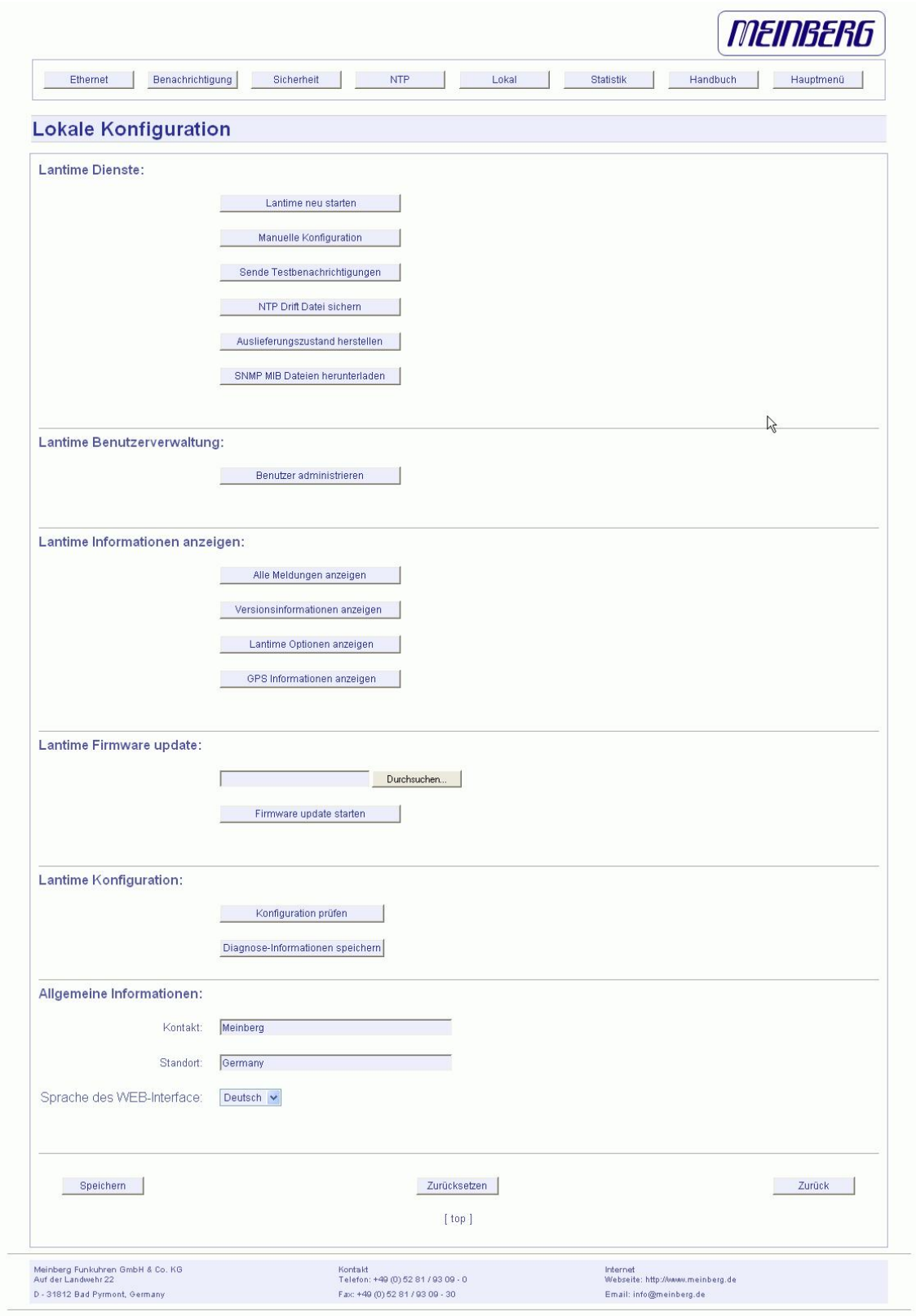


D und E sind NTP Server, die als Hosts der Gruppe nicht Trusted sind. Sie besitzen den Gruppenschlüssel und ein selbstsigniertes Zertifikat (das nicht als „Trusted“ markiert wurde). Die Clients besitzen jeweils den Gruppenschlüssel und ebenfalls ein selbstsigniertes Zertifikat.

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.

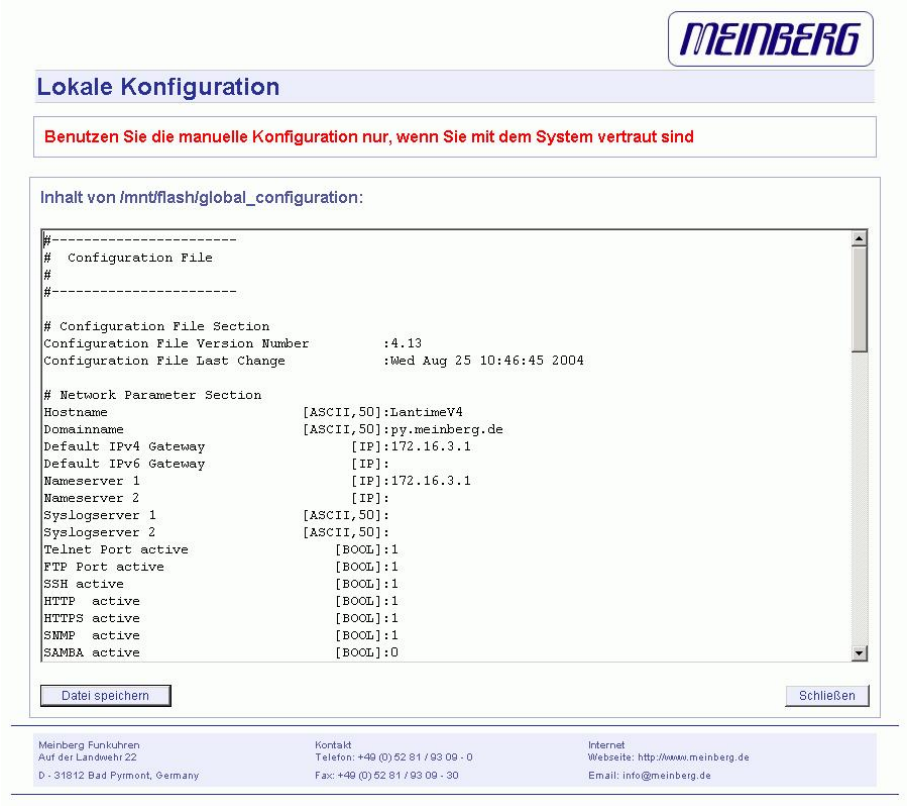
14.7 Konfiguration: Lokal



14.7.1 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.

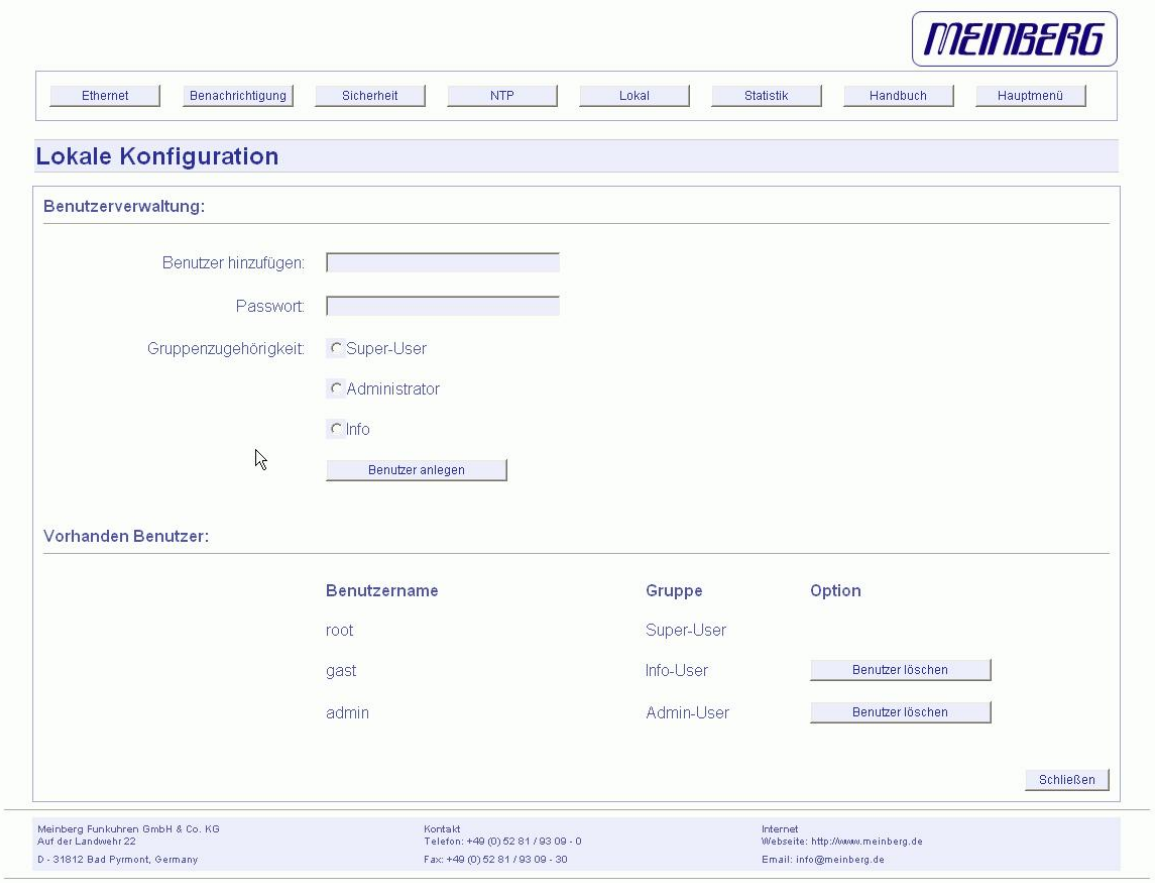
Über den Punkt „Auslieferungszustand herstellen“ werden alle Einstellungen auf den Auslieferungszustand zurückgesetzt. Dabei wir die alte Konfiguration unter /mnt/flash/global_configuration.old gespeichert und dann durch die Datei /mnt/flash/factory.conf ersetzt. Dabei wird auch das Standard Passwort „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.

14.7.2 Benutzerverwaltung

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 Adminitrator 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.



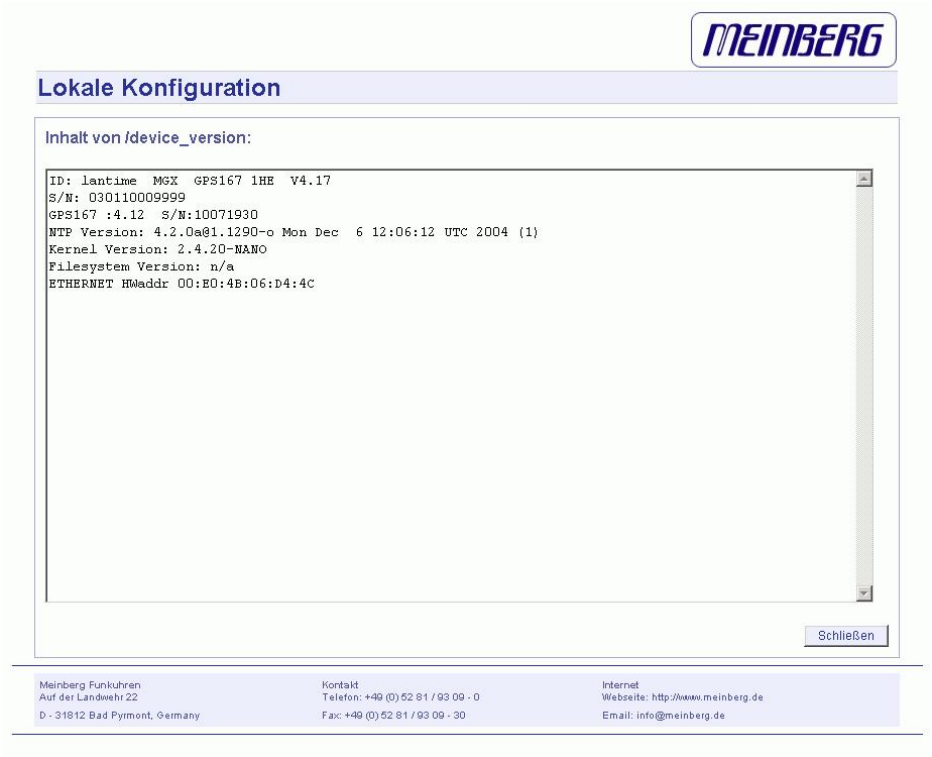
Über die Benutzerverwaltung können neue Benutzer jeweils mit Passwort und Gruppenzugehörigkeit angelegt und gelöscht werden. Zum Ändern eines Benutzers muß dieser erst gelöscht und dann neu angelegt werden. Im unteren Teil der Benutzerverwaltung wird eine Liste aller Benutzer angezeigt. Der Benutzer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

14.7.3 Administrative Informationen

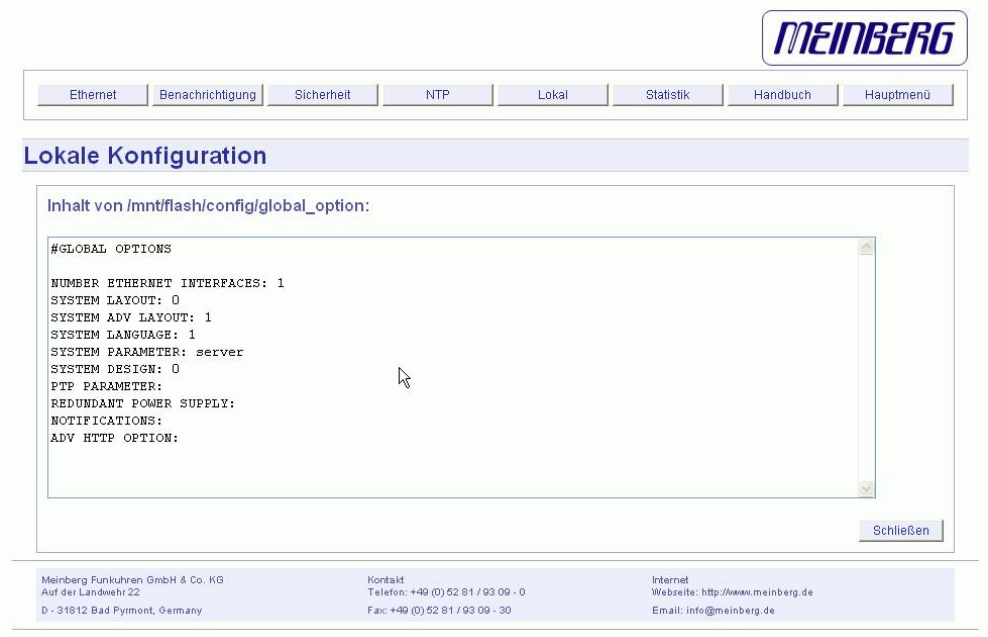
Über den Punkt „Alle Meldungen anzeigen“ wird die aktuelle SYSLOG Datei angezeigt. In dieser Datei werden von allen Programmen, wie auch von dem aktuellen Betriebssystem Kernel, die Meldungen abgelegt. In einem extra Fenster wird die gesamte Datei /var/log/messages angezeigt. Diese Datei steht in der 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 'ttyp1'from '172.16.3.45'
Mar 15 14:01:17 LanGpsV4 login[15711]:    root login on 'ttyp1'from '172.16.3.45'
```

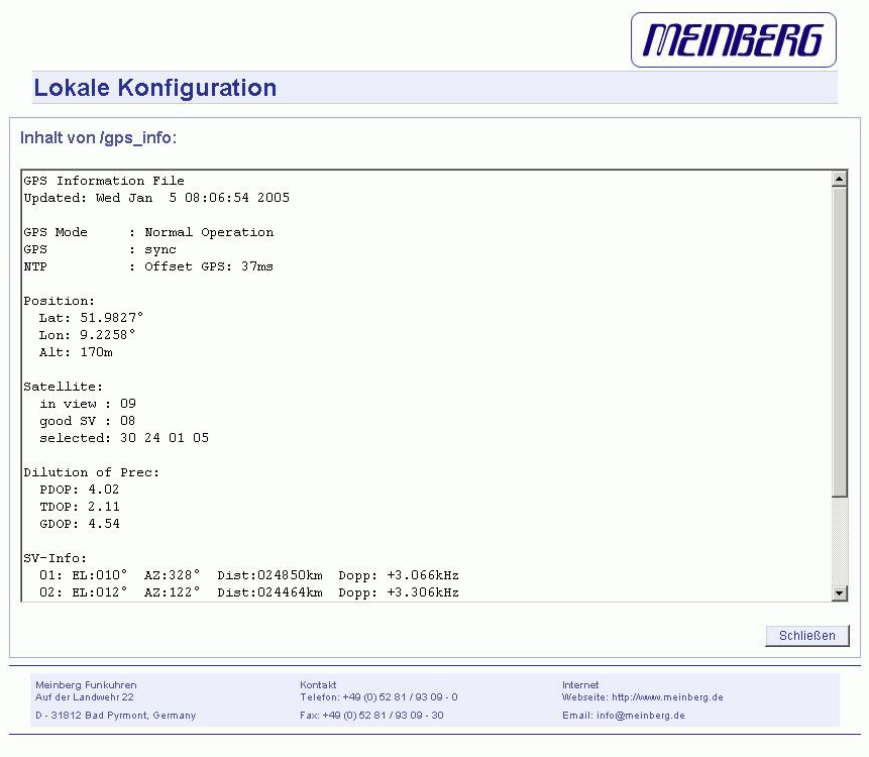
Der Punkt „Versionsinformationen anzeigen“ zeigt die aktuelle Version des LANTIME und der Softwarekomponenten an.



Der Punkt „LANTIME Optionen anzeigen“ zeigt die Optionen der integrierten Komponenten an. Diese Optionen werden vom Hersteller für zusätzliche Hardware Optionen eingerichtet und sollte nicht verändert werden.



Der Punkt „GPS Informationen anzeigen“ zeigt GPS spezifische Parameter. Der erste Parameter gibt Auskunft über den Zeitpunkt des letzten Updates der hier gezeigten Informationen. Der nächste Parameter gibt die Empfängerposition im Format Latitude, Longitude und Altitude an. Latitude und Longitude werden in Grad, Minuten und Sekunden dargestellt, Altitude in Metern (über WGS84 Ellipsoid). Unter Satellite wird die Anzahl der Satelliten, die sich „in Sicht“ (in view) befinden sowie der brauchbaren (good SV) angezeigt. Außerdem wird der gerade genutzte Satz (selected set) von vier Satelliten angezeigt.



Die Genauigkeit der berechneten Empfängerposition und Zeitabweichung ist abhängig von der Stellung der vier ausgewählten Satelliten zueinander. Aus den Satellitenpositionen und der Empfängerposition lassen sich Werte (Dilutions Of Precision; DOP) bestimmen, die eine Beurteilung der ausgewählten Konstellation zulassen. Diese Werte können in einem Untermenü angezeigt werden. PDOP ist die Abkürzung für Position Dilution Of Precision, TDOP für Time Dilution Of Precision und GDOP für General Dilution Of Precision. Niedrigere Zahlenwerte bedeuten hierbei höhere Genauigkeit.

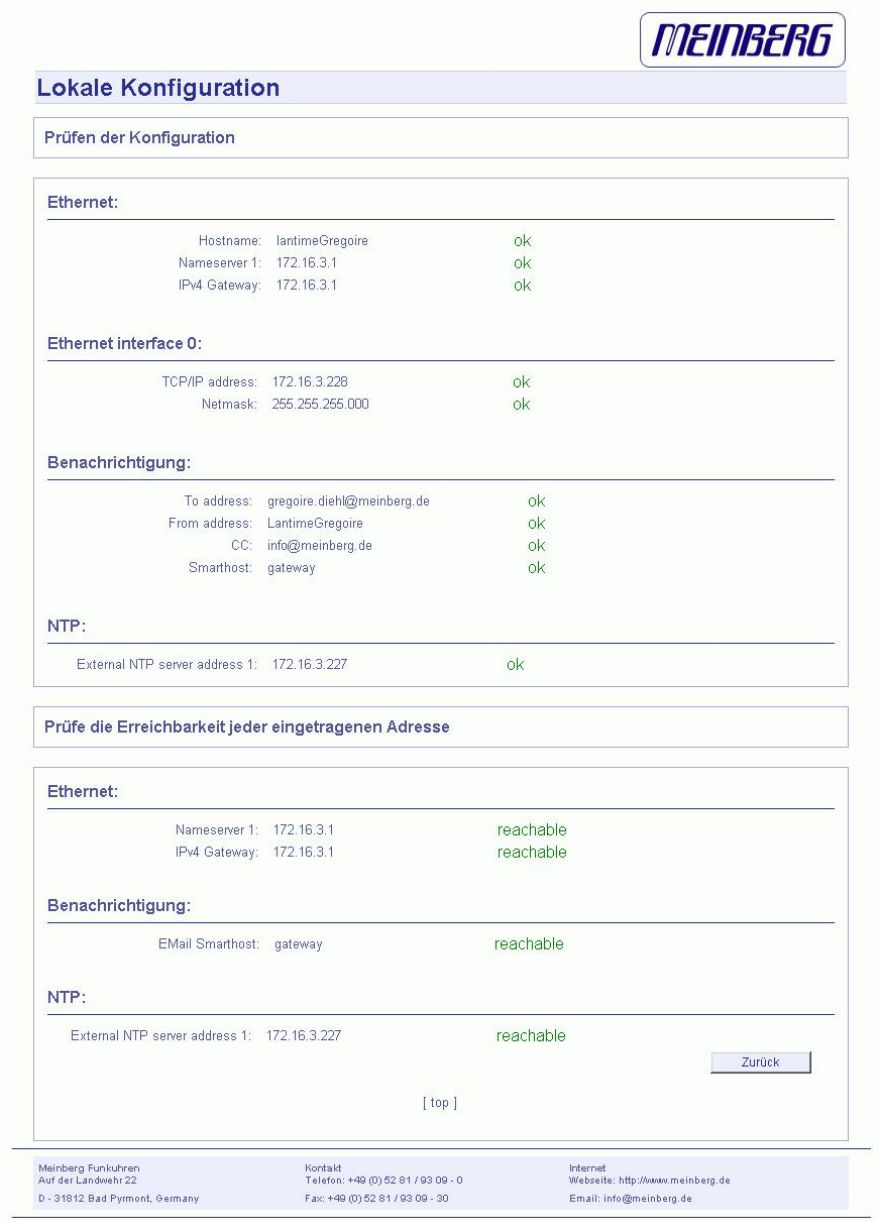
Die nächste Tabelle Satellite Info gibt Informationen über die gerade in Sicht befindlichen Satelliten: Die Satellitennummer, Elevation, Azimuth und die Entfernung zum Empfänger zeigen die Position des Satelliten am Himmel. Der Doppler zeigt, ob der Satellit vom Horizont her aufsteigt (positiver Wert) oder wieder verschwindet (negativer Wert).

14.7.4 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.

14.7.5 Automatische Konfigurationsprüfung

Über den Punkt „Konfiguration prüfen“ können alle aktuellen Einstellungen des Zeitservers 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.

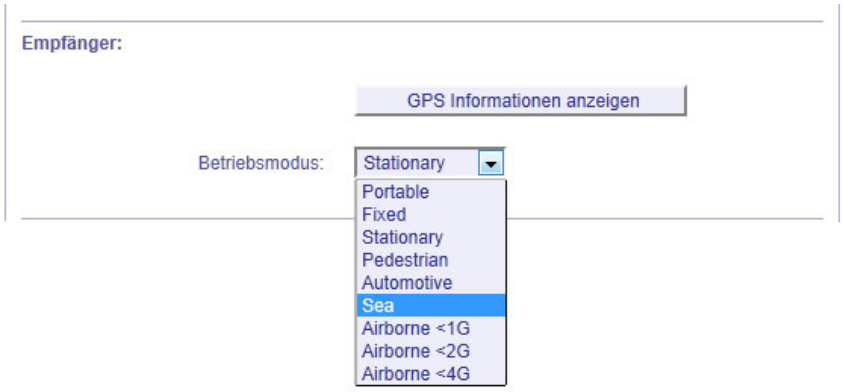


14.7.6 Diagnose Informationen speichern

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 zusmmengefasst 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.

14.7.7 Information des Empfängers

In diesem Menü werden alle wichtigen Informationen zur verwendeten Funkuhr bzw. zum verwendeten Empfänger angezeigt.

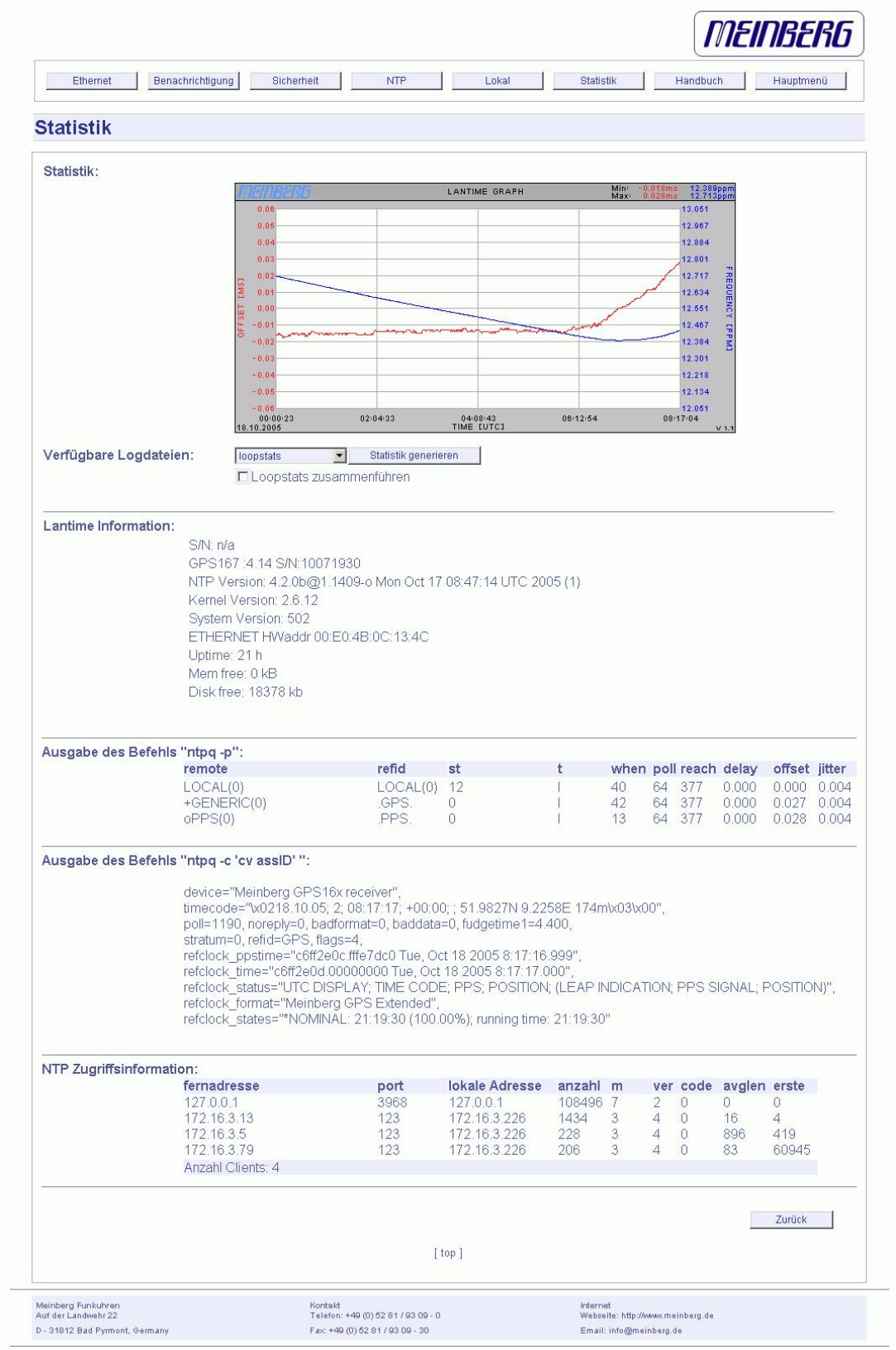


Das Beispiel zeigt das Menü bei einem GPS Empfänger mit MGR Modul. Über den Button „GPS Informationen anzeigen“ wird ein Textfeld mit allen relevanten Informationen des Empfängers geöffnet. Bei dem LANTIME mit GPS Empfänger und MGR Modul kann noch der Betriebsmodus auf die entsprechende Umgebung eingestellt werden. Damit wird sichergestellt, dass der Empfänger in Abhängigkeit von der zur erwartenden Geschwindigkeit seine Position berechnet.

14.7.8 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.

14.8 Konfiguration: Statistik



14.8.1 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.

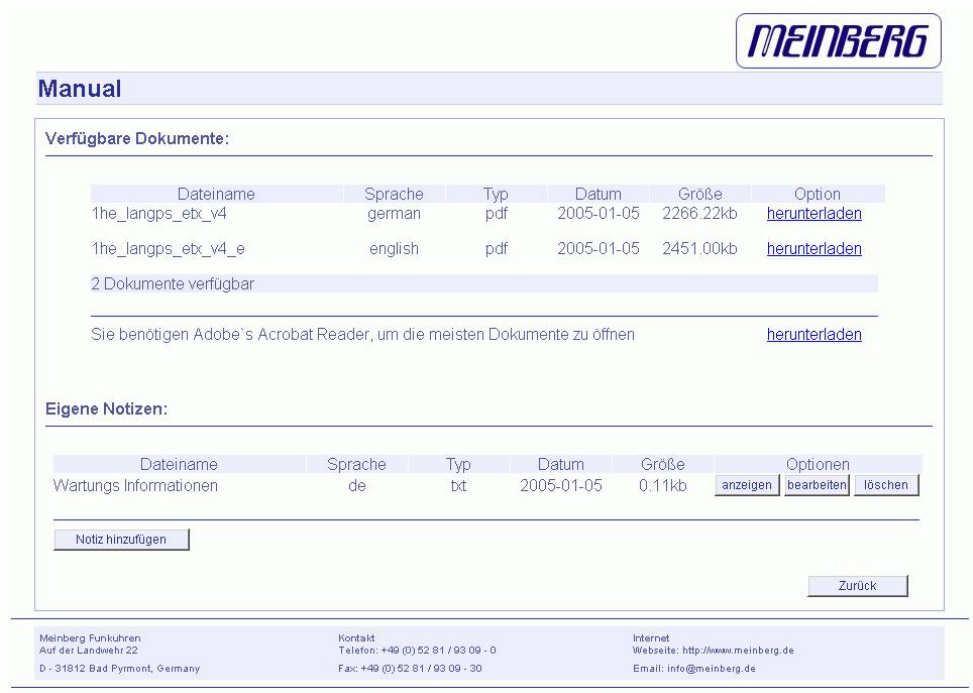
remote	refid	st	t	when	poll	reach	delay	offset	jitter
LOCAL(0)	LOCAL(0)	3	l	36	64	3	0.00	0.000	7885
lantime	.GPS.	0	l	36	64	1	0.00	60.1	15875

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)

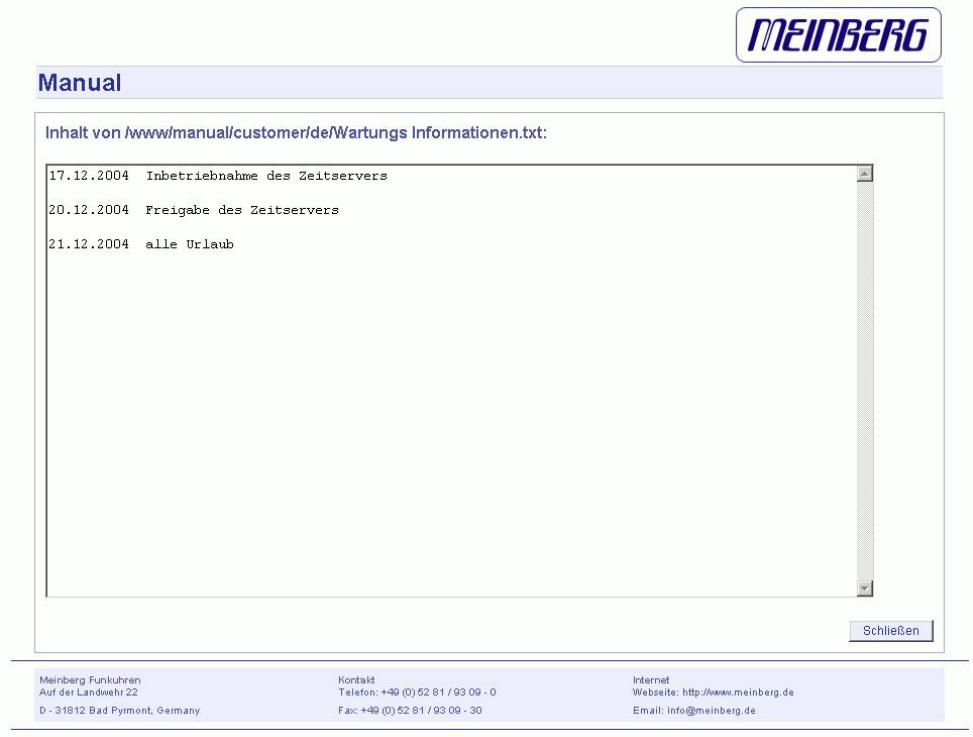
Im letzten Abschnitt werden NTP spezifische Informationen zur eingebauten Referenzuhr ausgegeben. Neben dem aktuellen und dem alten Status wird der Name der Referenzuhr und der letzte empfangene Zeitstring und die Laufzeiten aufgeschlüsselt nach dem Status „NOMINAL“ und „FAULT“.

14.9 Konfiguration: Handbuch



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.

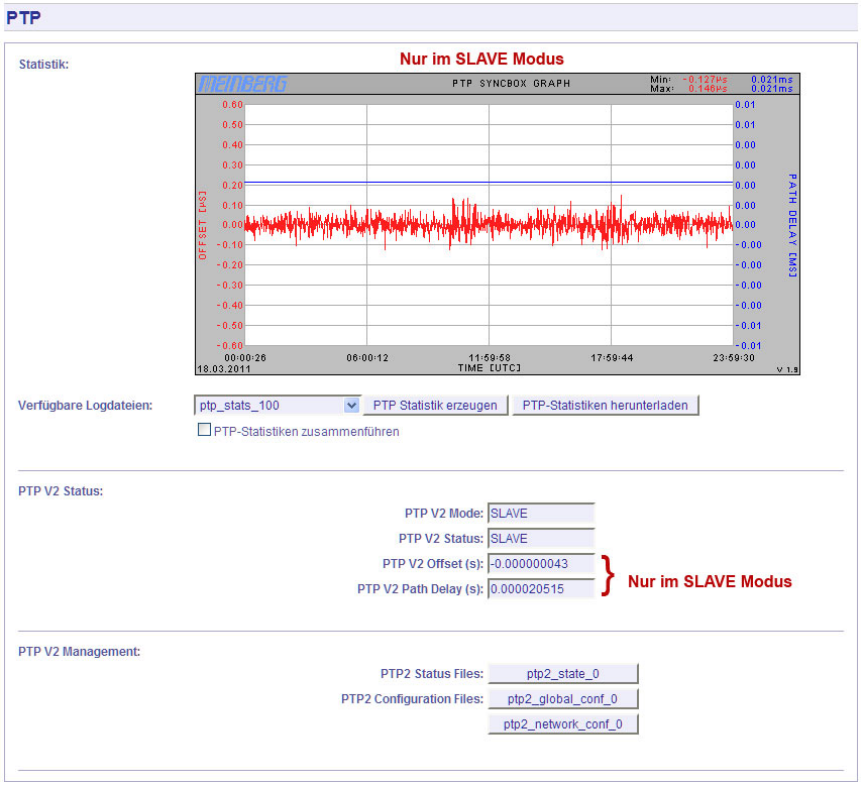
Im zweiten Teil werden die frei definierbaren Notizen angezeigt. Hier können vom Benutzer frei zugängliche Notizen und Anmerkungen abgelegt werden. Über den Punkt „Anzeigen“ wird die Datei in einem Fenster angezeigt. Über den Punkt „Bearbeiten“ wird die jeweilige Notiz bearbeitet und über „Löschen“ wird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



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.

14.10 Konfiguration: PTP

Im Menü PTP können die PTP Parameter des Gerätes editiert werden. Im SLAVE Modus wird zusätzlich eine grafische Darstellung des PTP Offsets und des PTP Pathdelays zum Grandmaster angezeigt:



- Über das PTP V2 Management Menü kann der aktuelle Status der PTP Einheit über die Statusdatei „ptp2_state_0“ abgefragt werden (siehe 14.10.4).

- Die PTP Konfiguration lässt sich über die Konfigurationsdatei „ptp2_global_conf_0“ editieren (siehe 14.10.1).

- Die IP-Konfiguration und die VLAN Parameter für die PTP-Netzwerkschnittstelle können in der Datei „ptp2_network_conf_0“ geändert werden (siehe 14.10.3).

- Wenn das Gesamtsystem mehr als eine PTP Karte enthält, kann für jede PTP Karte eine getrennte Konfiguration erstellt werden. Eine genaue Beschreibung der Parameter finden Sie im Kapitel 14.10.1 (Globale PTP Parameter).

14.10.1 PTPv2 - Globale Konfiguration

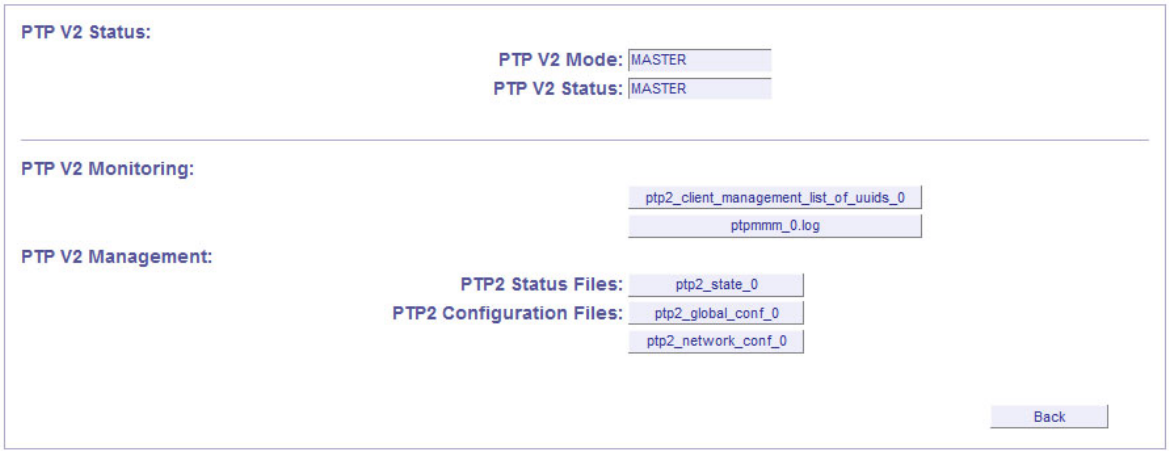
Inhalt der PTP Konfigurationsdatei (ptp2_global_conf_0):

Parameter	Wert/Einheit	Beschreibung
PTP Mode	[NUM]	0=Multicast (MC), 1=Unicast (UC)
PTP is slave	[BOOL]	1=Slave Betrieb, 0=Grandmaster Betrieb
PTP Delay Mechanism	[0,1]	0=End-to-End, 1=Peer-to-Peer
PTP V1 Hardware Compatibility	[0,1]	PTP Paketlänge wie beim V1 Standard (0: Default)
PTP Domain Number	[NUM,0:255]	Nummer einer logischen Gruppe (Domain) von PTP Geräten
PTP Network Protocol	[NUM,1,3]	1=UDP/IPv4 (Layer 3), 3=IEEE 802.3 (Layer 2)
PTP Timescale	[NUM,0:1]	0=ARB (arbitrary/benutzerdefiniert), 1=PTP (TAI,default)
PTP priority1	[NUM:0:255]	Priority1 für Best Master Clock Algorithmus
PTP priority2	[NUM:0:255]	Priority2 für Best Master Clock Algorithmus
PTP Sync Interval	[2^x]:0	verwendet bei Multicast Master bzw. Unicast Slave
PTP Announce Interval	[2^x]:1	verwendet bei Multicast Master bzw. Unicast Slave
PTP DelayRequest Interval	[2^x]:3	verwendet bei Multicast Master bzw. Unicast Slave
PTP Unicast interval duration [s]	[NUM]:60	Unicast: Dauer der Aussendung bis Erneuerung oder Timeout
PTP Unicast clockid of master	[ASCII,50]	Unicast: Master Clock ID (FF:FF:FF:FF:FF:FF:FF:FF default, oder zu verwendende GM ID)
PTP Unicast IP address of master	[IP]	Unicast: IP Adresse des PTP Grandmaster Ports (z.B. 172.29.9.236)
Feature Presets	[NUM]	1 = Power Profile, 2 = Telecom Profile
Power Profile Grandmaster ID	[NUM,3:254]:0	ID des Grandmasters, 3 - 254 (nur bei Power Profile)
Power Profile Network Inaccuracy	[NUM]:0	Akkumulierte Ungenauigkeit im Netzwerk in ns (nur bei Power Profile)
User defined Fix Offset positive	[BOOL]	1 = Positive Phasenverschiebung zur Referenzzeit
User defined Fix Offset [ns]	[NUM]	Wert der Phasenverschiebung zur Referenzzeit (0..1000000 ns)
HQ Filter active	[BOOL]:0	nur Slave: aktiviere Filter bei hoher Last oder Jitter
HQ Filter estimated accuracy [ns]	[NUM]:5000	HQ Filter: Erwartete Genauigkeit, max. Jitter im Netzwerk
PDSC active	[BOOL]:0	Path Delay Step Compensation (1=Erkennung aktiv) (siehe dazu auch Kapitel 8.4.11)
PTP Announce Receipt Timeout	[2^x]:3	nur bei Mulicast Master

14.10.2 Option: PTP Cient Überwachung

Ab Lantime Firmware Version 5.34m

Die PTP Client - Überwachung kann über das Front Panel (Time Service -> PTP IEEE1588 -> Setup PTP0 IEEE1588 V2 -> PTP Settings -> PTP Parameters -> PTP Client Management - siehe auch Kapitel im Abschnitt Benutzerschnittstellen zur Konfiguration) und über das Web Interface konfiguriert werden. Im Front Panel können maximal sieben Nodes (PTP Clients) angezeigt werden (nur VF-Display). Für eine vollständige Übersicht sollte daher das Web Interface verwendet werden.



Mit dem Button ***ptpmmm_0.log*** können über 100 PTP Nodes angezeigt werden. Die Liste der PTP Nodes mit den aktuellen Status Informationen hat die Form:

```
# PTP Client Management: found 6 PTP nodes
#
#   UUID              State-Txt   -Val  Offset          Pathdelay       Alias
#-------------------------------------------------------------------------
    EC4670FFFE0024CC  SLAVE       9     -0.000000015    0.000010420     alias_0
    EC4670FFFE002435  MASTER      6      0.000000000    0.000000000
    0050C2FFFEB717EA  SLAVE       9      0.000000146    0.000020675     alias_2
    0050C2FFFED287DE  SLAVE       9      0.000000107    0.000020859     alias_3
    EC4670FFFE000801  PASSIVE     7      0.000000000    0.000000000
```

Um einen oder mehrere PTP Nodes zu überwachen, muss eine Liste von PTP Clients angelegt werden. Diese Liste kann über das WEB Interface auf der Seite PTP angezeigt und editiert werden:
ptp2_client_management_list_of_uuids_0

Jede Zeile entspricht einem zu überwachenden PTP Node. Die Form der Zeile ist entsprechend der Status - Information (siehe oben) aufgebaut. Somit ist es möglich die entsprechende Zeile mit dem zu überwachenden PTP Node aus den Status Informationen per „Copy & Paste“ in diese Liste zu kopieren.

```
#   UUID               State text  val   offset        pathdelay     Alias
    0050C2FFFED287DE   Slave       9     0.000000500   0.000025000   alias_name
```

Der erste Wert ist die sogenannte PTP UUID, welche im Wesentlichen aus der MAC Adresse und einem festen mittleren Teil „FFFE“ besteht: **XX XX XX FF FE XX XX XX**

Die nächsten beiden Werte entsprechen dem PTP Status als Text und als Wert.
Folgende Status Werte sind möglich:

SLAVE	9
MASTER	6
PASSIV	7

Wenn der PTP Status gleich SLAVE ist, können zusätzlich der maximale Offset und das maximale Pathdelay zum PTP Master als Grenzen eingeben werden. Für jeden PTP Node werden die folgenden Bedingungen geprüft:

1. Erreichbarkeit
2. PTP Status
3. wenn PTP Status = SLAVE: Überschreiten der vorgegebenen absoluten Grenze des Offsets zum PTP Master
4. wenn PTP Status = SLAVE: Überschreiten der vorgegebenen absoluten Grenze des Pathdelays zum PTP Master
5. wenn PTP Status = SLAVE: Offset ändert sich innerhalb von 10 Minuten nicht

Alle Bedingungen werden über die eine Benachrichtigung „PTP State changed“ an die entsprechenden Notification Trigger weiter gegeben werden. Alle Benachrichtigungen werden nur einmal gesendet, solange der Zustand sich wie folgt nicht ändert:

1. Node ist wieder erreichbar
2. PTP Status ändert sich wieder
3. Offset geht wieder unter das vorgegebene Limit
4. Pathdelay geht wieder unter das vorgegebene Limit

Menü Benachrichtigung

14.10.3 PTP Netzwerk Konfiguration

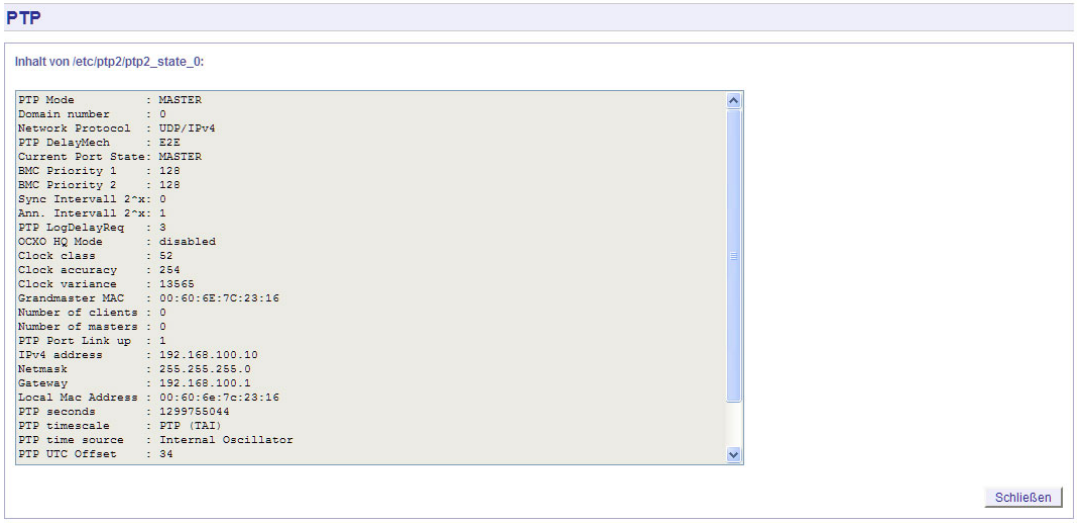
Alle Netzwerkeinstellungen der gewählten PTP Schnittstelle können über diesen Menüpunkt vorgenommen werden:

Inhalt der PTP Netzwerk - Konfigurationsdatei (ptp2_network_conf_0):

Parameter	Wert	Beschreibung
Hostname	[ASCII,50]:PTPv2	Hostname für den PTP Port
Domainname	[ASCII,50]:	Domainname für den PTP Port
Nameserver 1	[ASCII,50]:	
Nameserver 2	[ASCII,50]:	
TCPIP address	[IP]:192.168.100.10	IP Addresse des PTP Ports
NETMASK	[IP]:255.255.255.0	Netzmaske
Default Gateway	[IP]:192.168.100.1	Default Gateway
DHCP CLIENT	[BOOL]:0	1=DHCP client aktiv
VLan enabled	[BOOL]:0	1=Aktiviere Virtual LAN (IEEE 802.1Q)
VLan ID	[NUM]:	VLAN ID für das virtuelle Interface
VLan Priority	[NUM]:	VLAN Priorität für das virtuelle Interface
PTP IP TTL	[NUM]:	Multicast IP Paket Time-To-Live (TTL default:5)

14.10.4 PTP Status Datei

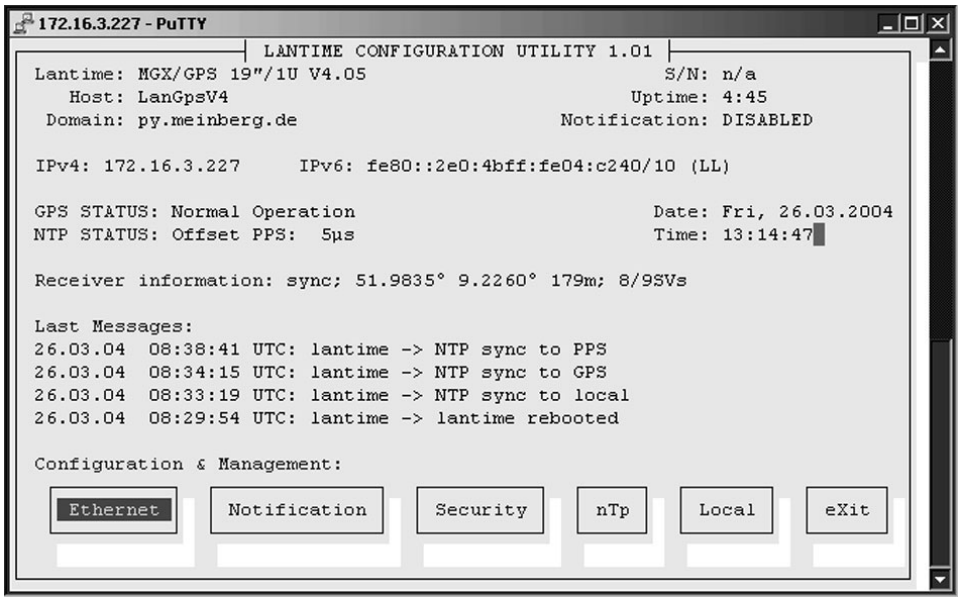
In diesem Menü werden alle Statusinformationen der gewählten TSU angezeigt:



PTP Mode	:	[MASTER,SLAVE]
Domain number	:	[0...3]
Network Protocol	:	[UDP IPv4 Layer3,IEEE 802.3 Layer 2]
PTP DelayMech	:	[E2E,P2P]
Current Port State	:	[INITIALIZING,LISTENING,UNCALIBRATED,MASTER, UnicastMASTER,SLAVE,UnicastSLAVE]
Clock class	:	[6=RefClock Sync,7=RefClock Holdover, 52=RefClock unsynchronized,255=Slave only]
Clock accuracy	:	33 (according to enumeration list in standard)
Clock variance	:	13565 [,65535=unknown]
Grandmaster MAC	:	00:60:6E:7C:27:2C
Number of clients	:	0 (not used yet)
Number of masters	:	0 (not used yet)
PTP Port Link up	:	1
IPv4 address	:	172.29.4.10
Netmask	:	255.255.255.0
Gateway	:	172.29.4.1
Local Mac Address	:	00:60:6E:7C:27:2C
PTP seconds	:	1299849447 [raw PTP seconds]
PTP timescale	:	PTP (TAI) [,ARB]
PTP time source	:	GPS [NTP,PTP,Internal Oszillator, unknown]
PTP UTC Offset	:	34
PTP Leapsecond	:	0 [Announcement active]
TSU Time	:	TAI:11.03.11 13:17:27.652680;
SYS Time	:	UTC:11.03.11 13:16:53.655558;

15 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.



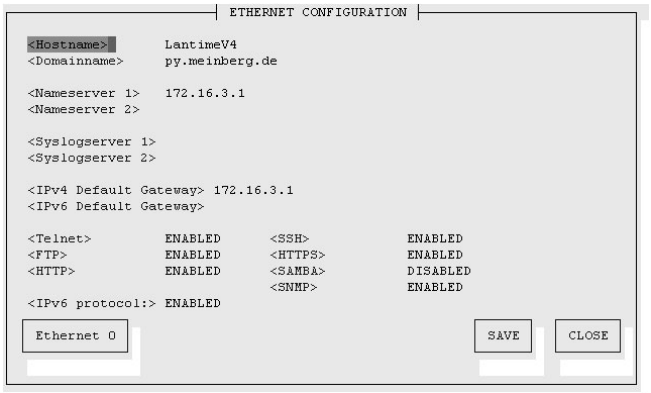
Diese Seite gibt einen kurzen Überblick über die wichtigsten Einstellungen und Laufzeitparameter des Gesamtsystems. Oben links ist die LANTIME Variante mit der Versionsnummer für die LANTIME Software, wobei es sich um einen übergeordneten Softwarestand aller enthaltenen Module und Software Pakete handelt. 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 GPS und des NTP wie oben schon beschrieben angezeigt, sowie zusätzliche Informationen zum GPS Empfänger mit Position und Anzahl der sichtbaren und guten Satelliten. 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.

15.1 CLI Ethernet



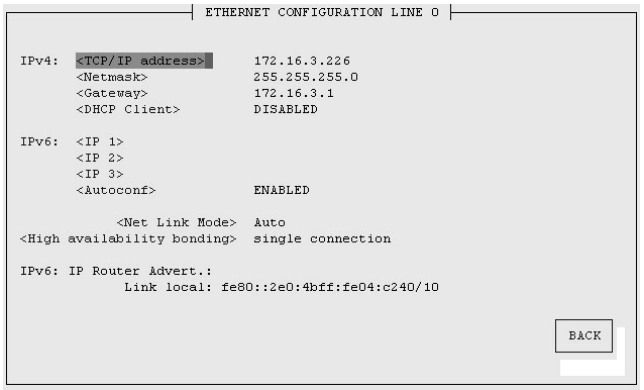
In der Netzwerk Konfiguration werden alle Parameter bezüglich der Netzwerkschnittstellen konfiguriert. Im ersten Abschnitt werden der Hostname, der Domainname, zwei Nameserver und zwei Syslogserver eingetragen. Bei den Nameservern und Syslogservern können wahlweise IPv4- oder IPv6-Adressen eingetragen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

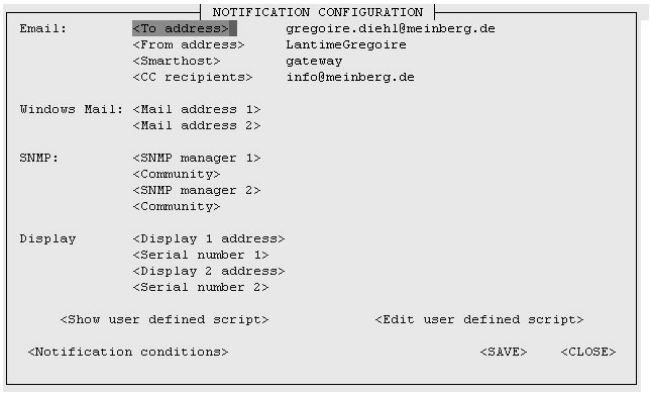
Beispiel:
„::“ ist die Adresse, die nur aus Nullen besteht.
„::1“ ist die Adresse, die aus Nullen und als letztem Bit einer 1 besteht.
Das ist die Host Local Adresse von IPv6, äquivalent 127.0.0.1 bei IPv4.
„fe80::0211:22FF:FE33:4455“ ist eine typische Link Local Adresse,
was man an dem Prefix „fe80“ 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. Bei dem hier implementierten Bonding wird nicht die MAC Adresse der Netzwerkschnittstellen, sondern nur die IP Adresse abhängig von dem Link-Status auf den nächsten möglichen ETH-Port umgeschaltet. Dabei werden alle Dienste neu gestartet.

15.2 CLI Notification



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.

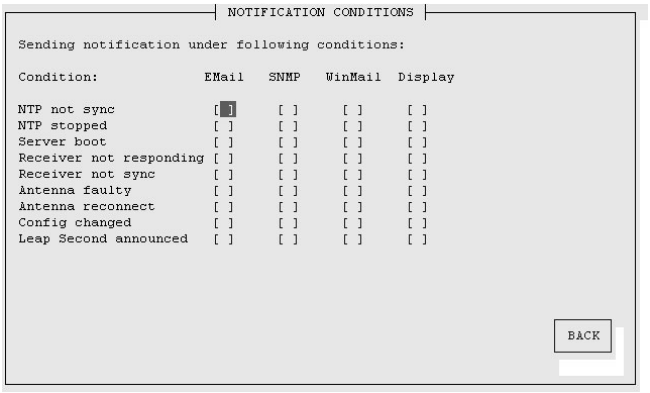
Bei diesem Zeitserver stehen die vier Aktionen EMAIL, SNMP-TRAP, WINDOWS POPUP MESSAGE und die Anzeige der Nachricht über das Großdisplay VP100/NET zur Verfügung. Jede Bedingung kann mit jeder Aktion beliebig verknüpft werden.

„Normal Operation“	NTP und Referenzuhr synchronisiert
„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 Funkuhr
„Receiver not sync“	GPS Empfänger nicht synchronisiert
„Antenna faulty“	GPS Antenne nicht angeschlossen
„Antenna reconnect“	GPS Antenne wieder angeschlossen
„Antenna short circuit“	GPS hat einen Kurzschluss auf der Antenne festgestellt
„Config changed“	Systemparameter vom Benutzer geändert
„Leap second announced“	Schaltsekunde angekündigt
"NTP Client Offset Limit"	Einer der NTP Clients hat das Limit überschritten

Für jedes Ereignis kann in dem letzten Abschnitt der „Notification Conditions“ eine beliebige „Trigger“ Aktion zugeordnet werden. Die entsprechenden Einstellungen für die 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. Zusätzliche Empfänger EMAIL Adressen können über den Button „CC recipients“ eingegeben 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 Netwerke“ 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.

VP100/NET Großanzeige

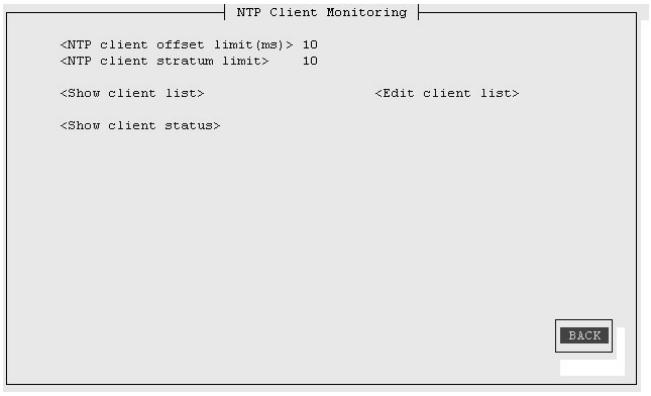
Die Großanzeige VP100/NET dient zur Anzeige von Uhrzeit und Datum. Diese Anzeige hat eine integrierte Netzwerkkarte und einen SNTP Client. Die Zeit wird von einem beliebigen NTP Zeitserver über das SNTP Protokoll abgeholt und damit die interne Uhr nachgeregelt. Diese Anzeige kann auch beliebige Texte 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).

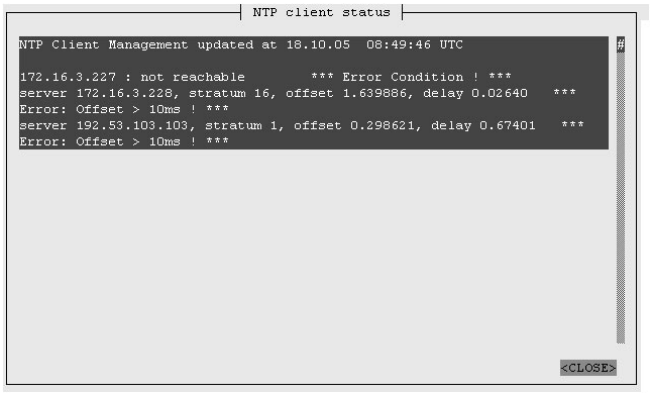
Über den Benachrichtigungspunkt „User“ kann ein frei definierbares Skript automatisch bei einer Bedingung ausgeführt werden. Über die Punkte „Show user defined script“ und „Edit user defined script“ kann dieses Skript angezeigt und bearbeitet werden. Das Skript ist auf der Flash unter „/mnt/flash/config/user_defined_notification“ zu finden. Dem Skript wird als Parameter der Index und der zugehörige Alarmtext übergeben. Der Index der Test-Bedingung ist dabei 0.

NTP Client Überwachung

Mit Hilfe der NTP Client Überwachung kann eine Gruppe von externen NTP Clients überwacht werden. Über den Schalter „Client Liste bearbeiten“ können alle NTP Clients, die überwacht werden sollen, zeilenweise als TCP/IP Adresse oder Hostname eingetragen werden.

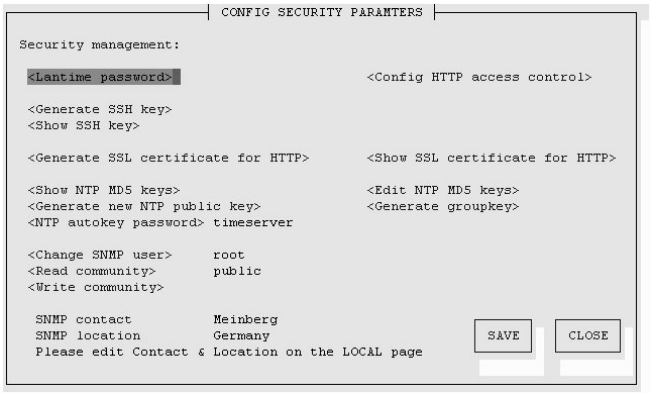


Drei Kriterien liegen der Client Überwachung zu Grunde: Zeit der Abweichung des NTP Clients zum Zeitserver, der Stratum des Clients und die Erreichbarkeit. Trifft eines dieser Bedingungen zu, wird die entsprechend konfigurierte Aktion ausgeführt. Über den Button „Client Status anzeigen“ wird der Status von allen NTP Clients in der Liste angezeigt:



15.3 CLI Security

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:

ssh root @ 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.

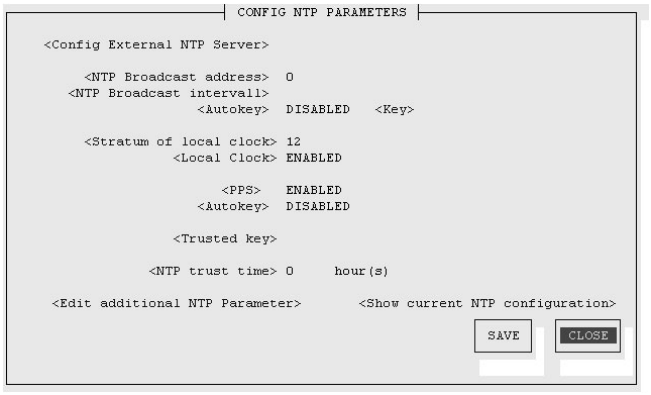
Nach der erfolgreichen Erzeugung des SSL Zertifikats wird das gesamte Ergebnis angezeigt.
Im dritten Abschnitt können die symmetrischen Schlüssel und die Autokey Zertifikate für den NTP angelegt und erzeugt werden.

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 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 „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.

15.4 CLI NTP Parameter



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/MRS:	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.

15.4.1 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 unglaubwürdig und für eine Synchronisation nicht geeignet gekennzeichnet, wenn sie entweder unauthentisierte Pakete, authentisierte Pakete die nicht entschlüsselt werden können oder authentisierte 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 authentisierte 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 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. Der Inhalt kann wie folgt aussehen:

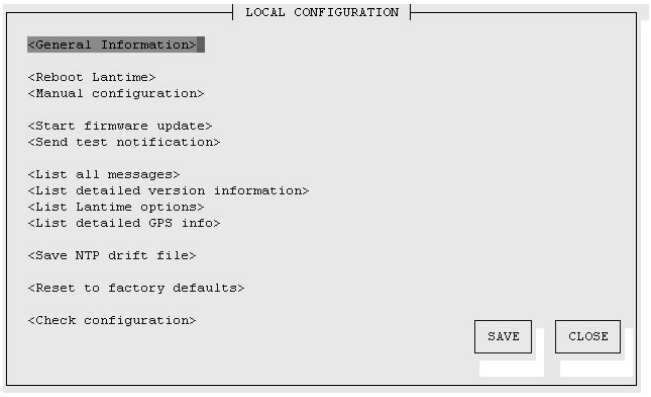
```
# ntp keys file (ntp.keys)
1       N 29233E0461ECD6AE      # des key in NTP format
2       M RIrop8KPPvQvYotM      # md5 key as an ASCII random string
14      M sundial               # md5 key as an ASCII string
15      A sundial               # des key as an ASCII string

# 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** gekennzeichneter 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** gekennzeichneter Key ist ein MD5 Key mit bis zu 31 ASCII Zeichen.
- Zu Beachten ist, dass die Zeichen ", '#', 't' (tab), 'n' (linebreak) 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.

15.5 CLI Local

Über die „General Information" können Parameter für die Kontaktperson und den Standort des Gerätes eingetragen werden. Diese Informationen werden automatisch in die entsprechenden SNMP Variablen übernommen.



Im nächsten 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 wir 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 Adminitrator 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.

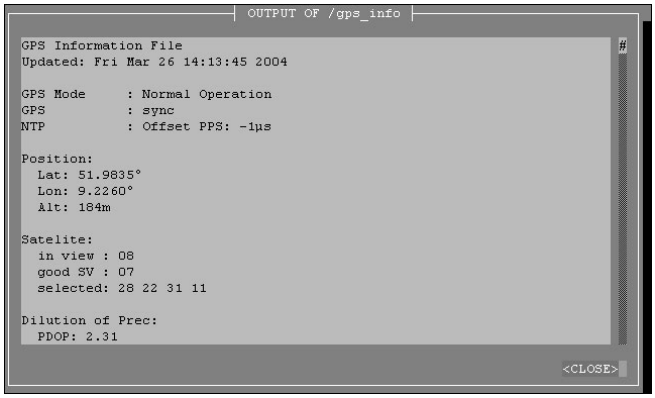
Über die Benutzerverwaltung können neue Benutzer jeweils mit Passwort und Gruppenzugehörigkeit angelegt und gelöscht werden. Zum Ändern eines Benutzers muß dieser erst gelöscht und dann neu angelegt werden. Im unteren Teil der Benutzerverwaltung wird eine Liste aller Benutzer angezeigt. Der Benutzer „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.

Der Punkt „List detailed GPS information“ zeigt GPS spezifische Parameter. Der erste Parameter gibt Auskunft über den Zeitpunkt des letzten Updates der hier gezeigten Informationen. Der nächste Parameter gibt die Empfängerposition im Format Latitude, Longitude und Altitude an. Latitude und Longitude werden in Grad, Minuten und Sekunden dargestellt, Altitude in Metern (über WGS84 Ellipsoid). Unter **Satellite** wird die Anzahl der Satelliten, die sich „in Sicht“ (in view) befinden sowie der brauchbaren (good SV) angezeigt. Außerdem wird der gerade genutzte Satz (selected set) von vier Satelliten angezeigt.



Die Genauigkeit der berechneten Empfängerposition und Zeitabweichung ist abhängig von der Stellung der vier ausgewählten Satelliten zueinander. Aus den Satellitenpositionen und der Empfängerposition lassen sich Werte (**Dilutions Of Precision**; DOP) bestimmen, die eine Beurteilung der ausgewählten Konstellation zulassen. Diese Werte können in einem Untermenü angezeigt werden. PDOP ist die Abkürzung für Position Dilution Of Precision, TDOP für Time Dilution Of Precision und GDOP für General Dilution Of Precision. Niedrigere Zahlenwerte bedeuten hierbei höhere Genauigkeit.

Die nächste Tabelle **Satellite Info** gibt Informationen über die gerade in Sicht befindlichen Satelliten: Die Satellitennummer, Elevation, Azimuth und die Entfernung zum Empfänger zeigen die Position des Satelliten am Himmel. Der Doppler zeigt, ob der Satellit vom Horizont her aufsteigt (positiver Wert) oder wieder verschwindet (negativer Wert).

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 DHCPC wird aktiviert.

Mit „Check configuration“ können alle aktuellen Einstellungen des Zeitservers 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.

16 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, notification, target, agent_mibs, agentx 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 Zeitservers abgefragt werden. Dabei werden Statusinformationen vom NTP und der angeschlossenen Referenzuhr als Text und als Value zur Verfügung gestellt. Um sich alle Statusinformationen des Zeitservers 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.

16.1 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 - LANTIME Dienste -SNMP MIB herunterladen“ bei V5 oder „SYSTEM - Dienste und Funktionen - SNMP MIB herunterladen“ bei V6).

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

16.1.1 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!

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 -v 2c -c public timeserver.meinberg.de mbgLtCfg

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

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

```
root@testhost:/# snmpset -v 2c -r 0 -t 10 -c rwsecret timeserver.meinberg.de
mbgLtCfgHostname.0 string „helloworld“

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

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 -v 2c -r 0 -t 10 -c rwsecret timeserver.meinberg.de
mbgLtCfgHostname.0 string „helloworld“ mbgLtCfgDomainname.0 string „internal.meinberg.de“

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

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

16.1.2 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.

16.1.3 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).

16.1.4 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:

SNMP Zweig	Variable	Datentyp	Beschreibung
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?

SNMP Zweig	Variable	Datentyp	Beschreibung
	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
	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
	mbgLtCfgStratumLocal Clock	integer(0..15)	Stratum-Wert der internen Systemuhr des Zeitservers
	mbgLtCfgNTPTrustedKey	integer	Verweis auf den zu verwendenden Key für die interne Referenzzeitquelle
	mbgLtCfgNTPBroadcast IP	string (IPv4 oder IPv6-Adresse)	IP-Adresse, die für NTP-Broadcasts (oder Multicasts) verwendet wird
	mbgLtCfgNTPBroadcast Key	integer	Verweis auf den zu verwendenden Key für ausgehende NTP-Broadcasts
	mbgLtCfgNTPBroadcast Autokey	integer (0 = disabled, 1 = enabled)	Autokey für NTP Broadcasts verwenden?
	mbgLtCfgAutokeyFeature	integer (0 = disabled, 1 = enabled)	Autokey Feature des NTP Servers aktivieren?

SNMP Zweig	Variable	Datentyp	Beschreibung
	mbgLtCfgAtomPPS	integer (0 = disabled, 1 = enabled)	Atom PPS (pulse per second) aktivert?
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
	mbgLtCfgSNMPROCommunity	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)
	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

SNMP Zweig	Variable	Datentyp	Beschreibung
	mbgLtCfgWMailAddress2	string	Zweiter Empfänger von per Windows Popup Messages verschickten Warnungen und Alarmmeldungen
mbgLtCfgWalldisplay	mbgLtCfgVP100Display 1IP	string (IPv4 oder IPv6-Adresse oder Hostname)	Hostname oder IP-Adresse des ersten Wanddisplays. auf dem Warnungen und Alarmmeldungen angezeigt werden sollen
	mbgLtCfgVP100Display 1SN	string (Hexstring)	Die Seriennummer des ersten Wanddisplays, auf dem Warnungen und Alarmmeldungen angezeigt werden sollen (kann am Display im Konfigurations-Menü abgefragt werden)
	mbgLtCfgVP100Display 2IP	string (IPv4 oder IPv6-Adresse oder Hostname)	Hostname oder IP-Adresse des zweiten Wanddisplays. auf dem Warnungen und Alarmmeldungen angezeigt werden sollen
	mbgLtCfgVP100Display 2SN	string (Hexstring)	Die Seriennummer des zweiten Wanddisplays, auf dem Warnungen und Alarmmeldungen angezeigt werden sollen (kann am Display im Konfigurations-Menü abgefragt werden)
mbgLtCfgNotify	mbgLtCfgNotifyNTPNot Sync	string(Kombination)	Keine, eine oder durch Komma getrennte Kombinationen von Benachrichtigungstypen **email** = Senden einer EMail, **wmail** = Senden einer Winpopup-Meldung, **snmp** = Senden eines SNMP-Traps, **disp** = Anzeige auf Wanddisplay für das Ereignis „NTP nicht synchron“
	mbgLtCfgNotifyNTP Stopped	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „NTP Daemon gestoppt“
	mbgLtCfgNotifyServer Boot	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Zeitserver Bootvorgang“
	mbgLtCfgNotifyRefclock NotResponding	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Referenzzeitquelle antwortet nicht“
	mbgLtCfgNotifyRefclock NotSync	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Referenzzeitquelle nicht synchron“
	mbgLtCfgNotifyAntenna Faulty	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „GPS Antenne nicht angeschlossen oder defekt“
	mbgLtCfgNotifyAntenna Reconnect	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „GPS Antenne wieder OK“

SNMP Zweig	Variable	Datentyp	Beschreibung
	mbgLtCfgNotifyConfig Changed	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Konfiguration geändert“
	mbgLtCfgNotifyLeapSecond Announced	string (Kombination)	(siehe mbgLtCfgNotifyNTPNotSync) für das Ereignis „Schaltsekunde angekündigt“
mbgLtCfgEthernet	mbgLtCfgEthernet If0IPv4IP	string (IPv4 IP-Adresse)	IPv4-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0 IPv4Netmask	string (IPv4 Netzmaske)	IPv4-Netzmaske des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0 IPv4Gateway	string (IPv4 IP-Adresse)	IPv4-Adresse des Default Gateways des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernet If0DHCPClient	integer (0 = disabled, 1 = enabled)	Konfiguration des ersten Netzwerkinterfaces des Zeitservers per DHCP aktiviert?
	mbgLtCfgEthernet If0IPv6IP1	string (IPv6 IP-Adresse)	Erste IPv6-IP-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernet If0IPv6IP2	string (IPv6 IP-Adresse)	Zweite IPv6-IP-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernet If0IPv6IP3	string (IPv6 IP-Adresse)	Dritte IPv6-IP-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernet If0IPv6Autoconf	integer (0 = disabled, 1 = enabled)	IPv6 - Konfiguration des ersten Netzwerkinterfaces des Zeitservers per Autoconf aktiviert?
	mbgLtCfgEthernet If0NetlinkMode	integer (0..4)	Konfiguration der Ethernet-Geschwindigkeit des ersten Netzwerkinterfaces des Zeitservers 0 = Autosensing, 1 = 10Mbit/s Half Duplex, 2 = 10Mbit/s Full Duplex, 3 = 100Mbit/s Half Duplex, 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.

16.2 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
„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.

16.2.1 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.

17 Anhang: Technische Daten

17.1 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 Herstelle empfohlenen gleichwertigen Typ.

Entsorgung gebrauchter Batterien nach Angaben des Herstellers.

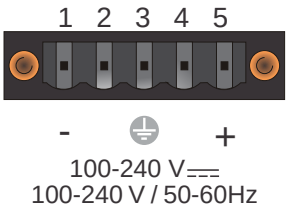
Diese Gerät erfüllt die Anforderungen 93/68/EWG „Elektromagnetische Verträglichkeit“.
Hierfür trägt das Gerät die CE-Kennzeichnung.

CE

17.2 Technische Daten LANTIME / M400/GPS

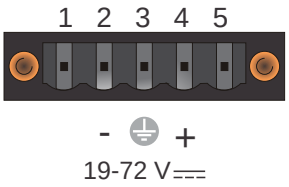
GEHÄUSE:	Gehäuse zur DIN-Schienenmontage Standard: 105 mm x 189 mm x 146 mm (B x H x T) XL - Variante: 105 mm x 189 mm x 166 mm (B x H x T)
SCHUTZART:	IP20
UMGEBUNGS-TEMPERATUR:	0...50 °C / 32 ... 122°F
LUFT-FEUCHTIGKEIT:	max. 85 %
SPANNUNGS-VERSORGUNG:	siehe Netzteil Varianten

Variante: 100-240VAC/DC



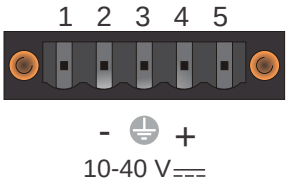
1: VCC -
2: nicht angeschlossen
3: GND (Ground)
4: nicht angeschlossen
5: VCC +

Variante: 19-72VDC



1: nicht angeschlossen
2: VCC -
3: GND (Ground)
4: VCC +
5: nicht angeschlossen

Variante: 10-40VDC



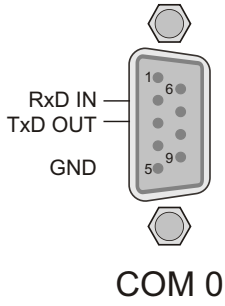
1: nicht angeschlossen
2: VCC -
3: GND (Ground)
4: VCC +
5: nicht angeschlossen

17.3 Ein- und Ausgänge

Bezeichnung	Steckverbindung	Art	Kabel
Terminal	9pol. D-SUB	RS232	Datenleitung geschirmt
Netzwerk	RJ-45	Ethernet	Datenleitung geschirmt
USB	USB Standard	Universal Serial Bus 1.1	(Anschluss eines USB Speichermediums)
IEEE1588 PTP	RJ-45	Ethernet	Datenleitung geschirmt
COM 0	9pol. D-SUB	RS232	Datenleitung geschirmt
PPS	BNC	TTL	Koax geschirmt
10 MHz	BNC	TTL	Koax geschirmt
Antenne	BNC	1575.42 MHz	Koax geschirmt
Netz	5pol. DFK	(siehe technische Daten)	

17.4 Belegung der seriellen Anschlüsse

17.4.1 Serielle Zeittelegramme



COM 0

Pin 2: RxD (Receive Data / input)
Pin 3: TxD (Transmit Data / output)

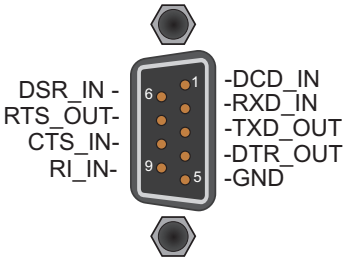
Pin 5: GND (Signal Ground)

Um den 9 poligen Stecker der seriellen Schnittstelle mit einem PC zu verbinden, muss ein Nullmodem Kabel verwendet werden. Die Leitungen RxD und TxD müssen gekreuzt werden.

17.4.2 TERMINAL (Konsole)

9-polige RS232 Schnittstelle zum Anschluss eines seriellen Terminals. Diese Schnittstelle dient zur Konfiguration von einem über ein NULL-MODEM Kabel angeschlossenen PC mittels eines Terminal Programmes. Die Einstellungen für die Schnittstelle auf dem PC müssen auf 38400 Baud, 8 Datenbits, keine Parität und ein Stopbit (8N1) eingestellt werden. Die Terminal Emulation muss auf VT100 gesetzt werden. Nach dem Herstellen der Verbindung sollte die Eingabeaufforderung für die Benutzerkennung angezeigt werden (evtl. noch einmal RETURN drücken).

(Default User: root; Passwort: timeserver).



TERM

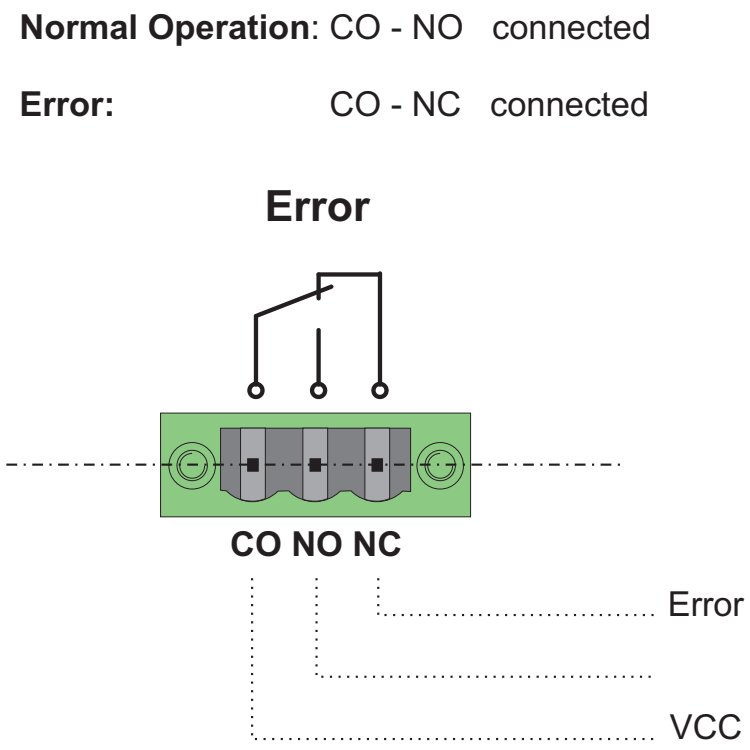
17.5 Error Relais

An der Unterseite des Gerätes befindet sich ein Relaisausgang der mit „Error“ beschriftet ist. Dabei handelt es sich um einen potentialfreien Kontakt, der direkt von der Referenzuhr (GPS, PZF, TCR, ...) angesteuert wird. Im Normalfall, wenn die Referenzuhr synchronisiert hat, schaltet das Relais und der Relais-Kontakt „NO“ ist aktiv. Ist der Empfang gerade gestört oder das Gerät ausgeschaltet, ist der Relais-Kontakt „NC“ aktiv.

Dieses Relais kann zusätzlich über die Benachrichtigungen in den Zustand „ON“ geschaltet werden. In der Zuordnungstabelle im WEB oder CLI Interface für die Benachrichtigungen gibt es eine Spalte, in der jedem Ereignis (mit Ausnahme von „Normal Operation“) der Relaisausgang zugewiesen werden kann. Vorrang hat allerdings immer das „Time Sync Error“ Ereignis der Referenzuhr: bei einem Wechsel nach „Time Sync Error“ wird das Relais auf „ON“ gesetzt. Fehlerzustände die über eine Benachrichtigung gesetzt wurden, werden automatisch zurückgenommen (Relais-Kontakt auf „OFF“, wenn kein „Time Sync Error“ anliegt) wenn ein beliebiger Zugriff über das WEB oder CLI Interface vorgenommen wird.

Technische Daten

SCHALT-SPANNUNG max.:	125 VDC 150 VAC	
SCHALT-STROM max.:	1A	
SCHALT-LEISTUNG max.:	DC AC	30 W 60 VA
SCHALT-LEISTUNG UL/CSA:	0.46A 0.46A 1A	150V AC 65V DC 30V DC
ANSPRECHZEIT:	ca.2ms	



17.6 Technische Daten GPS170

EMPFÄNGER:	Sechskanal C/A-Code Empfänger mit abgesetzter Antennen-/Konvertereinheit
ANTENNE:	Ferngespeiste Antennen-/Konvertereinheit Siehe „Technische Daten GPS Antenne“
ANTENNEN-EINGANG:	Spannungsfestigkeit 1000 V Informationen zum Antennenkabel, siehe Abschnitt “Antennenmontage”
ZEIT BIS ZUR SYNCHRONISATION:	Max. 1 Minute bei bekannter Empfängerposition und gültigen Almanachs Ca. 12 Minuten ohne gültige Daten im Speicher
IMPULS-GENAUIGKEIT:	Abhängig vom Oszillatortyp, nach Synchronisation und 20 Minuten Betriebszeit: < +- 250 nsec (TCXO, OCXO-LQ) < +- 100 nsec (OCXO-MQ,-HQ,-DHQ) < +- 2 μsec in den ersten 20 Minuten nach Synchronisation
SERIELLE SCHNITTSTELLEN:	2 asynchrone serielle Anschlüsse an der Rückwand (RS-232)

COM0:	fest; intern belegt
COM1:	konfigurierbar, sekündliche oder minütliche Ausgabe verschiedener Zeittelegramme

17.6.1 Oszillatorspezifikationen

Verfügbare Oszillatoren für Meinberg GPS Empfänger und NTP Zeitserver:
OCXO, TCXO, Rubidium

	TCXO	OCXO LQ	OCXO MQ	OCXO HQ	OCXO DHQ	Rubidium (only available for 3U models)
Kurzzeitstabilität (τ = 1 sec)	$2 \cdot 10^{-9}$	$1 \cdot 10^{-9}$	$2 \cdot 10^{-10}$	$5 \cdot 10^{-12}$	$2 \cdot 10^{-12}$	$2 \cdot 10^{-11}$
Genauigkeit des PPS (Sekundenimpuls)	< ±250 ns	< ±250 ns	< ±100 ns	< ±100 ns	< ±100 ns	< ±100 ns
Phasenrauschen	1Hz -60dBc/Hz 10Hz -90dBc/Hz 100Hz -120dBc/Hz 1kHz -130dBc/Hz	1Hz -60dBc/Hz 10Hz -90dBc/Hz 100Hz -120dBc/Hz 1kHz -130dBc/Hz	1Hz -75dBc/Hz 10Hz -110dBc/Hz 100Hz -130dBc/Hz 1kHz -140dBc/Hz	1Hz < -85dBc/Hz 10Hz < -115dBc/Hz 100Hz < -130dBc/Hz 1kHz < -140dBc/Hz	1Hz < -80dBc/Hz 10Hz < -110dBc/Hz 100Hz < -125dBc/Hz 1kHz < -135dBc/Hz	1Hz -75dBc/Hz 10Hz -89dBc/Hz 100Hz -128dBc/Hz 1kHz -140dBc/Hz
Genauigkeit freilaufend, ein Tag	$\pm 1 \cdot 10^{-7}$ ±1Hz (Note1)	$\pm 2 \cdot 10^{-8}$ ±0.2Hz (Note1)	$\pm 1.5 \cdot 10^{-9}$ ±15mHz (Note1)	$\pm 5 \cdot 10^{-10}$ ±5mHz (Note1)	$\pm 1 \cdot 10^{-10}$ ±1mHz (Note1)	$\pm 2 \cdot 10^{-11}$ ±0.2mHz (Note1)
Genauigkeit freilaufend, 1 Jahr	$\pm 1 \cdot 10^{-6}$ ±10Hz (Note1)	$\pm 4 \cdot 10^{-7}$ ±4Hz (Note1)	$\pm 1 \cdot 10^{-7}$ ±1Hz (Note1)	$\pm 5 \cdot 10^{-8}$ ±0.5Hz (Note1)	$\pm 1 \cdot 10^{-8}$ ±0.1Hz (Note1)	$\pm 5 \cdot 10^{-10}$ ±5mHz (Note1)
Genauigkeit GPS-synchron, 24h gemittelt	$\pm 1 \cdot 10^{-11}$	$\pm 1 \cdot 10^{-11}$	$\pm 5 \cdot 10^{-12}$	$\pm 1 \cdot 10^{-12}$	$\pm 1 \cdot 10^{-12}$	$\pm 1 \cdot 10^{-12}$
Genauigkeit der Zeit freilaufend, 1 Tag	± 4.3 ms	± 865 µs	± 65 µs	± 22 µs	± 4.5 µs	± 1.1 µs
Genauigkeit der Zeit freilaufend, 1 Jahr	± 16 s	± 6.3 s	± 1.6 s	± 788 ms	± 158 ms	± 8 ms
Temperaturdrift freilaufend	$\pm 1 \cdot 10^{-6}$ (-20...70°C)	$\pm 2 \cdot 10^{-7}$ (0...60°C)	$\pm 5 \cdot 10^{-8}$ (-20...70°C)	$\pm 1 \cdot 10^{-8}$ (5...70°C)	$\pm 2 \cdot 10^{-10}$ (5...70°C)	$\pm 6 \cdot 10^{-10}$ (-25...70°C)

Note 1:
Die Genauigkeit in Hertz basiert auf der Normalfrequenz von 10MHz.

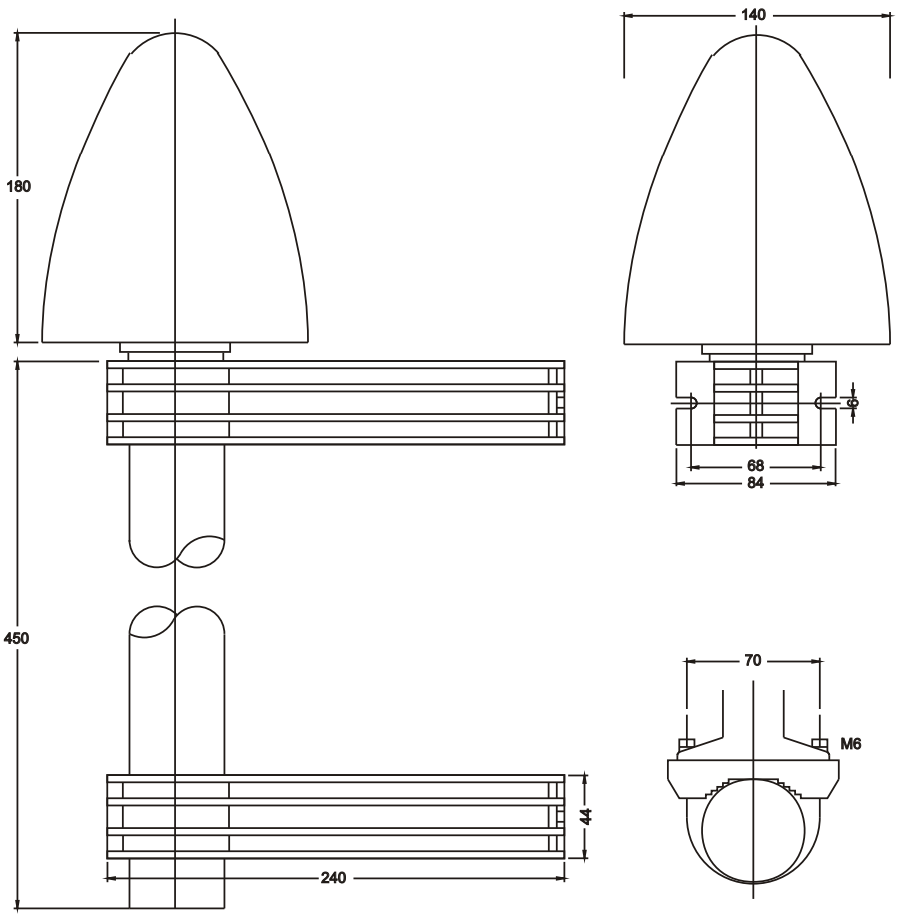
Zum Beispiel: Genauigkeit des TCXO (freilaufend, ein Tag) ist $\pm 1 \cdot 10^{-7} \cdot 10\text{MHz} = \pm 1$ HZ

Die angegebenen Werte für die Zeit und Frequenzgenauigkeit (nicht Kurzzeitstabilität) sind nur für eine konstante Umgebungstemperatur gültig!
Es sind mindestens 24 Stunden GPS-Synchronizität vor Freilauf erforderlich.

17.6.2 Technische Daten GPS Antenne

ANTENNE:	Dielektrische Patch Empfangsfrequenz:	Antenne, 25 x 25 mm 1575,42 MHz
BANDBREITE:	9 MHz	
KONVERTER:	Mischfrequenz: ZF-Frequenz:	10 MHz 35,4 MHz
STROM-VERSORGUNG:	12V ... 18V, ca. 100mA (über Antennenkabel)	
ANSCHLUSS:	N-Norm	
UMGEBUNGS-TEMPERATUR:	-40 ... +65°C	
GEHÄUSE:	ABS Kunststoff-Spritzgussgehäuse, Schutzart: IP66	

Abmessungen:



17.7 Technische Daten LAN CPU

PROZESSOR:	AMD Geode™ LX 800 (500 MHz, 128 KB L2 cache, 3.6 W)
HAUPTSPEICHER:	onboard 256 MByte
CACHESPEICHER:	16 KB 2nd Level Cache
FLASHDISK:	1 GB
NETZWERK ANBINDUNG:	10/100 MBIT über RJ45-Buchse
SERIELLE - SCHNITTSTELLEN:	Vier serielle RS232-Ports 16550 kompatibel mit FIFO davon: eine Schnittstelle über 9-poligen DSUB-Stecker drei Schnittstellen über 96-polige VG-Leiste (nur TxD, RxD, DCD)
PARALLELE SCHNITTSTELLE:	Ein LPT-Port über 96-polige VG-Leiste
VGA-ANSCHLUSS:	Über 10-polige Stiftleiste
TASTATURANSCHLUSS:	Über 10-polige Stiftleiste
STATUSANZEIGE:	- Netzversorgung - ‘Connect‘, ‘Activity‘ und ‘Speed‘ der Netzwerkverbindung
STROMVERSORGUNG:	5 V +- 5 %, ca. 1 A
FRONTPLATTE:	LANTIME im BGT Gehäuse 3 HE / 4 TE (128 mm hoch x 20,3 mm breit)
STECKVERBINDER:	Messerleiste DIN 41612, Typ C 96, Reihen a + b + c DSUB-Stecker, 9-polig, RJ45-Buchse, USB Anschluss
UMGEBUNGS-TEMPERATUR:	0 ... 50 °C
LUFTFEUCHTIGKEIT:	85 % max.

17.8 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]    :
```

17.9 Inhalt des USB Sticks

Der mitgelieferte USB-Stick enthält neben diesem Manual im PDF-Format eine Kurzanleitung zur schnellen Inbetriebnahme, NTP Software für WIndows Rechner und die NTP Time Server Monitor Software.

Das Programm Time Server Monitor bietet die Möglichkeit, den installierten NTP Dienst über eine grafische Benutzeroberfläche zu konfigurieren und zu steuern.

Die Software ist lauffähig
unter folgenden Betriebssystemen:

- Windows 7
- Windows VISTA
- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT
- Windows ME
- Windows 9x

Bei Verlust des USB-Sticks kann die Software aus dem Internet kostenlos heruntergeladen werden unter:

Meinberg Treiber und Tools:
http://www.meinberg.de/german/sw/index.htm

NTP - Software:
http://www.meinberg.de/german/sw/ntp.htm

17.10 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 aufführen. 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.

17.10.1 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

sowie auf der Homepage von GNU/Linux
www.linux.org

17.10.2 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

17.10.3 Network Time Protocol Version 4 (NTP)

Das von David L. Mills geleitete NTP-Projekt ist im Internet unter 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:

17.10.4 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:

Mehr zu mini_httpd finden Sie auf der ACME Labs Homepage:
www.acme.com

17.10.5 GNU General Public License (GPL)

Version 2, June 1991 - Copyright (C) 1989, 1991

Free Software Foundation, Inc.
675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

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

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

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

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

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

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

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

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

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

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

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

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium,

provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

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

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

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

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

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

These requirements apply to the modified work as a whole. If identifiable sections of that work are not 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

17.11 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
```

17.12 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

18 Konformitätserklärung

Declaration of Conformity

Doc ID: LANTIME M400/GPS/PTP-21.01.2010

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

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

Produktbezeichnung *Product Designation*	**LANTIME M400/GPS/PTP**

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

EN55022:2010, Class B	Limits and methods of measurement of radio interference characteristics of information technology equipment
EN55024:2010	Limits and methods of measurement of Immunity characteristics of information technology equipment
EN 60950-1:2006 (+A11:2009 +A12:2011)	Safety of information technology equipment
EN 50581:2012	Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances

gemäß den Richtlinien 2004/108/EG (Elektromagnetische Verträglichkeit), 2006/95/EG (Niederspannungsrichtlinie), 2011/65/EU (Beschränkung der Verwendung bestimmter gefährlicher Stoffe) und 93/68/EWG (CE Kennzeichnung) sowie deren Ergänzungen.
following the provisions of the directives 2004/108/EC (electromagnetic compatibility), 2006/95/EC (low voltage directive), 2011/65/EU (restriction of the use of certain hazardous substances) and 93/68/EEC (CE marking) and its amendments.

Bad Pyrmont, den 21.01.2010

Günter Meinberg
Managing Director