



## **HANDBUCH**

**LCES**

**NTP/RPS/BGT**

8. Februar 2016

Meinberg Funkuhren GmbH & Co. KG



# Inhaltsverzeichnis

<b>1</b>	<b>Impressum</b>	<b>1</b>
<b>2</b>	<b>Sicherheitshinweise für Geräte</b>	<b>2</b>
2.1	Weitere Sicherheitshinweise . . . . .	3
2.2	Versorgungsspannung . . . . .	4
2.3	Verkabelung . . . . .	4
2.4	Verwendete Symbole . . . . .	5
<b>3</b>	<b>LANTIME Basic Configuration Wizard</b>	<b>6</b>
<b>4</b>	<b>Komplettsystem LCES-NTP</b>	<b>7</b>
<b>5</b>	<b>LAN CPU Zeitserver Modul</b>	<b>8</b>
<b>6</b>	<b>Network Time Protocol (NTP)</b>	<b>9</b>
6.1	NTP Clients . . . . .	9
<b>7</b>	<b>Einleitung Konfiguration LANTIME</b>	<b>10</b>
<b>8</b>	<b>Das HTTP Interface</b>	<b>11</b>
8.1	Konfiguration: Hauptmenü . . . . .	11
8.2	Konfiguration: Netzwerk . . . . .	12
8.2.1	Netzwerkeinstellungen . . . . .	12
8.2.2	DHCP IPv4 . . . . .	17
8.2.3	IPv6 Adressen und Autoconf . . . . .	18
8.2.4	High availability bonding . . . . .	19
8.3	Konfiguration: Benachrichtigung . . . . .	20
8.3.1	SYSLOG Server . . . . .	20
8.3.2	Alarm EMAIL . . . . .	21
8.3.3	Windows Messenger Information . . . . .	21
8.3.4	SNMP Trap-Empfänger Information . . . . .	22
8.3.5	VP100/NET Display . . . . .	22
8.3.6	Benutzerdefinierte Benachrichtigung . . . . .	23
8.3.7	NTP Client Überwachung . . . . .	23
8.3.8	Verschiedenes . . . . .	24
8.3.9	Alarm Ereignisse . . . . .	25
8.4	Konfiguration: Sicherheit . . . . .	27
8.4.1	Anmeldung . . . . .	27
8.4.2	Frontplatte . . . . .	27
8.4.3	SSH Secure Shell Login . . . . .	27
8.4.4	SSL Zertifikat für HTTPS erstellen . . . . .	28
8.4.5	SNMP Parameter . . . . .	31
8.4.6	SHS Konfiguration . . . . .	32
8.5	Konfiguration: NTP . . . . .	33
8.5.1	Allgemeine Einstellungen . . . . .	33
8.5.2	Externe NTP Server . . . . .	34
8.5.3	NTP Lokale Uhr . . . . .	35
8.5.4	NTP Broadcast . . . . .	36
8.5.5	NTP Konfiguration anzeigen: . . . . .	37
8.5.6	NTP Berechtigungen: . . . . .	38
8.5.7	NTP Authentication . . . . .	39
8.5.8	NTP Autokey Einstellungen . . . . .	41
8.5.9	NTP Schaltsekunde . . . . .	44

8.6	Konfiguration: PTP	45
8.6.1	PTPv2 - Globale Konfiguration	46
8.6.2	PTP Netzwerk Konfiguration	48
8.6.3	PTP Status Datei	49
8.7	Konfiguration: System	50
8.7.1	Allgemeine Einstellungen	50
8.7.2	Sprache des WEB-Interface	50
8.7.3	Dienste und Funktionen	51
8.7.4	Benutzerverwaltung	53
8.7.5	Systeminformationen	58
8.7.6	Systeminformationen anzeigen	58
8.7.7	Software-/Firmwareupdate	63
8.7.8	Diagnosedatei herunterladen	63
8.7.9	Diagnose Datei herunterladen	63
8.7.10	Konfiguration und Firmwareverwaltung	64
8.7.11	Display	65
8.7.12	Option: Fan Control	65
8.8	Konfiguration: Statistik	66
8.8.1	Statistik Informationen	69
8.9	Konfiguration Funkempfänger	70
8.9.1	Serielle Ports	70
8.9.2	IRIG Settings	71
8.9.3	MRS Einstellungen	72
8.9.4	Synthesiser	73
8.9.5	Zeitzone	73
8.9.6	Freigabe der Ausgänge	73
8.9.7	Verschiedenes	74
8.9.8	Information des Empfängers	76
8.10	Konfiguration: Dokumentation	77
<b>9</b>	<b>SNMP Server</b>	<b>78</b>
9.1	Konfiguration über SNMP	79
9.1.1	Beispiele SNMP Konfiguration	80
9.1.2	Weitere Konfigurationsmöglichkeiten	81
9.1.3	Senden von Befehlen an den Zeitserver per SNMP	81
9.1.4	Konfiguration des Zeitservers via SNMP: Referenz	83
9.2	SNMP Traps	88
9.2.1	SNMP TRAP Referenz	88
<b>10</b>	<b>Anhang: Technische Daten</b>	<b>89</b>
10.1	Technische Daten LCES	89
10.2	Front- und Rückwandanschlüsse	89
10.3	LNE: Zusätzliche Ethernet-Schnittstellen für LANTIME Systeme	90
10.4	Anschluss Spannungsversorgung	91
10.5	Refclock In	91
10.6	PPS In	91
<b>11</b>	<b>Konformitätserklärung</b>	<b>92</b>

# 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](mailto:info@meinberg.de)

Datum: 08.02.2016

## 2 Sicherheitshinweise für Geräte



Dieses Einbaugerät wurde entsprechend den Anforderungen des Standards IEC 60950-1 „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 IEC 60950-1 zu beachten und einzuhalten.

### 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<sup>2</sup> - 2,5mm<sup>2</sup> / 17AWG - 13AWG

## 2.1 Weitere Sicherheitshinweise



Dieses Handbuch enthält wichtige Sicherheitshinweise für die Installation und den Betrieb des Gerätes. Lesen Sie dieses Handbuch erst vollständig durch bevor sie das Gerät in Betrieb nehmen.

Das Gerät darf nur für den in dieser Anleitung beschriebenen Zweck verwendet werden. Insbesondere müssen die gegebenen Grenzwerte des Gerätes beachtet werden. Die Sicherheit der Anlage in die das Gerät integriert wird liegt in der Verantwortung des Errichters!

Nichtbeachtung dieser Anleitung kann zu einer Minderung der Sicherheit dieses Gerätes führen! Bitte bewahren Sie dieses Handbuch sorgfältig auf

### **Zielgruppe**

Dieses Handbuch richtet sich ausschließlich an Elektrofachkräfte oder von einer Elektrofachkraft unterwiesene Personen die mit den jeweils gültigen nationalen Normen und Sicherheitsregeln insbesondere für die Errichtung von Starkstromanlagen vertraut sind.

## 2.2 Versorgungsspannung



### **WARNUNG!**

Dieses Gerät wird an einer gefährlichen Spannung betrieben. Nichtbeachtung der Sicherheitshinweise dieses Handbuchs kann zu ernsthaften Personen- und Sachschäden führen. Einbau, Inbetriebnahme und Bedienung dieses Gerätes dürfen nur von qualifiziertem Fachpersonal durchgeführt werden.

Es müssen die allgemeinen, jeweils gültigen Sicherheitsregeln und Normen (z.B. IEC, DIN, VDE, EN) insbesondere für die Errichtung und den Betrieb von Starkstromanlagen beachtet werden.

Nichtbeachtung kann zu ernsthaften Personen- und Sachschäden und zu Lebensgefahr führen!

Das Gerät darf nicht geöffnet werden, Reparaturen am Gerät dürfen nur durch den Hersteller oder durch autorisiertes Fachpersonal durchgeführt werden.

Die Versorgung des Gerätes muss über eine geeignete Trennvorrichtung (Schalter) erfolgen. Die Trennvorrichtung muss gut zugänglich in der Nähe des Gerätes angebracht werden, und als Trennvorrichtung für das Gerät gekennzeichnet sein.

Der Versorgungsstromkreis muss zum sicheren Betrieb des Gerätes, durch eine normgerechte Installationssicherung abgesichert und mit einem Fehlerstromschutzschalter, gemäß den jeweils gültigen nationalen Normen, ausgestattet sein.

**Das Gerät muss an eine ordnungsgemäße Erdung (PE) angeschlossen werden.**

## 2.3 Verkabelung










### **WARNUNG!**

Lebensgefahr durch elektrischen Schlag! Niemals bei anliegender Spannung arbeiten! Bei Arbeiten an den Steckern und Klemmen der angeschlossenen Kabel müssen immer beide Seiten der Kabel von den jeweiligen Geräten abgezogen werden!



## 2.4 Verwendete Symbole

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

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



## 3 LANTIME Basic Configuration Wizard

Nach dem Einschalten des Gerätes kann nach ca. einer Minute ein Terminalprogramm (z.B. Putty) über die neunpolige Schnittstelle (TERM) mit einem Nullmodemkabel gestartet werden. Die Einstellungen für die Schnittstelle müssen auf 38400 Baud, 8 Datenbits, keine Parität und ein Stopbit (8N1) eingestellt werden. Computer ohne serielle Schnittstelle müssen mit einem „Serial-to USB“ Konverter angeschlossen werden.

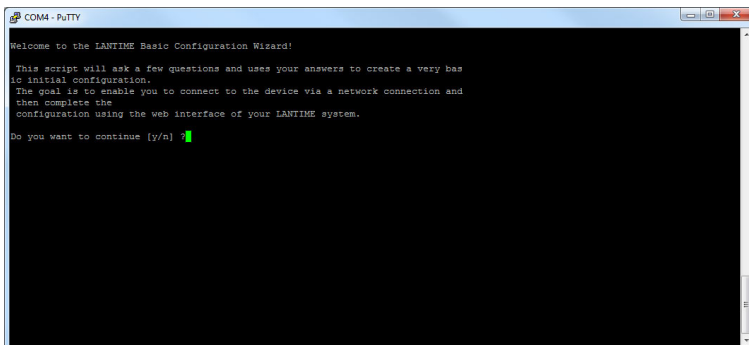
Nach dem Herstellen der Verbindung sollte die Eingabeaufforderung für die Benutzererkennung angezeigt werden:

```
Welcome to Meinberg LANTIME
login: _
```

Als Benutzer (mit Default Login) sollte **root** eingegeben werden.  
Das Passwort ist im Auslieferungszustand **timeserver**.  
(evtl. noch einmal RETURN drücken):

Wechseln Sie mit der Konsole in das Verzeichnis `/wizard/`. Der LANTIME Basic Configuration Wizard kann jetzt mit „startwizard“ gestartet werden.

Nach dem erfolgreichen Starten des Wizards wird der folgende Begrüßungsbildschirm angezeigt:

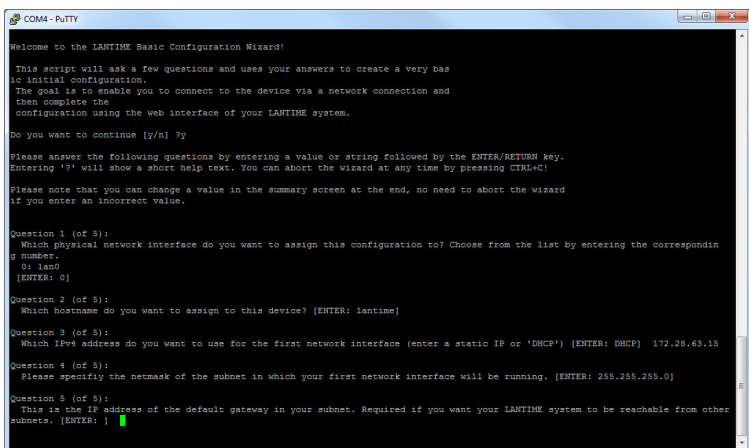


```
COM4 - PUTTY
Welcome to the LANTIME Basic Configuration Wizard!

This script will ask a few questions and uses your answers to create a very basic
initial configuration.
The goal is to enable you to connect to the device via a network connection and
then complete the
configuration using the web interface of your LANTIME system.

Do you want to continue [y/n] ?
```

Durch die Eingabe „y“ starten sie die Konfiguration, mit dem alle weiteren Einstellungen vorgenommen werden können:



```
COM4 - PUTTY
Welcome to the LANTIME Basic Configuration Wizard!

This script will ask a few questions and uses your answers to create a very basic
initial configuration.
The goal is to enable you to connect to the device via a network connection and
then complete the
configuration using the web interface of your LANTIME system.

Do you want to continue [y/n] ?y

Please answer the following questions by entering a value or string followed by the ENTER/RETURN key.
Entering '?' will show a short help text. You can abort the wizard at any time by pressing CTRL+C!

Please note that you can change a value in the summary screen at the end, no need to abort the wizard
if you enter an incorrect value.

Question 1 (of 5):
Which physical network interface do you want to assign this configuration to? Choose from the list by entering the corresponding
number.
0: lan0
[ENTER: 0]

Question 2 (of 5):
Which hostname do you want to assign to this device? [ENTER: lantime]

Question 3 (of 5):
Which IPv4 address do you want to use for the first network interface (enter a static IP or 'DHCP') [ENTER: DHCP] 172.28.63.15

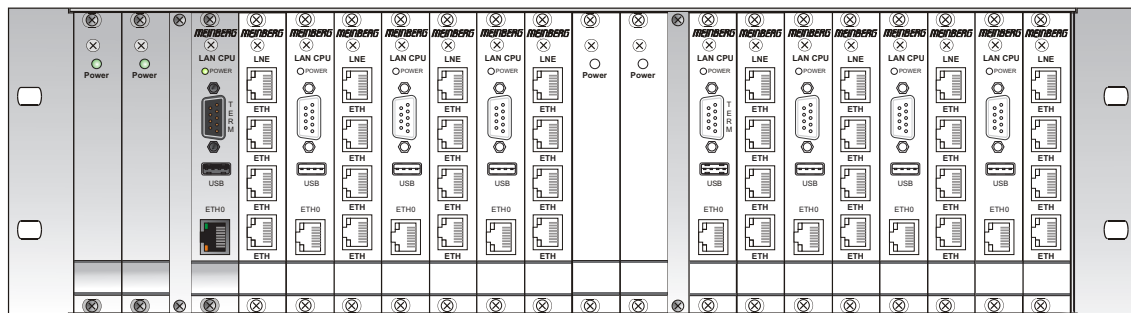
Question 4 (of 5):
Please specify the netmask of the subnet in which your first network interface will be running. [ENTER: 255.255.255.0]

Question 5 (of 5):
This is the IP address of the default gateway in your subnet. Required if you want your LANTIME system to be reachable from other
subnets. [ENTER: ]
```

Bestätigen Sie ihre anschließend ihre Konfigurationen.

## 4 Komplettsystem LCES-NTP

Das System LCES-NTP besteht aus der LAN-CPU, LNE-Karten und Netzteilen (siehe technische Daten), betriebsbereit in einer Baugruppenträger montiert. Die Schnittstellen sowie die Ein-/Ausgangssignale der Baugruppe sind an der Rückwand des Systems über Steckverbinder herausgeführt. Die zusätzlichen Baugruppen werden nachfolgend beschrieben.

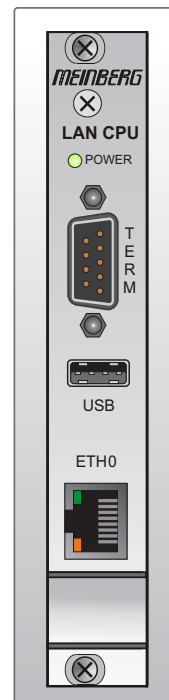


## 5 LAN CPU Zeitserver Modul

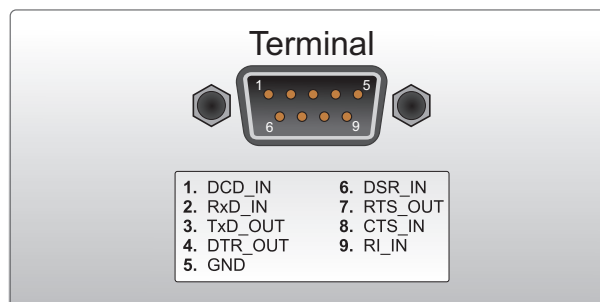
Die Baugruppe LANCPU ist ein kompletter Einplatinenrechner mit LINUX Betriebssystem und vorinstalliertem NTP Server. Die Baugruppe kann in verschiedene GPS-, DCF77, WWVB, MSF oder IRIG-Systeme von Meinberg integriert werden, um diese zu einen NTP Stratum 1 Server zu erweitern. Das System lässt vielfältige Management- und Konfigurationsarten zu, die aus Gründen der Sicherheit einzeln aktiviert/deaktiviert werden können: Web-Oberfläche (HTTP/HTTPS), textbasiertes Setupprogramm (TELNET/SSH) und SNMP. Zum Transfer von Firmware-Updates kann FTP oder SFTP/SCP benutzt werden.

### Technische Daten LAN CPU

<b>Prozessor:</b>	Geode™ LX800 mit 500 MHz
<b>Hauptspeicher:</b>	256 MB
<b>Cachespeicher:</b>	16 KB 2nd Level Cache
<b>Flashdisk:</b>	1 GB
<b>Netzwerkanbindung:</b>	10/100 MBIT über RJ45-Buchse
<b>Serielle Schnittstellen:</b>	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)



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 Benutzererkennung angezeigt werden:



Default User: *root*; Passwort: *timeserver*

## 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 Clients

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:  
<https://www.meinberg.de/german/sw/ntp.htm>

## 7 Einleitung Konfiguration LANTIME

Das LANTIME bietet mehrere Möglichkeiten zur Konfiguration der Parameter:

- TELNET
- SSH
- HTTP Interface
- Secure HTTP Interface (HTTPS)
- Seriell - Terminal im Frontpanel (38400/8N1/VT100)
- SNMP Management

Zur ersten Inbetriebnahme des LANTIME muss das Frontpanel LCD/VFD Interface benutzt werden, um dem Gerät eine IP Adresse zu vergeben (siehe auch DHCP IPv4 oder AUTOCONF IPv6). Wurde einmal das Netzwerkkinterinterface 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.

**Hinweis:** Sollte das System über kein Display verfügen (z.B. LANTIME M100), dann gehen Sie bitte zum Kapitel LANTIME Setup-Wizard in diesem Handbuch.

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

**Default Benutzer: root**

**Default Passwort: timeserver**

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

**ssh root@198.168.10.10** // Default User @ IP Adresse vom LANTIME

**Default Passwort: timeserver**

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

**http://198.168.10.10** // IP Adresse vom LANTIME

**Default Benutzer: root**

**Default Passwort: 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

**Default Benutzer: root**

**Default Passwort: timeserver**

## 8 Das HTTP Interface

Um eine HTTP Verbindung zu dem LANTIME aufzubauen, geben Sie die folgende Zeile in Ihrem WEB-Browser ein: `http://198.168.10.10` - wobei die IP Adresse des LANTIME eingegeben werden muss.

### 8.1 Konfiguration: Hauptmenü

**MEINBERG** LANTIME Konfigurationsprogramm 6.16

Angemeldet als: root  
Zugriffsberechtigung: Super-User  
Build: 6.16.002

Hauptmenü Netzwerk Benachrichtigung Sicherheit NTP System Statistik Dokumentation Empfänger XtraStats Abmelden

### LANTIME - NTP Time Server - Hauptmenü

**Allgemeine Informationen**

LANTIME	M300/GPS (ELX GLX)	Seriennummer	030111293340
Kontakt	Unconfigured ( <a href="#">Jetzt konfigurieren</a> )	Einsatzort	Unconfigured ( <a href="#">Jetzt konfigurieren</a> )
Betriebszeit	4 days, 8:18		

**Netzwerk Informationen**

Hostname	M300gps	Domain	py.meinberg.de
IPv4 (IF 1 - lan0:0)	172.28.11.3/16	IPv6 (IF 1)	Nicht zugewiesen
IPv4 (IF 2 - lan1:1)	Nicht zugewiesen	IPv6 (IF 2)	Nicht zugewiesen

**Empfänger Information**

GPS Status	NORMAL OPERATION	Info des Empfängers	sync; 51.9828 9.2261 166m; 10/10SVs
------------	------------------	---------------------	-------------------------------------

**NTP Informationen**

NTP Status	Offs. GPS 1us	Datum/Uhrzeit	UTC 13:51:58 Tue, 14.10.2014
------------	---------------	---------------	------------------------------

**Systemmeldungen**

```

2014-10-14 13:51:50 UTC: LANTIME -> DEVICE CONFIGURATION CHANGED
2014-10-10 05:37:17 UTC: LANTIME -> OSCILLATOR ADJUSTED [Refclock: 1 ]
2014-10-10 05:36:23 UTC: LANTIME -> NORMAL OPERATION
2014-10-10 05:36:21 UTC: LANTIME -> 1. REFLOCK SYNC
2014-10-10 05:36:21 UTC: LANTIME -> NTP Restart
2014-10-10 05:36:21 UTC: LANTIME -> NTP Sync To GPS
2014-10-10 05:36:21 UTC: LANTIME -> NTP SYNC
2014-10-10 05:36:21 UTC: LANTIME -> GPS Normal Operation
2014-10-10 05:36:21 UTC: LANTIME -> ANTENNA RECONNECT
2014-10-10 05:36:20 UTC: LANTIME -> SYSTEM REBOOT
2014-10-10 05:36:16 UTC: LANTIME -> Device Configuration Changed
2014-10-10 05:36:14 UTC: LANTIME -> 1. Refclock Not Sync

```

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

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

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

Nachdem das Passwort erfolgreich eingegeben wurde, öffnet sich die Startseite des Konfigurations- und Verwaltungsprogramms. Diese Seite gibt einen kurzen Überblick über die wichtigsten Einstellungen und Laufzeitparameter des Gesamtsystems.

#### Folgende Systeminformationen werden hier angezeigt:

- Informationen über den LANTIME Zeitserver
- Netzwerk Informationen der ersten verwendeten Schnittstelle
- Statusinformationen des eingesetzten Empfängers
- NTP Informationen
- PTP Informationen (optional)
- Letzte Nachrichten

Im Feld „Systemmeldungen“ 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 Startvorgang neu erstellt wird. Mit der Navigation im oberen Teil der Web - Oberfläche werden die Untermenüs geöffnet.

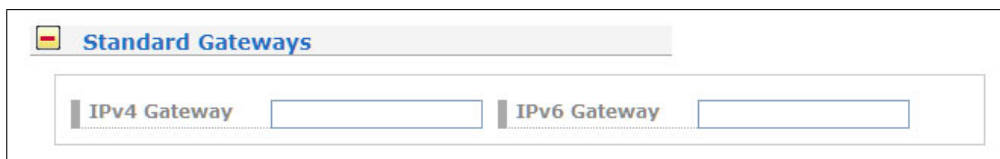
## 8.2 Konfiguration: Netzwerk



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

### 8.2.1 Netzwerkeinstellungen

#### Standard Gateways



Im Abschnitt „Standard Gateways“ kann jeweils für IPv4 und IPv6 ein Default Gateway eingetragen werden.

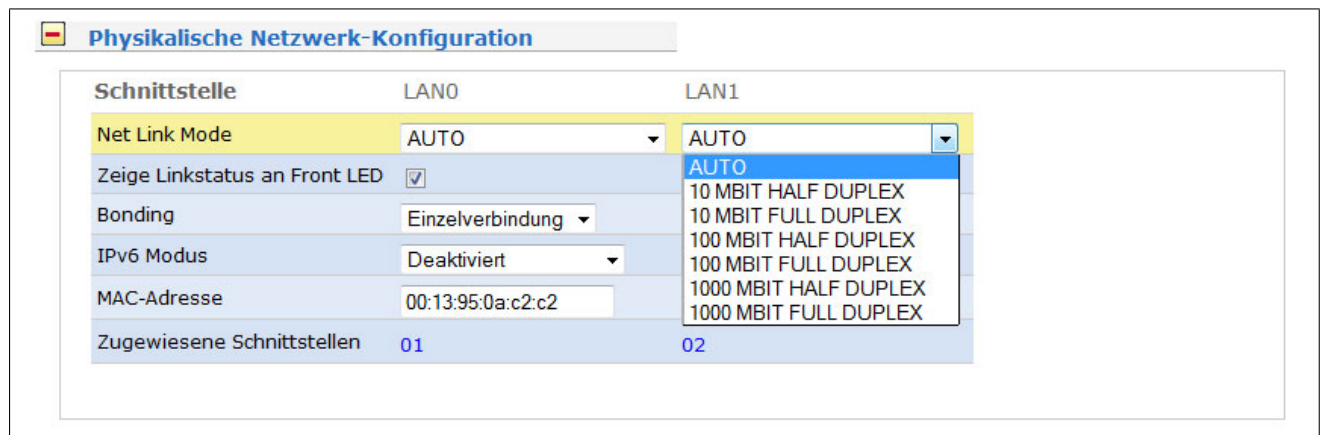
#### Netzwerk Dienste

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

Hier werden die möglichen Zugriffsarten angezeigt: NTP, HTTP, HTTPS, TELNET, SSH, SNMP, FTP, TIME, DAYTIME, FPC und WEBSHELL. Die einzelnen Dienste können über die Checkboxes aktiviert oder deaktiviert und werden direkt nach dem Abspeichern entsprechend gestartet oder beendet.



## Physikalische Netzwerk-Konfiguration



Hier kann der Netzwerk-Verbindungsmodus (Link Speed) der Schnittstelle eingestellt werden. Unter normalen Umständen kann der voreingestellte Wert „AUTO“ unverändert bleiben.

Mögliche Werte sind:

AUTO

Autonegotiation oder Autosensing - der Verbindungsmodus wird automatisch gesetzt.

10 MBIT HALF DUPLEX  
100 MBIT HALF DUPLEX  
1000 MBIT HALF DUPLEX

Hierbei können auf einem Kanal Informationen in jeweils beide Richtungen fließen, allerdings nicht gleichzeitig, sondern nur abwechselnd.

10 MBIT FULL DUPLEX  
100 MBIT FULL DUPLEX  
1000 MBIT FULL DUPLEX

Vollduplex Modus lässt die Übertragung der Informationen in beide Richtungen zur gleicher Zeit zu.

### Weitere Einstellungen:

Die LED am LANTIME kann den Verbindungsstatus der jeweiligen physikalischen Schnittstelle anzeigen (bei aktivierter Checkbox) und der IPv6 Modus kann hier aktiviert werden.

### Ethernet Schnittstellen

Mit diesem Menü können alle Parameter für die physikalischen Netzwerkschnittstellen sowie für die virtuellen Schnittstellen (VLAN) bearbeitet werden. Außerdem können virtuelle Interfaces hinzugefügt werden.

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

Für jede Netzwerkschnittstelle steht ein separates Klappmenü zur Verfügung. Die einzelnen Parameter der jeweiligen Schnittstelle können über die Reiter (Klappmenü) geöffnet und bearbeitet werden.

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**

**Ethernet Schnittstellen**

Interface hinzufügen

Schnittstelle 01: IPv4 IPv6 Sonstiges VLAN Cluster

Schnittstelle 02: IPv4 IPv6 Sonstiges VLAN Cluster

Schnittstelle 03: IPv4 IPv6 Sonstiges VLAN Cluster

Schnittstelle 04: IPv4 IPv6 Sonstiges VLAN Cluster

Schnittstelle 05: IPv4 IPv6 Sonstiges VLAN Cluster

**NEW** Schnittstelle 06: IPv4 IPv6 Sonstiges VLAN Cluster

**IPv4:**

TCP/IP-Adresse

Netzmaske

DHCP-Client aktivieren

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.

**Hinweis für die Erstinbetriebnahme:**

Abhängig von der Anzahl der integrierten physikalischen Netzwerkschnittstellen werden entsprechende Abschnitte für die Netzwerkkonfiguration eingeblendet.

## NTP Cluster

Um NTP-Redundanz für Netzwerk-Clients, die nur einen Zeitserver ansprechen können, zu ermöglichen, können mehrere Zeitserver einem Cluster zugeordnet werden. Dazu werden die ausgewählten Schnittstellen der beteiligten Zeitserver einer gemeinsamen Cluster-IP zugewiesen, an diese Adresse können die Clients dann ihre NTP Anfragen senden. Der aktuelle Master versendet über diese IP seine NTP Pakete an die Clients.

Clustering ermöglicht die Verwendung von mindestens zwei oder mehreren LANTIME Zeitservern, die wie ein einzelner NTP-Server im Netzwerk arbeiten.

The screenshot shows the configuration for 'Ethernet Schnittstellen'. A button 'Interface hinzufügen' is at the top. Below it, two interface entries are visible: 'Schnittstelle 01 - lan0:0' and 'Schnittstelle 02 - lan1:1'. For 'Schnittstelle 01', the 'Cluster' tab is active. The 'Clusterfunktion aktivieren' checkbox is checked. The 'TCP/IP-Adresse' is '172.28.22.16' and the 'Netzmaske' is '255.255.000.000'. The 'Priorität' is set to '0'. The 'Cluster Status' section shows 'Mode' as 'LISTENING (Umkonfiguration aktiv: SLAVE=>MASTER)'. Buttons for 'IPv4', 'IPv6', 'Sonstiges', 'VLAN', and 'Cluster' are present for each interface.

In unserem Beispiel wählen wir die virtuelle Schnittstelle 01 (der physikalischen Schnittstelle LAN 0 dieses Zeitservers zugewiesen) als Cluster-Port. Der Cluster-Tag dieser Schnittstelle wird ausgewählt und die Felder werden gefüllt mit der Cluster-IP und der Netzmaske, wie in der Abbildung dargestellt.

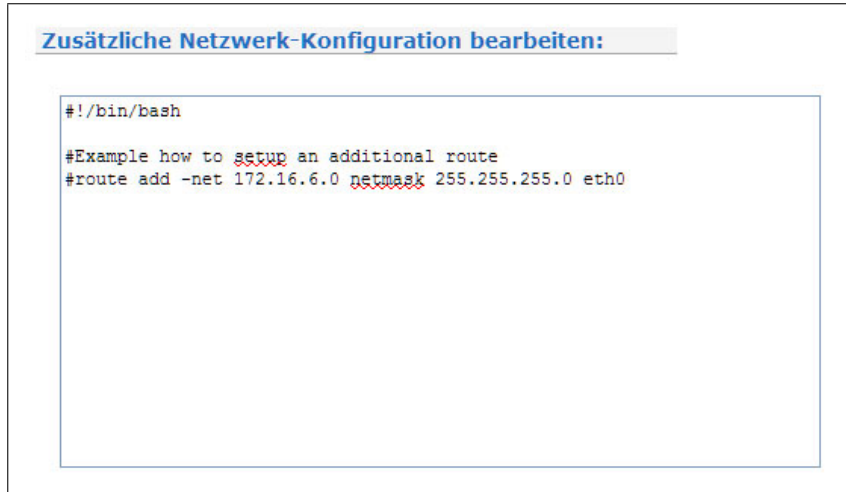
Die gleiche Cluster-IP-Konfiguration wird auf allen NTP-Servern im Cluster eingetragen. Wenn man die Priorität eines bestimmten Servers als Master setzen möchte, dann muss der Prioritätenwert in der Liste auf einen kleineren Wert gestellt werden, als der Wert der anderen am Cluster beteiligten Server.

Der Master-Server wird nach folgenden Parametern in dieser Reihenfolge ausgewählt:

1. NTP-Status (sync, nicht synchron);
2. Priorität (vom Benutzer konfigurierbar, der niedrigste Wert hat die höchste Priorität, Voreinstellung = 0)
3. Ref-Clock Typ - GNSS-Empfänger haben die höchste Bewertung
4. Ref-Clock Status (sync, nicht sync)

**Erweiterte Netzwerkkonfiguration:**

Mit Hilfe der „Erweiterte Netzwerkkonfiguration“ 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.



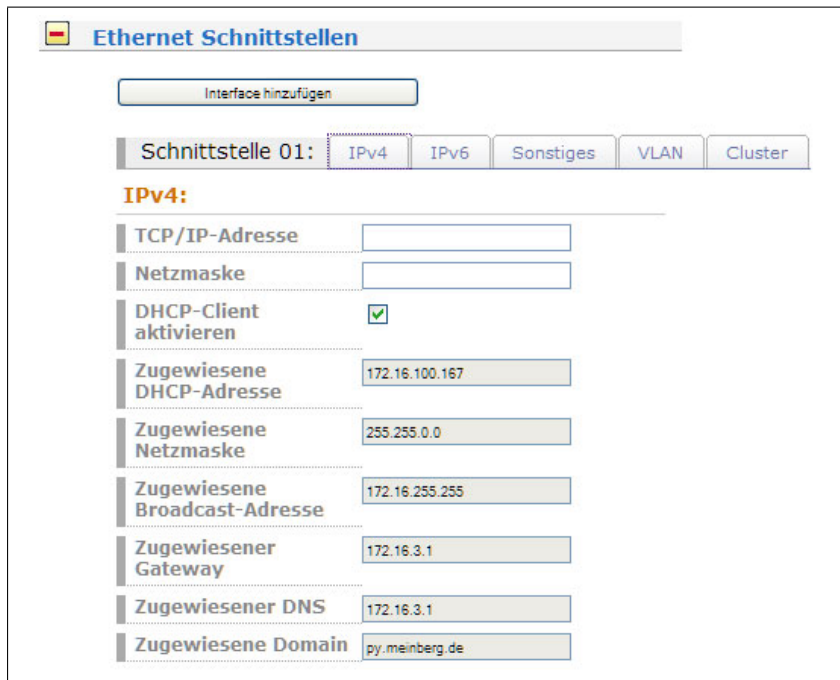
The screenshot shows a terminal window with a title bar that reads "Zusätzliche Netzwerk-Konfiguration bearbeiten:". The terminal content is as follows:

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

Über den Schalter „Zusätzliche Netzwerkkonfiguration“ kann diese Datei direkt editiert werden.

## 8.2.2 DHCP IPv4

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



**Ethernet Schnittstellen**

Interface hinzufügen

Schnittstelle 01: IPv4 IPv6 Sonstiges VLAN Cluster

**IPv4:**

TCP/IP-Adresse	<input type="text"/>
Netzmaske	<input type="text"/>
DHCP-Client aktivieren	<input checked="" type="checkbox"/>
Zugewiesene DHCP-Adresse	172.16.100.167
Zugewiesene Netzmaske	255.255.0.0
Zugewiesene Broadcast-Adresse	172.16.255.255
Zugewiesener Gateway	172.16.3.1
Zugewiesener DNS	172.16.3.1
Zugewiesene Domain	py.meinberg.de

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

### 8.2.3 IPv6 Adressen und Autoconf

Über den Reiter IPv6 im Menü Ethernet Schnittstellen 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/“).

The screenshot shows the configuration page for 'Schnittstelle 01'. At the top, there are tabs for 'IPv4', 'IPv6', 'Sonstiges', 'VLAN', and 'Cluster'. The 'IPv6' tab is selected. Below the tabs, the 'IPv6:' section contains the following fields:

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

At the bottom of the configuration area, there are tabs for 'Schnittstelle 02: IPv4', 'IPv6', 'Sonstiges', 'VLAN', and 'Cluster'.

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.

### 8.2.4 High availability bonding

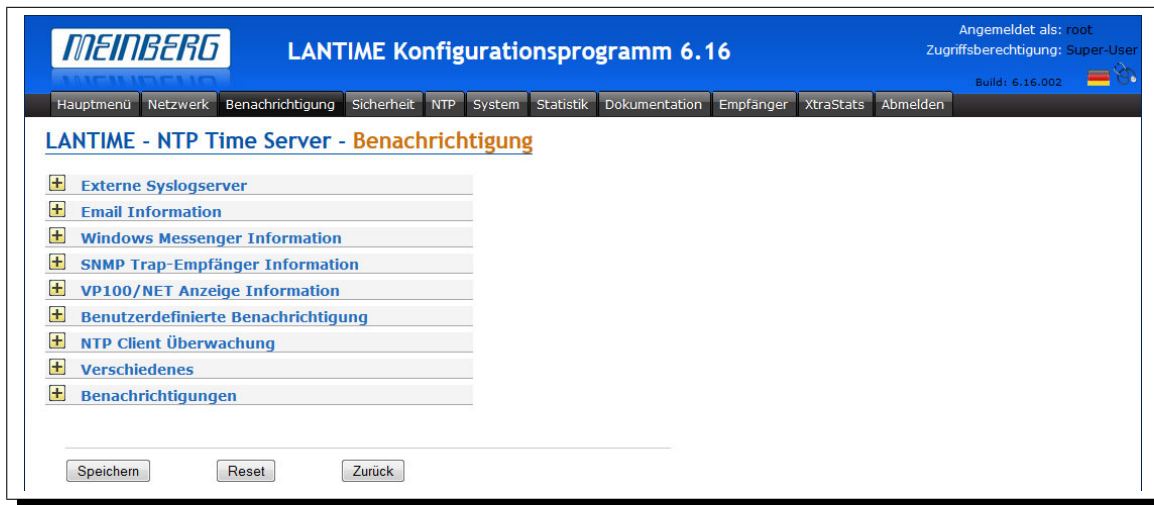
Nach IEEE802.3 ist es möglich, eine logische Netzwerkverbindung auf mehrere physikalische Verbindungen zu verschiedenen Switches aufzuteilen. Nur eine physikalische Verbindung wird zur gleichen Zeit verwendet. Offiziell als Bonding for High Availability bezeichnet, bieten es mehrere Hersteller unter verschiedenen Namen an: Link Aggregation, bonding, trunking, teaming.

The screenshot shows a configuration window titled "Physikalische Netzwerk-Konfiguration". It contains a table with columns for "Schnittstelle", "LAN0", and "LAN1". The "Bonding" row is highlighted in yellow. A dropdown menu is open for the LAN0 "Bonding" setting, showing options: "Einzelverbindung", "Gruppe 1", "Gruppe 2", "Gruppe 3", "Gruppe 4", and "Gruppe 5".

Schnittstelle	LAN0	LAN1
Net Link Mode	AUTO	AUTO
Zeige Linkstatus an Front LED	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Bonding	Einzelverbindung	Einzelverbindung
IPv6 Modus	Deaktiviert	Deaktiviert

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.

## 8.3 Konfiguration: Benachrichtigung



### 8.3.1 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.

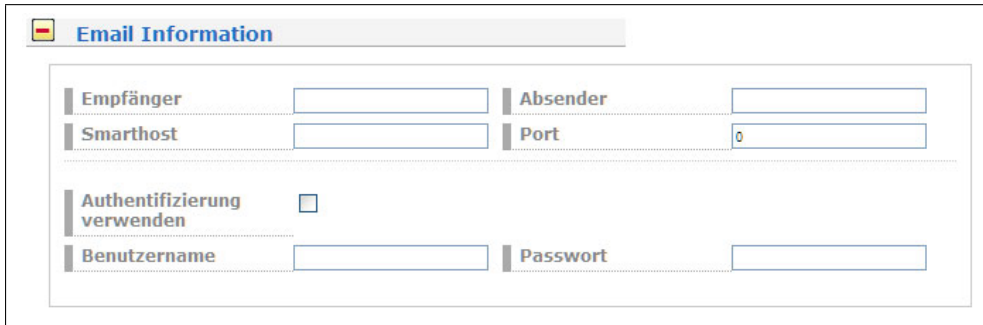
In der Konfiguration können unter dem Menüpunkt „Externe Syslogserver“ zwei IP-Adressen für SYSLOG Server angegeben werden. Sind beide Adressen auf 0.0.0.0 gesetzt oder bleiben beide Felder leer, dann wird der REMOTE SYSLOG-Dienst nicht verwendet.

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 Log-Dateien und löscht diese, wenn sie zu groß werden.



### 8.3.2 Alarm EMAIL

In verschiedenen Systemzuständen können E-Mails mit den entsprechenden Zuständen automatisch vom LAN-TIME versendet werden. In dem Abschnitt „Email Information“ können die Absender Adresse (From:), die E-Mail Adresse (To:) und ein eventuell vorhandener E-Mail Smarthost (ausgehender Mailserver) angegeben werden. Über den Button CC-Empfänger können zusätzliche EMAIL Adressen eingestellt werden, zu denen diese Nachricht gesendet werden soll. Die E-Mail Einstellungen können nicht über das LCD-Frontpanel geändert werden.

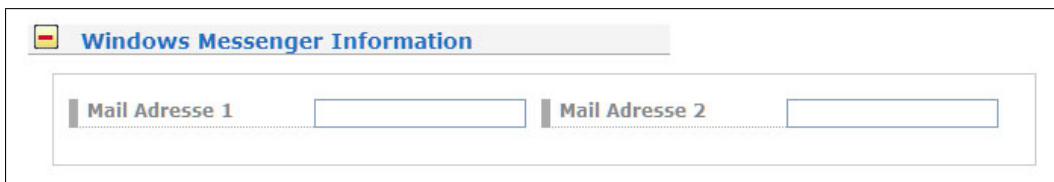


The screenshot shows the 'Email Information' configuration screen. It has a title bar with a German flag icon and the text 'Email Information'. Below the title bar, there are several input fields: 'Empfänger' (Receiver), 'Absender' (Sender), 'Smarthost' (Smarthost), 'Port' (Port), 'Authentifizierung verwenden' (Use authentication) with a checkbox, 'Benutzername' (Username), and 'Passwort' (Password). The 'Port' field contains the number '0'.

#### Folgende Hinweise zur Konfiguration der E-Mails 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

### 8.3.3 Windows Messenger Information



The screenshot shows the 'Windows Messenger Information' configuration screen. It has a title bar with a German flag icon and the text 'Windows Messenger Information'. Below the title bar, there are two input fields: 'Mail Adresse 1' (Mail Address 1) and 'Mail Adresse 2' (Mail Address 2).

### 8.3.4 SNMP Trap-Empfänger Information

In den Einstellungen für die SNMP TRAPs als Benachrichtigung und Alarmpmeldung 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.

### 8.3.5 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 Alarmpmeldungen 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. Bei der IP Adresse werden führende Nullen in den Adressblöcken nicht eingetragen. Die Seriennummer des Displays wird angezeigt, wenn man die rote SET Taste am Display 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).

### 8.3.6 Benutzerdefinierte Benachrichtigung

Über den Benachrichtigungspunkt „Benutzerdefinierte Benachrichtigung“ kann ein frei definierbares Skript automatisch bei einer Bedingung ausgeführt werden. Über den Button „Benachrichtigung Bearbeiten“ kann dieses Skript angezeigt und bearbeitet werden.

```
Benachrichtigung bearbeiten:

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

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.

### 8.3.7 NTP Client Überwachung

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

NTP Client Überwachung

NTP Client Liste bearbeiten    NTP Client Status anzeigen

NTP Client Offset (ms)    10

NTP Client Stratum Limit (ms)    10

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:

### 8.3.8 Verschiedenes

Ein Heartbeat ist eine Verbindung zwischen Rechnern in einem Cluster, um sich gegenseitig darüber zu benachrichtigen, dass sie betriebsbereit sind und ihre Aufgaben erfüllen, also aktiv sind.



The image shows a configuration window titled "Verschiedenes" with a German flag icon. Inside the window, there are two settings:

- "Heartbeat aktivieren" with an unchecked checkbox.
- "Heartbeat-Intervall (m)" with a dropdown menu showing the value "1".

Wenn die Benachrichtigungen eines Rechners ausbleiben, geht ein Programm auf einem aktivem Rechner davon aus, dass dieser „Partner“ nicht mehr verfügbar ist (z. B. durch einen Defekt oder einen Programmfehler) und dass es dafür sorgen soll, dass diese Aufgaben von einem noch funktionierenden Rechner übernommen werden.

### 8.3.9 Alarm Ereignisse

Benachrichtigungen		Ansteuerung							
Ereignis	Status	EMAIL	WMAIL	SNMP	DISP	USER	ALED	RELAY	
NORMAL OPERATION	🕒 seit 21h 57m 30s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP NOT SYNC		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP SYNC	🕒 seit 02s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP STOPPED	🕒 Zuletzt: Thu Oct 16 12:12:31 2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SYSTEM REBOOT	🕒 Zuletzt: Wed Oct 15 14:14:58 2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1. REFCLOCK NOT RESPONDING		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1. REFCLOCK NOT SYNC	🕒 Zuletzt: Wed Mar 16 00:02:01 2011	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1. REFCLOCK SYNC	🕒 seit 21h 57m 36s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ANTENNA FAULTY		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ANTENNA RECONNECT	🕒 seit 21h 57m 37s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ANTENNA SHORT CIRCUIT		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DEVICE CONFIGURATION CHANGED	🕒 Zuletzt: Thu Oct 16 12:12:30 2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LEAP SECOND ANNOUNCED		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP CLIENT LIMIT EXCEEDED		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NETWORK LINK DOWN		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NETWORK LINK UP	🕒 seit 1310d 12h 10m 36s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
LOW SYSTEM RESSOURCES		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SUFFICIENT SYSTEM RESSOURCES		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CERTIFICATE EXPIRED		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
OSCILLATOR ADJUSTED	🕒 seit 21h 34m 54s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
OSCILLATOR NOT ADJUSTED	🕒 Zuletzt: Wed Oct 15 14:15:58 2014	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLUSTER MASTER CHANGED		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLUSTER FALSETICKER DETECTED		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLUSTER FALSETICKER CLEARED		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Automatische Ereignis-Wiederholung:

Max. Anzahl Wiederholungen:

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

**Achtung: mbgLtTrapNormalOperation überschreibt alles! Das ist ein Master-Trap, der anzeigt, dass der LANTIME fehlerfrei arbeitet!**

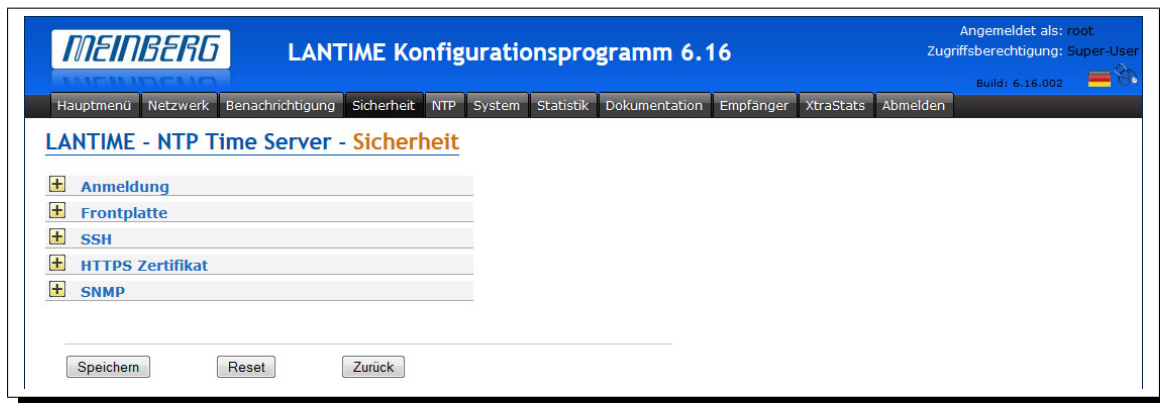
Trapname	Cleared By
NTPStopped	NTPNotSync or NTP Sync
NTPNotSync	NTPSync
ReceiverNotResponding	ReceiverNotSync or ReceiverSync
ReceiverNotSync	ReceiverSync
AntennaFaulty	AntennaReconnect
SecondaryRecNotSync	SecondaryRecSync
PowerSupplyFailure	PowerSupplyUp
NetworkDown	NetworkUp
SecondaryRecNotResp	RecNotSync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

Die folgenden Traps sind Benachrichtigungen, die keinen „Clearing Trap“ haben:

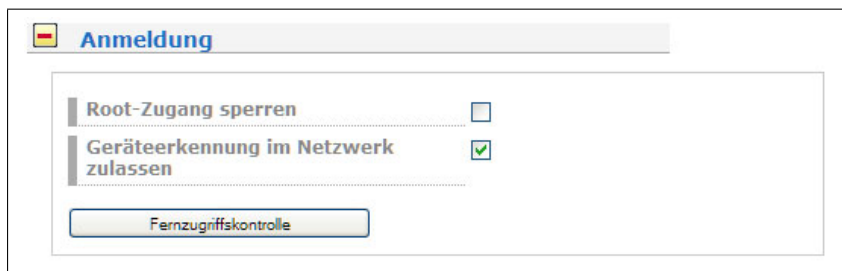
- mbgLtTrapConfigChanged
- mbgLtTrapLeapSecondAnnounced
- mbgLtTrapServerBoot

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.

## 8.4 Konfiguration: Sicherheit



### 8.4.1 Anmeldung



Über den Punkt „Anmeldung“ kann der Zeitserver für den Netzwerkzugang gesperrt werden und über den Schalter Fernzugriffskontrolle kann eine Liste direkt bearbeitet werden: Die entsprechenden IP-Adressen, die Fernzugriff auf diesen Zeitserver erhalten sollen, werden hier eingetragen. Alle anderen Adressen werden geblockt.

**Hinweis:** Bitte nur eine Adresse pro Zeile eintragen!

### 8.4.2 Frontplatte



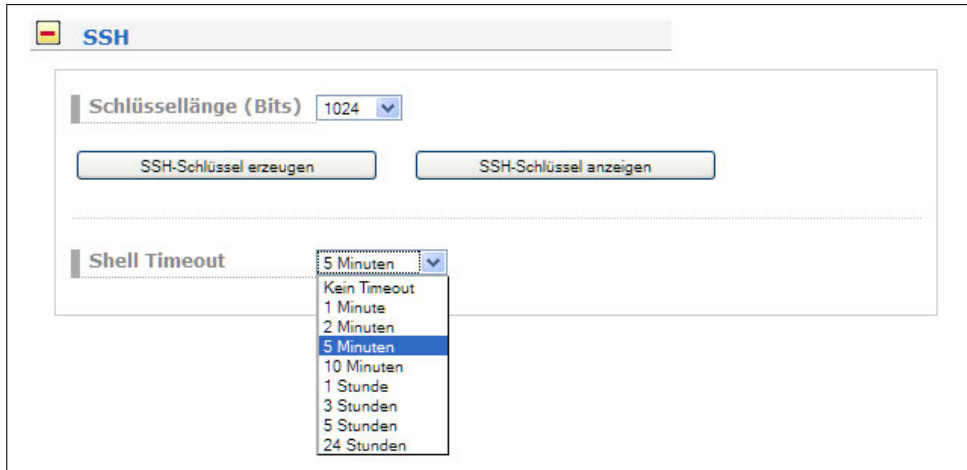
Mit den Checkboxes können die Funktionstasten am LANTIME sowie der USB Port gesperrt werden.

### 8.4.3 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

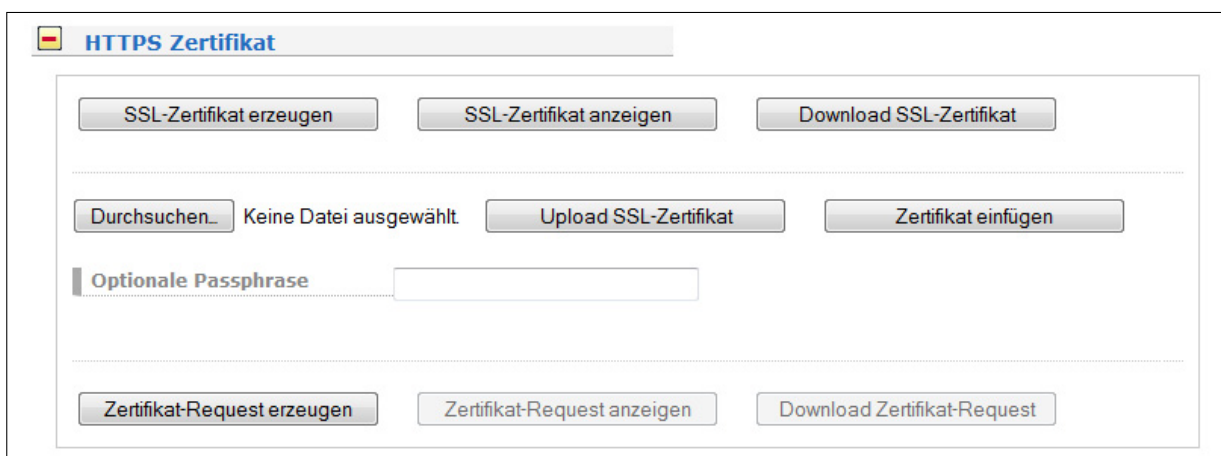
Beim ersten Zugriff muss das neue Zertifikat bestätigt werden und dann werden Sie nach dem Passwort **Default: timeserver** gefragt.



Über den Schalter „SSH Schlüssel erzeugen“ kann ein neuer Schlüssel erzeugt werden. Dieser Schlüssel kann dann über den Schalter „SSH Schlüssel anzeigen“ geöffnet und per „Cut & Paste“ in die lokale SSH Konfiguration des Clients übertragen werden.

#### 8.4.4 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 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.

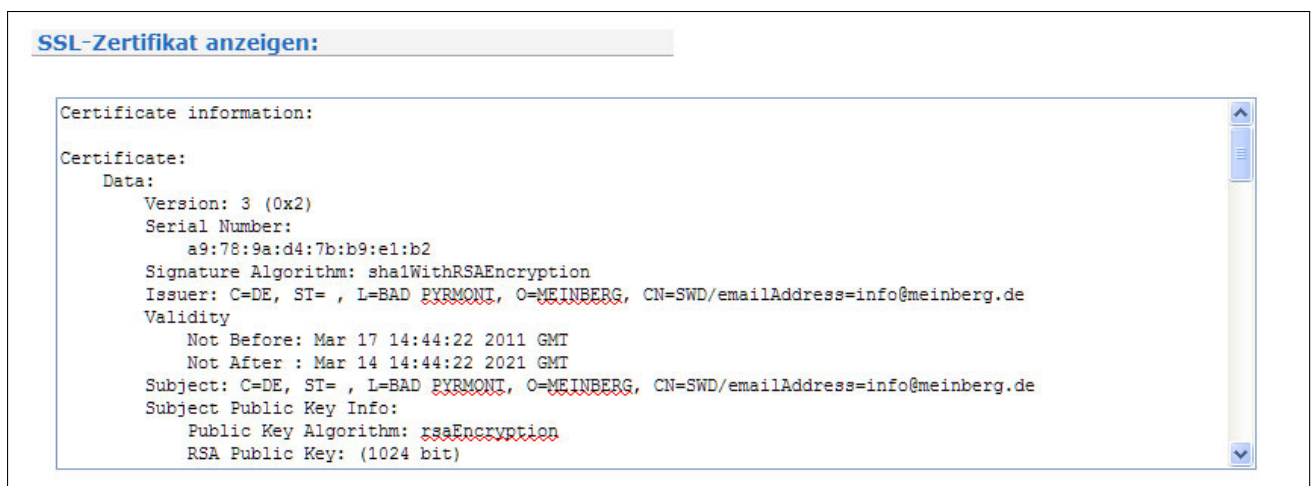


The screenshot shows a web form titled "SSL-Zertifikat erzeugen". It contains several input fields for certificate generation:

- Länderkennung (2 Buchstaben): DE
- Ort: BAD PYRMONT
- Firma: MEINBERG
- Abteilung: SOFTWARE
- Allgemeiner Name: SWD
- Email-Adresse: info@meinberg.de

At the bottom of the form, there are two buttons: "SSL Zertifikat erzeugen" and "Zurück".

Nach der erfolgreichen Erzeugung des SSL Zertifikats kann das gesamte Ergebnis mit dem Schalter „SSL Zertifikat anzeigen“ geöffnet werden.



The screenshot shows a web page titled "SSL-Zertifikat anzeigen:" displaying the details of a generated SSL certificate. The information is presented in a text area with a scrollbar:

```
Certificate information:
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      a9:78:9a:d4:7b:b9:e1:b2
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, ST= , L=BAD PYRMONT, O=MEINBERG, CN=SWD/emailAddress=info@meinberg.de
    Validity
      Not Before: Mar 17 14:44:22 2011 GMT
      Not After : Mar 14 14:44:22 2021 GMT
    Subject: C=DE, ST= , L=BAD PYRMONT, O=MEINBERG, CN=SWD/emailAddress=info@meinberg.de
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
```

Zusätzlich kann ein eigenes Zertifikat mittels des Buttons „Upload SSL Zertifikat“ eingespielt werden.

### Beglaubigtes SSL-Zertifikat einspielen

Ein von einer Zertifizierungsstelle (engl. CA) beglaubigtes Zertifikat kann über den Schalter „Upload SSL-Zertifikat“ eingespielt werden. Das Zertifikat muss im PEM Format vorliegen und den privaten Schlüssel sowie das Zertifikat selber enthalten.

Der Inhalt des privaten Schlüssels ist mit  
„`-----BEGIN RSA PRIVATE KEY-----`“  
„`-----END RSA PRIVATE KEY-----`“ zu umschließen,

das Zertifikat selber mit  
„`-----BEGIN CERTIFICATE-----`“  
„`-----END CERTIFICATE-----`“.

Als Beispiel dient ein Auszug aus einer PEM Datei:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC6FkGxyJ6+Bqxzfp3bNtEYyiRIAbQAIsHblYPG7aQk+8XbIXWB
...
aiLbmu7N3TEdWVDgro8kMuQC/Ugktttx7TdJJbqJoVsF5
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEJTCCA46gAwIBAgIJANF4d1CI2saDMA0GCSqGSIb3DQEBBQUAMIG+MQswCQYD
...
ekZ970dAaPca
-----END CERTIFICATE-----
```

**WICHTIG:** Das Zertifikat darf nicht mit einem Passwort geschützt sein, denn andernfalls kann der Webserver nicht automatisch gestartet werden.

### Beglaubigte mehrstufige / verkettete Zertifikate einspielen

Die nachfolgend beschriebenen Schritte erfordern SSH-Zugang zum LANTIME.

Außerdem werden mehrstufige / verkettete Zertifikate unterstützt. In diesem Fall werden der private Schlüssel und die Zertifikatskette in zwei Dateien aufgeteilt und beide müssen im PEM Format vorliegen. Die eigentliche PEM Datei enthält den privaten Schlüssel, der wie o.g. zu umschließen ist, die CA Datei enthält die Zertifikatskette, wobei die einzelnen Zertifikate ebenfalls wie o.g. zu umschließen sind.

Die PEM Datei mit dem privaten Schlüssel ist manuell nach „`./etc/https.pem`“ zu kopieren, die CA nach „`./etc/https_cert.pem`“.

Anschließend ist die Konfigurationsdatei des Webservers unter „`./etc/httpsd.conf`“ um die Zeile  
‘`ssl.ca-file = ./etc/https_cert.pem`‘ zu erweitern. Das nachfolgende Ausführen des Befehls „`saveconfig`“ speichert die Einstellungen persistent, der Befehl „`restart https`“ wendet die Einstellungen an.

**WICHTIG:** Auch hier dürfen die Zertifikate aus o.g. Gründen nicht mit einem Passwort versehen sein.

### 8.4.5 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 (SNMP Konfiguration).

**SNMP**

**Allgemeine Information**

SNMP Kontakt  SNMP Einsatzort   
Bitte editieren Sie die Werte auf der System-Seite (Allgemeine Einstellungen).

Versuche  Timeout (Sekunden)

Aktivierte Protokoll-Versionen

**V1 & V2C Parameter**

Leser-Community  Schreib-Community

**V3 Parameter**

Security Name  Sicherheitslevel

Engine-ID

Rechte

Authentifizierungsprotokoll

Authentifizierungs-Passphrase  Wiederholung Passphrase

Privacy Protocol

Privacy Passphrase  Wiederholung Passphrase

## 8.4.6 SHS Konfiguration

The screenshot shows a web configuration page titled "SHS Konfiguration". It contains the following settings:

- SHS-Modus:** A dropdown menu set to "Deaktiviert" with a yellow question mark icon to its right.
- Time Limit Warning Level (ms):** A text input field containing the value "10".
- Time Limit Error Level (ms):** A text input field containing the value "25".
- NTP-Dienst beenden bei Time Limit Fehler:** A checkbox that is checked.

### SHS Parameter

SHS ist die Abkürzung von Secure Hybrid Systems und ist auf Systemen mit zwei Referenzzeiten verfügbar. Der SHS-Modus beinhaltet einen Plausibilitätscheck zwischen den empfangenen Zeiten. Die Zeiten der integrierten Zeitempfänger werden kontinuierlich miteinander verglichen und nur wenn die Zeitdifferenz ein einstellbares Limit nicht überschritten hat wird die Zeit an den NTP-Dienst übergeben. Andernfalls wird die Zeitübergabe an NTP sofort eingestellt.

### SHS-Modus

Dieser Parameter aktiviert den SHS-Modus und damit den Zeitvergleich. Ist der SHS-Modus deaktiviert, so findet kein Zeitvergleich statt und die Zeiten beider Empfänger werden direkt an den NTP-Dienst übergeben. NTP entscheidet autonom welche Zeit verwendet wird. Steht die Master-Referenzzeit nicht mehr zur Verfügung, so wechselt der NTP automatisch auf die andere Zeitquelle und bleibt weiter synchronisiert.

### Time Limit Warning Level(ms)

Dieser Wert gibt an, ab welcher Zeitdifferenz eine Warnung über das integrierte Alarmierungssystem gesendet wird. Die Warnung zeigt an, dass die Zeiten der beiden Empfänger nicht mehr übereinstimmen und dass ein Zeitfehler evtl. kurz bevorsteht.

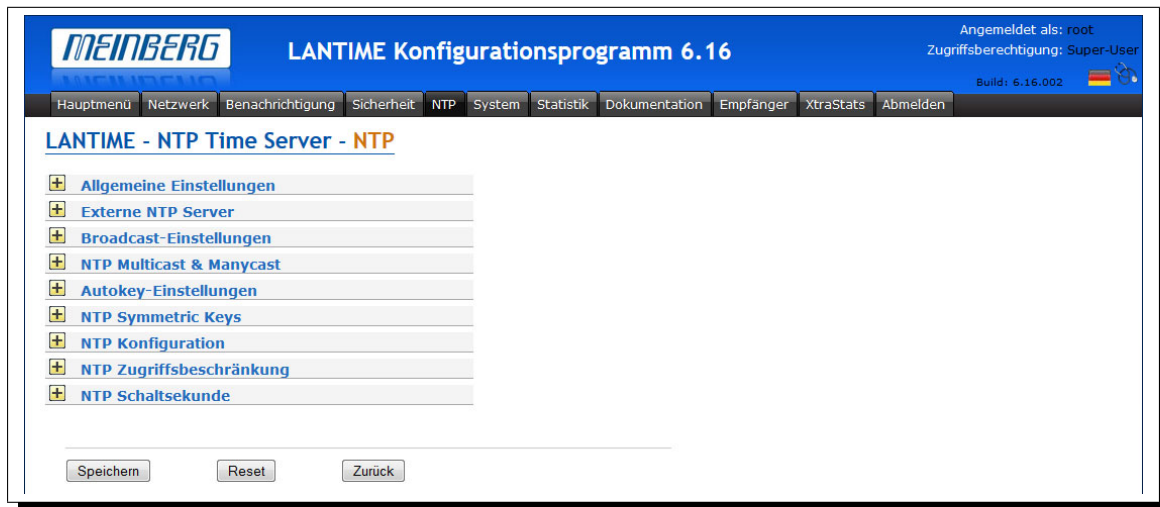
### Time Limit Error Level(ms)

Dieser Wert gibt an, ab welcher berechneten Zeitdifferenz die Zeitübergabe an NTP eingestellt werden soll und ein entsprechender Alarm über das Benachrichtigungssystem generiert wird. Wird der SHS-Fehler ausgelöst so ist ein Administratorzugriff notwendig, um den NTP-Dienst wieder in den Normalzustand zu versetzen. Der Administrator muss die Zeiten prüfen und bestätigen, dass alles wieder in Ordnung ist. Ein entsprechender Dialog wird im Web-Interface angezeigt. Nach der Bestätigung wird die Zeitübergabe an den NTP-Dienst wieder gestartet und der NTP synchronisiert wieder.

### Stop NTP Service on Time Limit Error

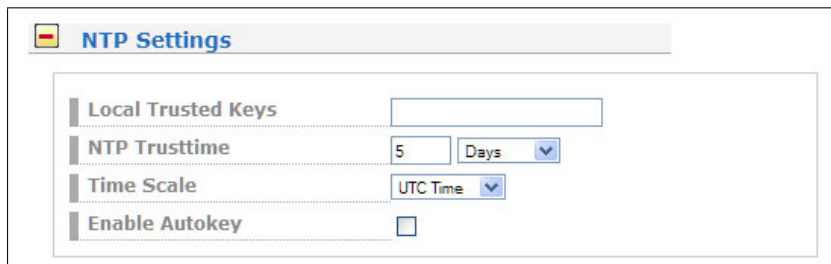
Hier kann entschieden werden, ob bei einem Fehler des Zeitvergleichs auch gleich der NTP-Dienst beendet werden soll. In diesem Fall würden anfragende NTP-Clients keine Antwort mehr vom Zeitserver erhalten.

## 8.5 Konfiguration: NTP



Die NTP Konfiguration wird für das Setup von zusätzlichen NTP Parametern und für spezifizierte Einstellungen des NTP Subsystems benötigt.

### 8.5.1 Allgemeine Einstellungen



Das Feld „Vertrauenswürdige Schlüssel“ beinhaltet eine Liste von allen vertrauenswürdigen symmetrischen Schlüsseln (getrennt durch Komma oder Leerzeichen), welche durch den NTPD des LANTIME akzeptiert werden.

## 8.5.2 Externe NTP Server

Über diese Konfigurationsseite können zusätzliche NTP Parameter eingestellt werden. Im oberen Teil können bis zu 7 externe NTP Server als Redundanz zu der internen Referenzuhr angegeben werden. Dabei kann wahlweise, ein symmetrischer Schlüssel eingegeben werden und AUTOKEY aktiviert werden.

**Externe NTP Server**

Externe NTP Server Adresse 1	<input type="text"/>	Symmetrische Schlüssel <input type="text"/>	Autokey verwenden <input type="checkbox"/>
Minpoll	<input type="text" value="Standard"/> Sekunden	Maxpoll	<input type="text" value="Standard"/> Sekunden
...			
Externe NTP Server Adresse 7	<input type="text"/>	Symmetrische Schlüssel <input type="text"/>	Autokey verwenden <input type="checkbox"/>
Minpoll	<input type="text" value="Standard"/> Sekunden	Maxpoll	<input type="text" value="Standard"/> Sekunden
...			

### 8.5.3 NTP Lokale Uhr



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 über dem PPS (PulsePerSecond) der Referenzuhr erreicht, welcher vom Betriebssystem ausgewertet wird. 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 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.

## 8.5.4 NTP Broadcast

NTP Broadcast

Broadcast Adresse 1	<input style="width: 100%;" type="text"/>
Broadcast Intervall	Standard <span style="font-size: small;">▼</span> Sekunden
Symmetrische Schlüssel	<input style="width: 100%;" type="text"/> <input type="checkbox"/> Autokey verwenden
Broadcast Adresse 2	<input style="width: 100%;" type="text"/>
Broadcast Intervall	Standard <span style="font-size: small;">▼</span> Sekunden
Symmetrische Schlüssel	<input style="width: 100%;" type="text"/> <input type="checkbox"/> Autokey verwenden
Broadcast Adresse 3	<input style="width: 100%;" type="text"/>
Broadcast Intervall	Standard <span style="font-size: small;">▼</span> Sekunden
Symmetrische Schlüssel	<input style="width: 100%;" type="text"/> <input type="checkbox"/> Autokey verwenden
Broadcast Adresse 4	<input style="width: 100%;" type="text"/>
Broadcast Intervall	Standard <span style="font-size: small;">▼</span> Sekunden
Symmetrische Schlüssel	<input style="width: 100%;" type="text"/> <input type="checkbox"/> Autokey verwenden
Broadcast Adresse 5	<input style="width: 100%;" type="text"/>
Broadcast Intervall	Standard <span style="font-size: small;">▼</span> Sekunden
Symmetrische Schlüssel	<input style="width: 100%;" type="text"/> <input type="checkbox"/> Autokey verwenden

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 NTP4 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 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 - OCXO HQ Quarz (je nach LANTIME Modell) 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.

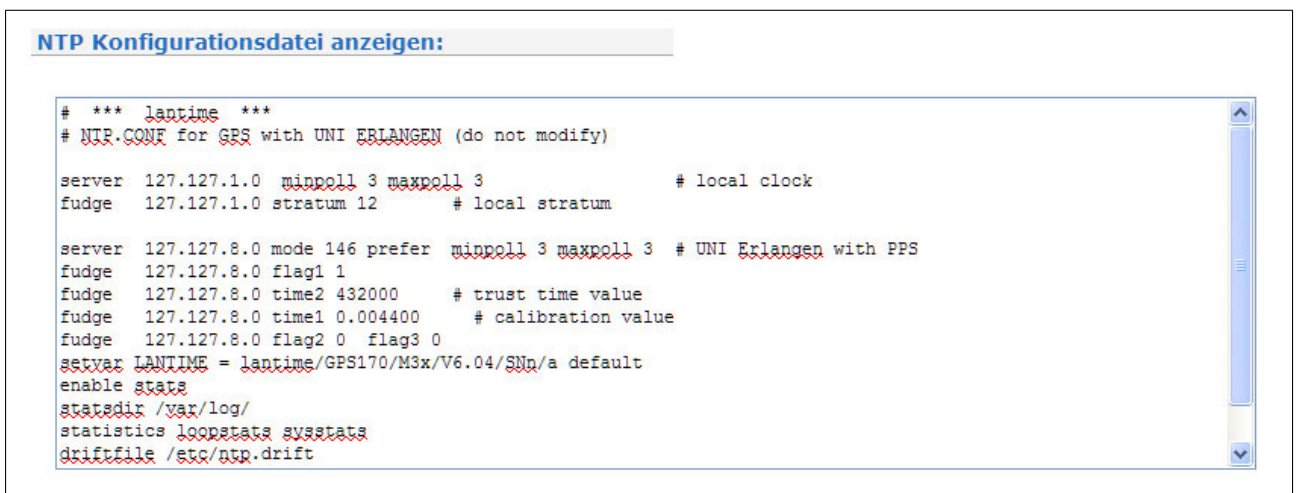


### 8.5.5 NTP Konfiguration anzeigen:

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.



### 8.5.6 NTP Berechtigungen:

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

Die folgenden Eintragungen werden automatisch in der NTP Konfigurationsdatei gemacht:

```
#NTP RESTRICTION SECTION - LAST MODIFIED: Wed Jan 5 07:47:58 2011
restrict 0.0.0.0 mask 0.0.0.0 ignore      # block IPv4 completely
restrict 127.0.0.1 mask 255.255.255.255 # allow localhost
restrict ::0 ignore                       # block IPv6 completely

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

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

#### NTP Berechtigung hinzufügen

IP-Adresse	<input type="text"/>
Netzmaske	<input type="text"/>
<input type="button" value="Berechtigung hinzufügen"/>	

#### Aktuelle NTP Berechtigungen

Aktuelle keine Berechtigungen gespeichert.

### 8.5.7 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 ungläubwürdig und für eine Synchronisation nicht geeignet gekennzeichnet, wenn sie entweder unauthentisierte Pakete, authentifizierte Pakete die nicht entschlüsselt werden können oder authentifizierte Pakete, die einen falschen Key benutzen, senden. Zu beachten ist, dass ein Server der viele Keys kennt (identifiziert durch viele Key IDs) möglicherweise nur einen Teil dieser verwendet. Dies ermöglicht dem Server einen Client, der eine authentifizierte Zeitinformation verlangt, zu bedienen ohne diesem selbst zu trauen. Einige zusätzliche Konfigurationen sind erforderlich um die Key ID zu spezifizieren, die jeden Partner auf Authentizität prüft. Die Konfigurationsdatei 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 festgelegt. In der **trustedkey**-Zeile werden die Keys angegeben, die als uncompromised bekannt sind; der Rest sind verfallene oder compromised Keys. Beide Sätze von Keys müssen in der unten beschriebenen Datei **ntp.keys** deklariert werden. Dies ermöglicht es, alte Keys zu reaktivieren, während das wiederholte Senden von Keys minimiert wird. Die **requestkey 15** Zeile deklariert den Key für mode-6 control messages wie in RFC-1305 spezifiziert und vom **ntpq** Utility Programm benutzt, während die Zeile **controlkey 15** den Key für mode-7 private control messages deklariert, wie vom **ntpd** Utility Programm benutzt wird. Diese Keys werden benutzt um die Daemon Variablen vor unberechtigten Modifikationen zu schützen.

Die Datei **ntp.keys** beinhaltet eine Liste der Keys und zugehöriger IDs, die der Server kennt und muss deshalb auf nicht lesbar gesetzt werden. 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 Rlrop8KPPvQvYotM # md5 key as an ASCII random string
14     M sundial          # md5 key as an ASCII string
```

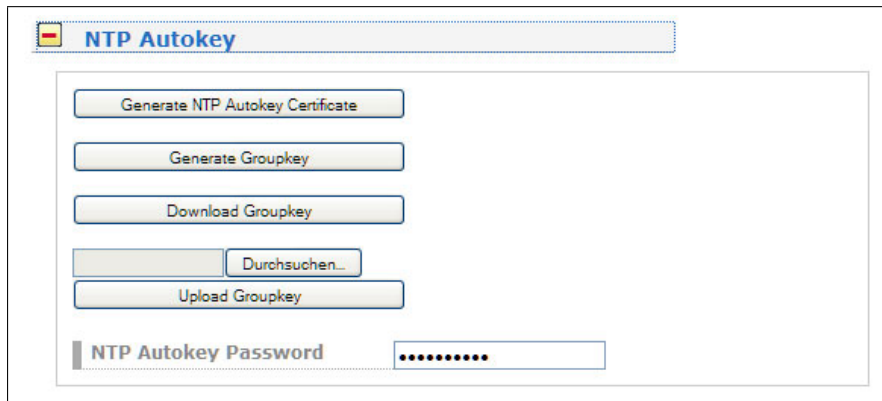
Die erste Spalte der Datei beinhaltet die Key ID, die zweite Spalte das Format des Keys und die dritte den Key selbst. Es gibt vier Key-Formate:

- Ein **A** steht für einen DES Key mit bis zu acht 7-Bit ASCII Characters, bei dem jeder Character für ein Key-Octet steht (wie bei einem Unix Passwort).
- Ein **S** steht für einen DES Key als Hex Ziffer, bei welchem das niederwertigste Bit (LSB) jedes Octets das ungerade Parity Bit ist.

- Ein mit **N** gekennzeichnete Key ist wiederum als Hex Ziffer geschrieben, jedoch im NTP Standard Format mit dem höchwertigen Bit (HSB) jedes Octets als das ungerade Parity Bit.
- Ein mit **M** gekennzeichnete Key ist ein MD5 Key mit bis zu 31 ASCII Zeichen.
- Zu Beachten ist, dass die Zeichen „ , ‘#’, ‘t’, ‘n’ und ‘0’ weder im DES noch im MD5 ASCII Key verwendet werden können!
- Key 0 (zero) ist reserviert für spezielle Zwecke und sollte deshalb hier nicht auftauchen. Vom LANTIME werden über das Benutzerinterface nur MD5 Keys unterstützt.

### 8.5.8 NTP Autokey Einstellungen

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 (im Menüpunkt „NTP“ 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 („NTP“ -> „NTP Autokey“ -> „Upload Groupkey“) und ein eigenes, selbstsigniertes Zertifikat erzeugen (ohne es als „Trusted“ zu markieren). Da beim Generieren eines Zertifikats über das Webinterface oder das CLI-Setupprogramm grundsätzlich immer als „Trusted“ markierte Zertifikate erstellt werden, müssen Sie zum Erstellen von Zertifikaten ohne „Trusted“-Merkmal das Programm ntp-keygen manuell auf dem LANTIME aufrufen (in einer SSH-Sitzung):

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

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

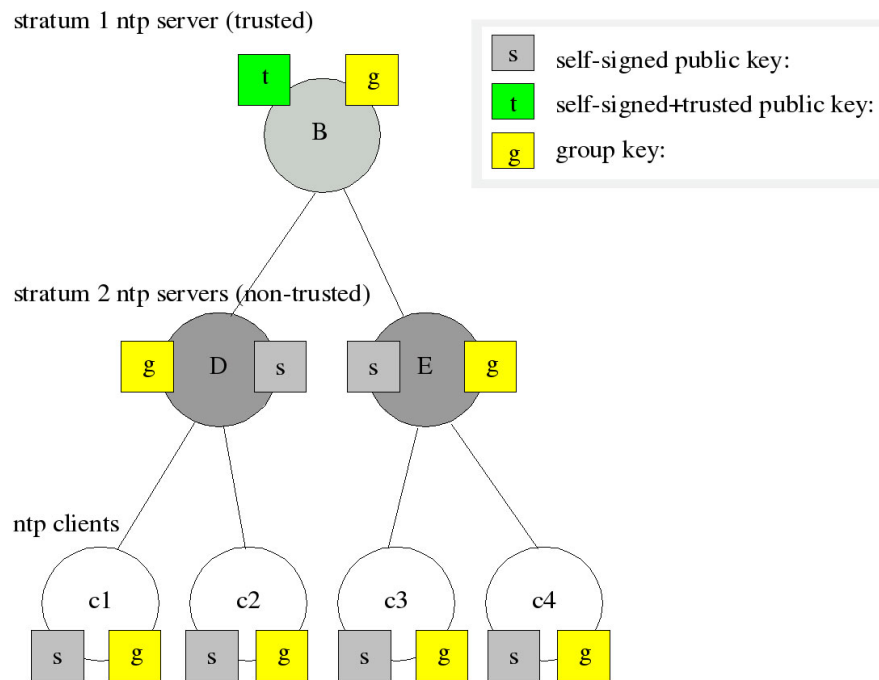
```
cp /etc/ntp/ntpkey_* /mnt/flash/config/ntp/uploaded_groupkeys
```

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

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

### Beispiel:

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



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

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

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

### 8.5.9 NTP Schaltsekunde

**NTP Schaltsekunde**

Durchsuchen... Leap-Sekunden Datei manuell hochladen

Schaltsekundendatei automatisch herunterladen  Download-Intervall Einmal am Tag

Download-URL --- Bitte wählen ---

Eigene Download-URL --- Bitte wählen ---

http://www.meinberg.de/download/ntp/leap\_second

ftp://time.nist.gov/pub/leap-seconds.3427142400

Datei herunterladen Datei anzeigen

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 und Langwellensender enthalten, so dass der Empfänger intern synchron zur internationalen Zeitskala UTC läuft.

Sie können in diesem Menü einen Link auf eine Datei setzen, die sich auf dem Meinberg oder NTP Server befindet. Selbstverständlich können Sie hier auch einen eigenen Link eintragen oder eine Datei manuell auf den LANTIME laden.

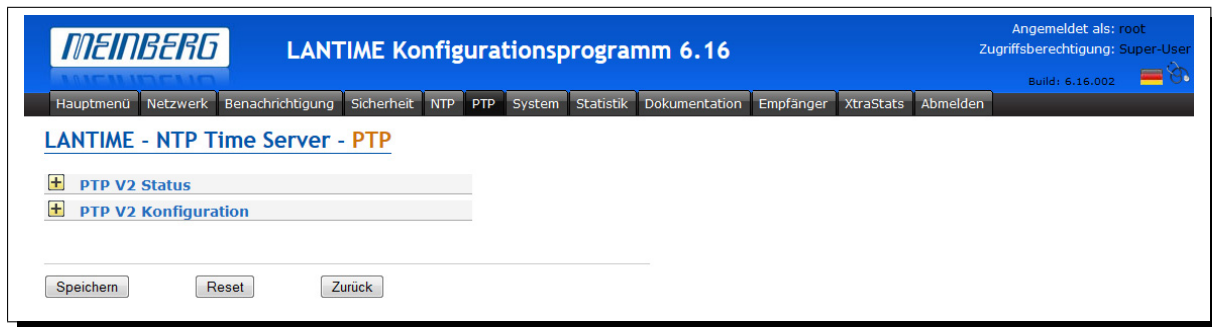
#### Verfügbare Download Quellen

Meinberg: [http://www.meinberg.de/download/ntp/leap\\_second](http://www.meinberg.de/download/ntp/leap_second)

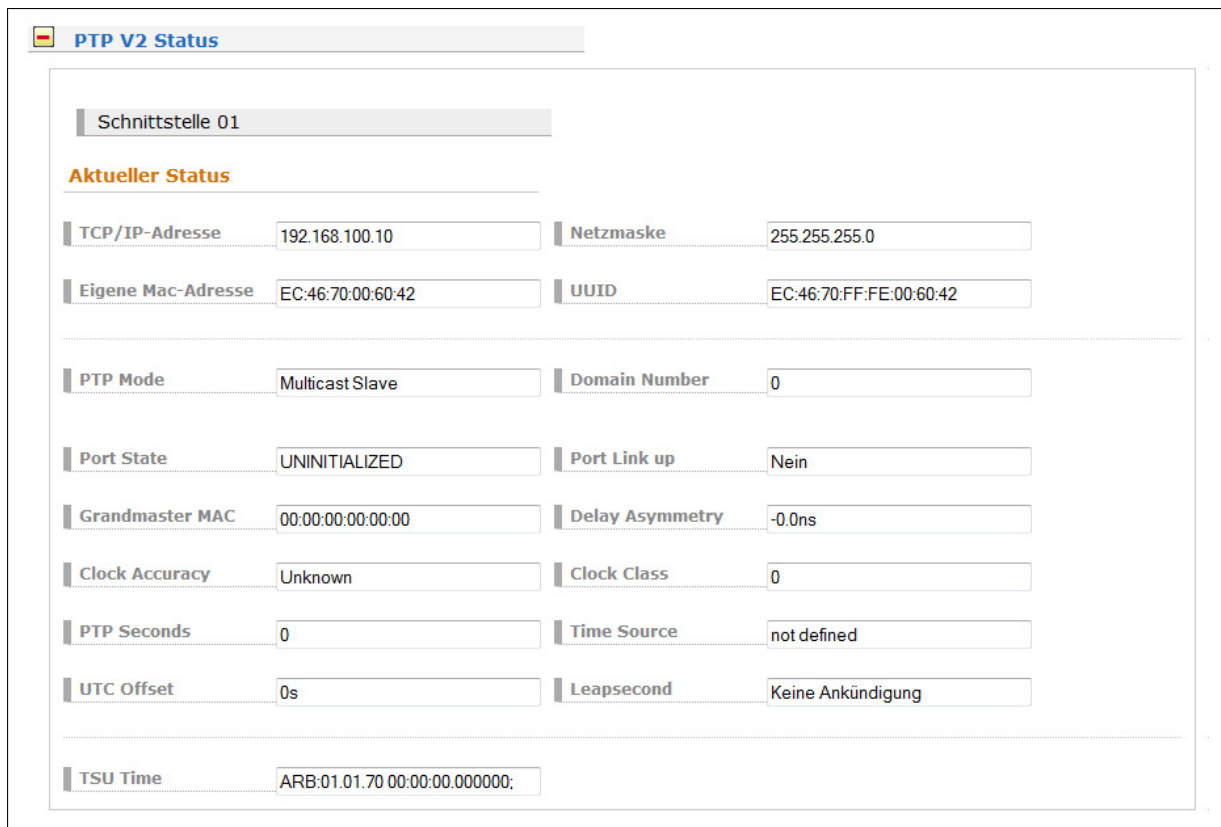
NTP.ORG: <ftp://time.nist.gov/pub/> (leap-seconds.xxxxxxxxx)



## 8.6 Konfiguration: PTP



Im Menü „PTPv2 Status“ werden die wichtigsten PTP Parameter des Gerätes angezeigt (Modus und PTP Status). Im SLAVE Modus wird zusätzlich eine grafische Darstellung des PTP Offsets und des PTP Pathdelays von der internen Uhr zum Grandmaster angezeigt (Menü Statistik -> PTPV2 Statistik)



Über die PTPv2 Konfiguration kann auf die Datei „ptp2\_global\_conf\_0“ zugegriffen werden um die PTP Konfiguration anzupassen. Die Einstellungen der Parameter für die PTP-Netzwerkschnittstelle können über den Reiter „Netzwerk“ geändert werden (Host, Domain, Nameserver, IP Adresse, Netzmaske und Def. Gateway).

Mit dem Menüpunkt Profil können Sie das PTP Profil des Gerätes anpassen (Unicast oder Multicast).

Wenn das Gesamtsystem mehr als eine PTP Karte enthält, wird für jede PTP Karte ein eigenes Konfigurationsmenü angezeigt. Eine genaue Beschreibung der Parameter finden Sie im Kapitel 8.6.1 (Globale PTP Parameter).

## 8.6.1 PTPv2 - Globale Konfiguration

**PTP V2 Konfiguration**

Schnittstelle 01: Netzwerk Global

**Global:**

Aktuelles Profil: Custom

---

PTP Mode: Multicast Slave

Delay Mechanism: E2E

Network Protocol: UDP/IPv4 (L3)

Priorität1: 128

Announce Interval: 1 announce message every 2 seconds

Sync Intervall: 1 sync message per second

Delay Request Interval: 1 request message every 2 seconds

Interval Duration [s]: 60

Use Power Profile TLVs: Nein

Grandmaster ID: 3

PTP Management Nachrichten deaktivieren:

Grandmaster Address: 172.29.9.210

Domain Number: 0

Timescale: PTP Standard (TAI)

Priorität2: 128

Default Asymmetry Offset [ns]: 0

HQ-Filter: Nein

Announce Receipt Timeout: 3

Network Inaccuracy [ns]: 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 Paketgröße wie beim V1 Standard (0 ist Standard)
PTP Domain Number	[NUM,0:3]	Nummer einer logische Gruppe 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]	Priority 1 für Best Master Clock Algorithmus
PTP priority2	[NUM:0:255]	Priority 2 für Best Master Clock Algorithmus
PTP Sync Interval	[2 <sup>x</sup> ]:0	verwendet bei Multicast Master bzw. Unicast Slave
PTP Announce Interval	[2 <sup>x</sup> ]:1	verwendet bei Multicast Master bzw. Unicast Slave
PTP DelayRequest Interval	[2 <sup>x</sup> ]: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 korrekte 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
User defined Fix Offset positive	[BOOL]	1 = Positive Phasenverschiebung zur Referenzzeit
User defined Fix Offset [ns]	[NUM]	0-1000000 = Wert der Phasenverschiebung zur Referenzzeit

HQ Filter active	[BOOL]:0	Slave: aktiviere Filter für hohe Lasten/hoher Jitter
HQ Filter estimated accuracy [ns]	[NUM]:5000	Erwartete Genauigkeit, maximaler Jitter im Netzwerk
PDSC active	[BOOL]:0	Path Delay Step Compensation (1=Erkennung aktiv) (siehe dazu auch Kapitel ??)

## 8.6.2 PTP Netzwerk Konfiguration

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

**PTP V2 Konfiguration**

Schnittstelle 01: Netzwerk Global

**Netzwerk:**

Hostname  Domainname

Nameserver 1  Nameserver 2

---

DHCP-Client aktivieren Static ▾

TCP/IP-Adresse  Netzmaske

Default Gateway

---

IPv6 Mode Static ▾

IPv6-Adresse

---

VLAN-Funktion aktivieren

VLAN-Tag (1-4094)  Priorität 0 ▾

---

SSH Service deaktivieren

DSCP PTP Klassifizierung CUSTOM 00 (HEX: 00) ▾

Multicast TTL 5 ▾

### Inhalt der PTP Netzwerk - Konfigurationsdatei:

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 Adresse 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	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)

### 8.6.3 PTP Status Datei

In diesem Menü werden alle Statusinformationen der gewählten TSU angezeigt:

**PTP V2 Status**

Schnittstelle 01

**Aktueller Status**

TCP/IP-Adresse	192.168.100.10	Netzmaske	255.255.255.0
Eigene Mac-Adresse	EC:46:70:00:60:42	UUID	EC:46:70:FF:FE:00:60:42
PTP Mode	Multicast Slave	Domain Number	0
Port State	UNINITIALIZED	Port Link up	Nein
Grandmaster MAC	00:00:00:00:00:00	Delay Asymmetry	-0.0ns
Clock Accuracy	Unknown	Clock Class	0
PTP Seconds	0	Time Source	not defined
UTC Offset	0s	Leapsecond	Keine Ankündigung
TSU Time	ARB:01.01.70 00:00:00.000000;		

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

Clock variance : 13565

Grandmaster MAC : 00:60:6E:7C:27:2C

Number of clients : 0

Number of masters : 0

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

PTP timescale : PTP (TAI)

PTP time source : GPS

PTP UTC Offset : 34

PTP Leapsecond : 0

TSU Time: TAI:11.03.11 13:17:27.652680;

SYS Time: UTC:11.03.11 13:16:53.655558;

## 8.7 Konfiguration: System



### 8.7.1 Allgemeine Einstellungen

Hier kann eine Kontaktadresse, der Standort des Gerätes sowie die Sprache dieser Weboberfläche eingetragen und festgelegt werden. Mit aktivierter Checkbox werden alle Konfigurationsänderungen sofort als neue Startkonfiguration gespeichert.

### 8.7.2 Sprache des WEB-Interface

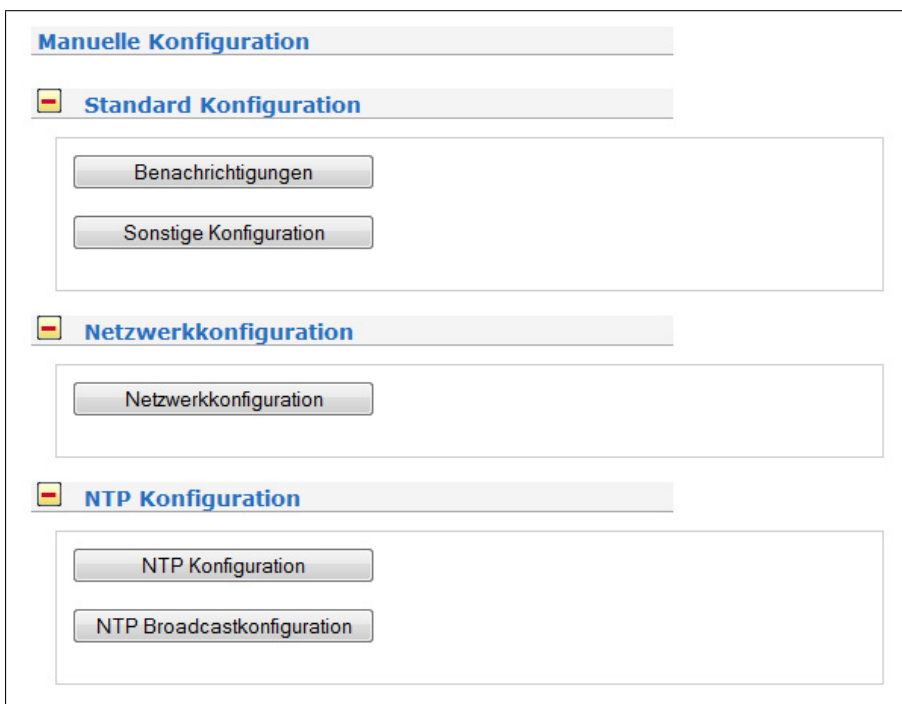
Über den Punkt „Sprache des WEB-Interface“ kann die Ausgabe der Texte in der HTTP Benutzerschnittstelle auf Deutsch oder Englisch eingestellt werden. Die Änderung erfolgt beim nächsten Neuladen der aktuellen Seite.

### 8.7.3 Dienste und Funktionen

Im ersten Abschnitt werden verschiedene Funktionen für den Administrator zur Verfügung gestellt. Über den Punkt „Gerät neustarten“ 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 „Testbenachrichtigung senden“ 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 sichern“ 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 wiederherstellen“ werden alle Einstellungen auf den Auslieferungszustand

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

Über den Punkt „SNMP MIB 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.



### 8.7.4 Benutzerverwaltung




Zur Administration des LANTIME können eigene Benutzer angelegt werden. Dabei werden 3 Benutzergruppen unterschieden. Die Gruppe „Super-User“ hat alle Rechte zur Administration. Der Super User kann alle Parameter über das Webinterface konfigurieren und hat Zugriff auf die Konsole über TELNET, SSH oder über die serielle Schnittstelle.

Die Gruppe Administrator kann nur über die Web-Benutzerschnittstellen Änderungen vornehmen. Somit hat der Administrator keinen direkten Zugriff auf Linux Befehle. Die Benutzergruppe Info kann lediglich Statusinformationen und Konfigurationsparameter über das Webinterface einsehen - eine Änderung der Einstellung ist nicht möglich.

The screenshot shows the 'Benutzerpasswort ändern' (Change User Password) form. It contains two input fields: 'Neues Passwort' (New Password) and 'Passwort wiederholen' (Repeat Password). A 'Passwort ändern' (Change Password) button is located to the right of the second input field.

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.

The screenshot shows the 'Benutzer anlegen' (Create User) form. It contains four input fields: 'Benutzername' (Username), 'Passwort' (Password), 'Passwort wiederholen' (Repeat Password), and 'Gruppenzugehörigkeit' (Group Membership). The 'Gruppenzugehörigkeit' field is a dropdown menu with 'Super-User' selected. A 'Benutzer anlegen' (Create User) button is located to the right of the dropdown menu.

 **Benutzerliste**

Benutzername	Gruppenzugehörigkeit	Option
root	Super-User	Benutzer löschen
MaxMuster	Admin-User	Benutzer löschen
MaxiMusterfrau	Info-User	Benutzer löschen

## Authentifizierung - Optionen

**Authentifizierung-Optionen**

Externe Authentifizierung verwenden

Timeout (ms)

**Externe Authentifizierung**

Authentifizierungsverfahren

Authentifizierungsserver

Schlüssel

Port

### Verschiedene Authentifizierungsmethoden können ausgewählt werden:

**TACACS:** Terminal Access Controller Access-Control System (TACACS) ist eine Remote-Authentifizierungsprotokoll welches dazu dient, mit einem Authentifizierungs-Server, der üblicherweise in UNIX-Netzwerken eingesetzt wird, zu kommunizieren.

Die LANTIME TACACS Authentifizierung erfordert es, dass jeder Account, der sich am LANTIME anmelden möchte, ein Attribut mit dem Namen „priv-lvl“ benötigt. Dieses Attribut muss auf dem TACACS Server definiert werden. Für „Super-User“ muss das Attribut den Wert 100 haben, für „Admin-User“ den Wert 200 und für „Info-User“ den Wert 300.

Zu beachten ist, dass das Attribut für den Service „lantime\_mgmt“ definiert werden muss - beispielsweise:

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

**RADIUS:** Remote Authentication Dial In User Service (RADIUS) ist ein Netzwerkprotokoll, welches zentralisierte Authentifizierung für Meinbergs Zeitserver bereitstellt, um sie mit anderen Netzwerkteilnehmern oder Diensten zu verbinden. RADIUS ist ein Client / Server-Protokoll, es läuft in der Anwendungsschicht unter Verwendung von UDP als Übertragungsprotokoll.

Die LANTIME Radius Authentifizierung erfordert es, dass jeder Account der sich am LANTIME anmelden möchte, ein sogenanntes Vendor Specific Attribute (VSA) mit dem Namen „MBG-Management-Privilege-Level“ benötigt. Dieses VSA muss in dem Dictionary des Radius Servers definiert werden. Zusätzlich muss jedem Benutzer auf dem Radius Server ein Wert für

dieses Attribut hinzugefügt werden. Für „Super-User“ muss das Attribut den Wert 100 haben, für „Admin-User“ den Wert 200 und für „Info-User“ den Wert 300.

## Passwort-Optionen

In diesem Abschnitt können spezielle Optionen aktiviert werden, um die Sicherheit der Benutzerpasswörter zu erhöhen.

### Mindest-Passwortlänge

Dieser Parameter legt fest, aus wievielen Zeichen ein Passwort mindestens bestehen muss, um vom System als gültiges Passwort akzeptiert zu werden. Der Parameter gilt für das Anlegen eines neuen Benutzers und für das Ändern eines bestehenden Benutzerpasswortes.

### Nur sichere Passwörter zulassen

Wenn aktiviert muss ein Passwort aus mindestens einem Kleinbuchstaben [a-z], einem Großbuchstaben [A-Z], einer Zahl [0-9] und einem Sonderzeichen bestehen.

### Liste der erlaubten Sonderzeichen:

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

### Passwort muss zyklisch geändert werden

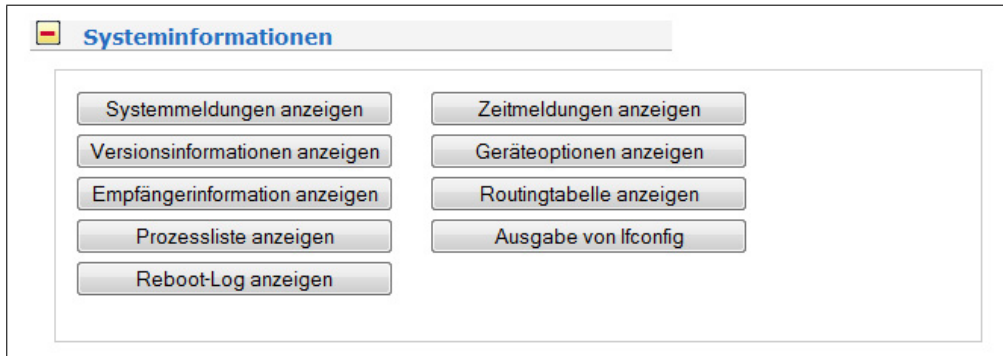
Benutzer werden automatisch aufgefordert das Passwort in regelmäßigen Abständen zu ändern. Ist ein Passwort abgelaufen, so kann sich der Benutzer nicht mehr anmelden bis es geändert worden ist.

### Verfügbare Intervalle:

```
Monatlich      = Alle 30 Tage  
Halbjährlich   = Alle 180 Tage  
Jährlich       = Alle 360 Tage
```

## 8.7.5 Systeminformationen

Über den Punkt „Systemmeldungen 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.



## 8.7.6 Systeminformationen anzeigen

**Systemmeldungen anzeigen:**

1-200      201-400      401-498

Text:

Zeige Einträge: 1-200

Date	Time	Host	Process	Message
Mar, 19	00:01:04	timeserver	crontab[4692]:	(root) REPLACE (root)
Mar, 19	00:01:04	timeserver	crond[4693]:	(CRON) INFO (pidfile fd = 3)
Mar, 19	00:01:04	timeserver	crond[4694]:	(CRON) STARTUP (fork ok)
Mar, 19	00:01:04	timeserver	crond[4694]:	(CRON) INFO (Running @reboot jobs)
Mar, 19		timeserver	ifplugd(lan0)[4758]:	ifplugd 0.28 initializing, using NETLINK device monitoring.
Mar, 19		timeserver	ifplugd(lan0)[4758]:	Using interface lan0/00:13:95:03:71:57 with driver (version: 1.36.4)

**Zeitmeldungen anzeigen:**

**Zeitmeldungen anzeigen:**

1-13

Text:

Zeige Einträge: 1-200

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

**Anzahl Einträge: 13**

Hier erscheint eine Liste von Zeitmeldungen, die durch ein bestimmtes Ereignis, wie etwa Server Reboot, Änderung der Konfiguration usw. eingetragen werden. Nach einem Neustart des Systems ist diese Liste gelöscht.

**Versionsinformationen anzeigen**

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

**Versionsinformationen anzeigen:**

```

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

```

## Geräteoptionen anzeigen

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

```
Geräteoptionen anzeigen:
#GLOBAL OPTIONS
NUMBER ETHERNET INTERFACES: 1
SYSTEM LAYOUT: 0
SYSTEM ADV LAYOUT: 0
SYSTEM LANGUAGE: 1
SYSTEM PARAMETER: server
SYSTEM DESIGN: 0
RTP PARAMETER:
REDUNDANT POWER SUPPLY:
NOTIFICATIONS:
ADV HTTP OPTION:
```

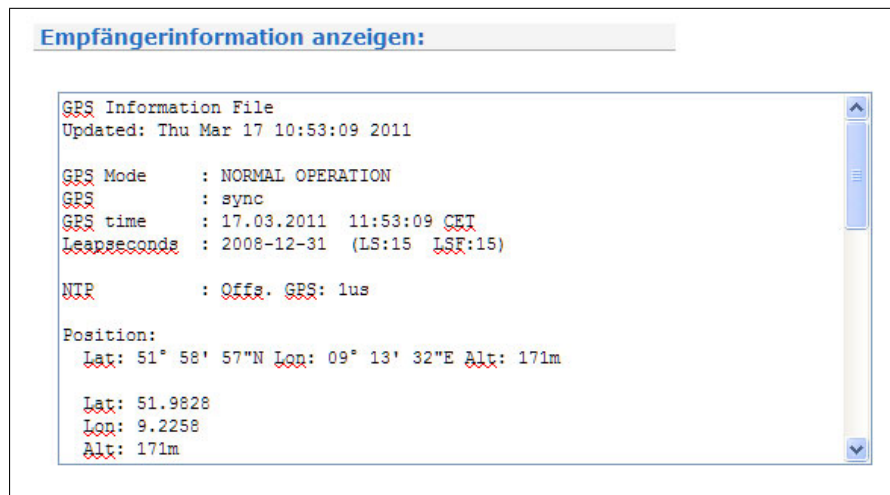


### Empfängerinformation anzeigen

Der Punkt „Empfängerinformation anzeigen“ zeigt empfängerspezifische Parameter. Der erste Parameter gibt Auskunft über den Zeitpunkt des letzten Updates der hier gezeigten Informationen.

#### Beispiel: GPS Empfänger

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).

**Hinweis:** Bei MRS Systemen werden auch die konfigurierten externen NTP Server angezeigt:

---

List of external NTP server:

```

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

---

In dieser Liste erscheint auch der momentan verwendete NTP Server (adjust).

## Routing Tabelle anzeigen

### Routingtabelle anzeigen:

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

Die Tabelle zeigt alle verfügbaren und konfigurierten Netzwerkrouen.

## Prozessliste anzeigen:

### Prozessliste anzeigen:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
31386	root	20	0	3916	1924	1572	R	33.8	1.9	0:00.18	ssh
31383	root	20	0	2256	936	736	R	3.8	0.9	0:00.03	top
5306	root	20	0	88672	2860	1020	S	1.9	2.8	40:41.72	lantimed
1	root	20	0	1740	576	504	S	0.0	0.6	0:01.58	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd

Hier wird eine Liste aller laufenden Prozesse der LAN-CPU angezeigt.

## Ausgabe von Ifconfig

### Ausgabe von Ifconfig:

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

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

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

## Reboot-Log anzeigen

### Show Reboot Log :

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

### 8.7.7 Software-/Firmwareupdate

Über den Punkt „Software-/Firmwareupdate“ 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 „Durchsuchen“ 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.



### 8.7.8 Diagnosedatei herunterladen

Eine Diagnosedatei, welche alle Status Daten eines LANTIME nach dem letzten Systemstart beinhaltet, kann über das Web-Interface heruntergeladen werden. Das Dateiformat der Diagnosedatei ist ein TGZ-Archiv. Dieses Archiv enthält alle wichtigen Konfigurationsinformationen und Log-Dateien. Bei vielen Supportfällen ist das Herunterladen der Diagnosedateien die erste Aktion, die direkt vom Benutzer ausgeführt werden kann. Es ist sehr hilfreich für unseren Technischen Support anhand dieser Dateien den aktuellen Status des Zeitservers zu ermitteln, um daraus Ursachen für aufgetretene Fehler ermitteln zu können.



#### Download der Diagnosedatei über das Web-Interface

1. Öffnen Sie die „System“ Seite und das Untermenü „Diagnose“.
2. Drücken Sie die Schaltfläche „Diagnose-Datei herunterladen“.
3. Senden Sie das Archiv mit einer kurzen Problembeschreibung an unseren Technischen Support: [techsupport@meinberg.de](mailto:techsupport@meinberg.de)

### 8.7.9 Diagnose Datei herunterladen

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

### 8.7.10 Konfiguration und Firmwareverwaltung

Mit diesem Menü kann die aktuelle Konfiguration gespeichert und auf dem LANTIME abgelegt werden. Damit können mehrere und unterschiedliche Konfigurationen gesichert werden, die dann auch jederzeit aktiviert werden können.

Außerdem können mehrere Firmwares auf dem Gerät archiviert werden. Nach einem Firmwareupdate kann also auch eine frühere Version wieder eingespielt werden. Die OSV ist die Auslieferungsfirmware und kann daher auch nicht gelöscht werden. Bei einem Factory Reset wird diese Version wieder aktiviert.

**Konfiguration & Firmwareverwaltung**

**Konfigurationsverwaltung**

Aktuelle Konfiguration speichern:

Konfiguration hochladen:

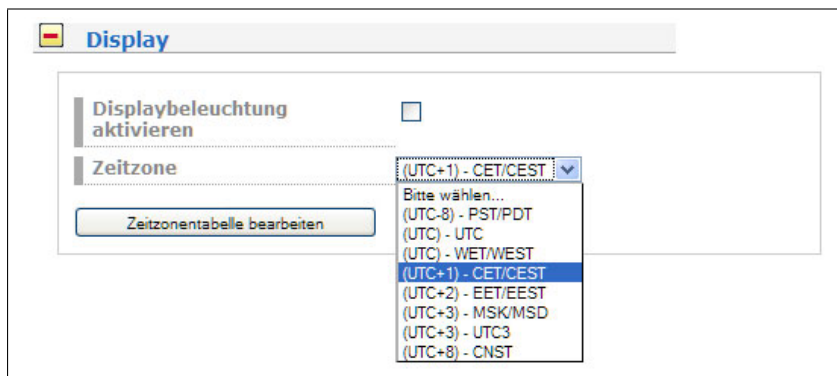
Gespeicherte Konfigurationen	Optionen		
startup	<input type="button" value="Aktivieren"/>	<input type="button" value="Löschen"/>	<input type="button" value="Herunterladen"/>

**Firmwareverwaltung**

Laufende Firmware OSV  
Aktivierte Firmware OSV

Gespeicherte Firmwares	Version	Optionen	
OSV (Auslieferungsfirmware)	6.13.035	<input type="button" value="Aktivieren"/>	<input type="button" value="Löschen"/>

### 8.7.11 Display



#### Zeitzonentabelle bearbeiten:

Mit diesem Menüpunkt kann die Zeitzonentabelle direkt bearbeitet werden. Die Tabelle kann mit der gewünschten Zeitzone ergänzt werden, um dann auch die lokale Zeit im Display korrekt anzeigen zu lassen.

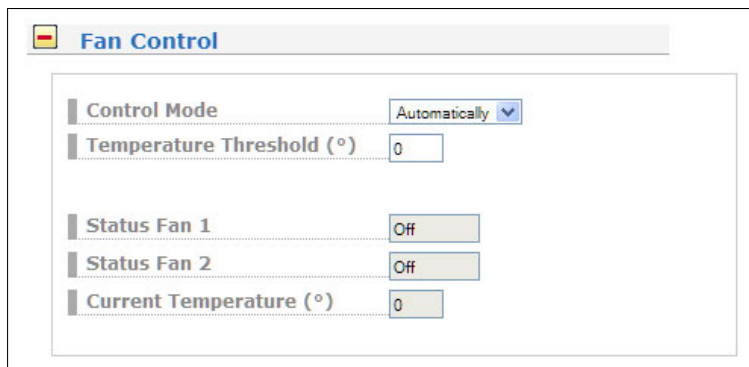
#### Beispiel:

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

Diese Zeit hat eine Abweichung von +1 Stunde von der UTC Zeit. Außerdem wird am 25.03. des Jahres um 2:00 Uhr auf Sommerzeit umgeschaltet - die Abweichung beträgt dann +2 Stunden. Die Umschaltung auf Normalzeit erfolgt dann am 25.10. um 3:00 Uhr.

Die Zeichenkette bis zum ersten Komma wird dann in der DropDown Auswahlliste als optionaler Wert angezeigt.

### 8.7.12 Option: Fan Control



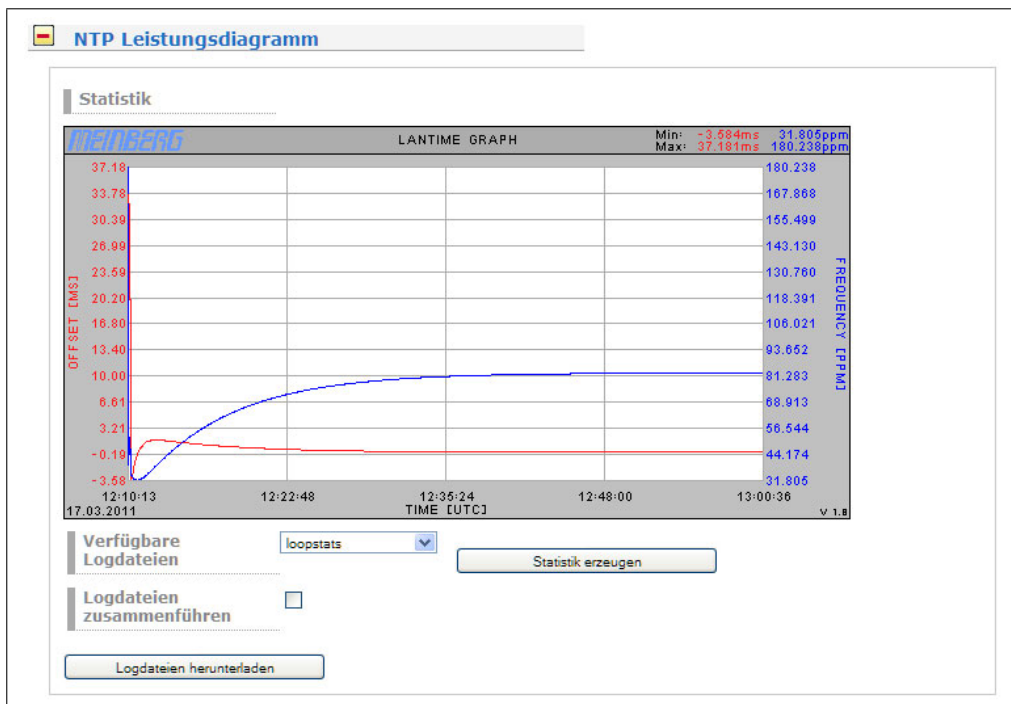
Mit dem optionalen Menü Fan Control wird der aktuelle Status der Ventilatoren angezeigt. Außerdem kann hier der Modus eingestellt werden:

- On** Die Ventilatoren laufen immer
- Off** Die Ventilatoren sind ausgeschaltet
- Automatisch** Die Belüftung läuft ab der Temperatur an, die durch den Parameter „Temperature Threshold“ festgelegt wird. Dieser Wert lässt sich nur nach Auswahl der Option „Automatisch“ eingeben. Die Temperatur des Gerätes muss erst den festgelegten Wert um ca. 7 Grad Celsius unterschreiten, damit die Ventilation automatisch abgeschaltet wird.

## 8.8 Konfiguration: Statistik



### NTP Leistungsdiagramm



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.

### Status des NTP

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

Remote	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
LOCAL(0)	.LOCL.	12	I	53m	8	0	0.000	0.000	0.000
oGENERIC(0)	.GPS.	0	I	5	8	377	0.000	0.001	0.002

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 geschiftet werden.
- delay: gemessene Verzögerung der Netzwerkübertragung (in Millisekunden)
- offset: Differenz zwischen Systemzeit und Referenzzeit (in Millisekunden)
- jitter: statistische Streuung des Offsets (in Millisekunden)

### NTP Monitor

Remote Address	Port	Local Address	Count	M	Version	Code	Avg Length	First/Last
172.16.100.124	123	172.16.100.167	1	3	4	0	57	57

### NTP Debug

Index	assID	Status	Conf	Reach	Auth	Condition	Last Event	Count
1	26059	8033	yes	no	none	reject	unreachable	3
2	26060	973a	yes	yes	none	pps.peer	sys_peer	3

assID: 0

assID: 26059

assID: 26060

### NTP Zugriffsstatistik

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.



### 8.8.1 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 Zeitserver zugriffen haben: also eine Liste aller NTP-Clients. Diese kann sehr lang werden. Benutzer, die lange nicht mehr auf den NTP zugriffen 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 geschiftet 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“.

## 8.9 Konfiguration Funkempfänger

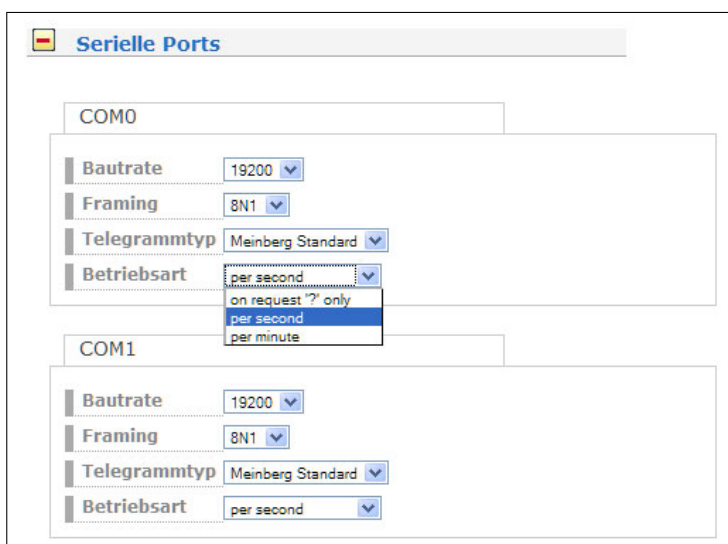


Auf dieser Seite können alle relevanten Einstellungen des verwendeten Empfängers vorgenommen werden.

### 8.9.1 Serielle Ports

Mit Hilfe dieses Untermenüs können Übertragungsgeschwindigkeit, Framing, Datenformat und Betriebsart der seriellen Schnittstelle eingestellt werden. Folgende Werte der seriellen Ausgänge sind bei Auslieferung voreingestellt:

Baudrate: 19200 baud,  
 Framing: 8N1  
 Telegrammtyp: Meinberg Standard Time String  
 Betriebsart: pro Sekunde



Der serielle COM Port gibt ein Zeittelegramm sekundlich, 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.

#### Auswählbare Telegramme

- Meinberg Standard
- SAT

- NMEA RMC
- Uni Erlangen
- Computime
- Sysplex 1
- Meinberg Capture
- SPA
- RACAL
- Meinberg GPS
- NMEA GGA
- NMEA RMC GGA
- NMEA ZDA
- ION

### 8.9.2 IRIG Settings

Mit IRIG Settings kann der Code der IRIG/AFNOR Ausgänge eingestellt werden:

B002+B122	IRIG-B 100PPS: DC Level Shift (DCLS), No carrier(DCLS), Kodierung der Zeit (HH,MM,SS,DDD) + Moduliert, 1 kHz / 1 millisecond resolution, Kodierung der Zeit (HH,MM,SS,DDD), Control Functions
B003+B123	wie B002+B122, mit Tagessekunde (0....86400)
AFNOR NF S87-500	AFNOR NFS 87-500 ist ein genormter französischer Timecode ähnlich dem IRIG Code, jedoch mit zusätzlichen Informationen wie Tag, Tag des Monats und Jahr.
IEEE1344	Neben einer zweistelligen Jahreszahl werden auch der Offset zur UTC-Zeit, der aktuelle Sommerzeit-Status und Ankündigungen von Beginn und Ende der Sommerzeit, sowie Informationen zu einer bevorstehenden Schaltsekunde übertragen.

### 8.9.3 MRS Einstellungen

Für die Auswahl einer Referenzzeit durch das System können Sie mit diesem Menü einige wichtige Parameter konfigurieren.

	Offset	Precision	Limit
GPS	0 ns	0 ns	0 ns
PPS in	0 ns	0 ns	0 ns
IRIG	0 ns	0 ns	0 ns
NTP	0 ns	0 ns	0 ns
PTP (IEEE1588)	0 ns	0 ns	0 ns
Fixed Freq. in	0 ns	0 ns	0 ns
PPS plus string	0 ns	0 ns	0 ns

Die Prioritäten für die verschiedenen Referenzen zur Steuerung des internen Oszillators kann mit diesem Untermenü eingestellt werden:

#### Festlegung der Eingangssignal - Priorität:

GPS	GPS Signal über interne Uhr
PPS in	PulsePerSecond Eingangssignal
IRIG	IRIG Time Code (DCLS/AM)
NTP	externer NTP Zeitserver
PTP (IEEE1588)	IEEE 1588 Grandmaster
Fixed Freq. in	Frequenzeingang

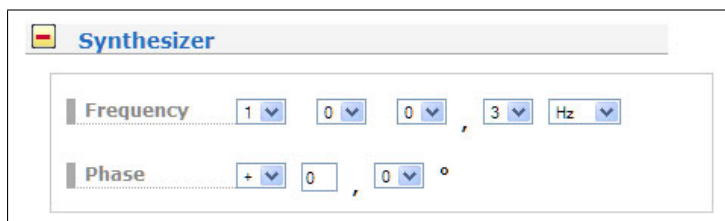
Mittels der Drop Down Boxen können die „Fixed Offsets“ und die „Precision“ ausgewählt werden. Der „Fixed Offset“ gibt für jede Referenzuhr einen festen Offset zur Referenzzeit an. Hiermit können bekannte und konstante Abweichungen einer Referenzzeitquelle kompensiert werden. Für die GPS Referenz kann kein konstanter Offset eingestellt werden – dies kann nur indirekt über die Antennenlänge gemacht werden.

Die „Precision“ gibt die Genauigkeit einer Referenzquelle an. Anhand dieser Genauigkeit werden die Umschaltzeiten zwischen den einzelnen Referenzen berechnet. Die Umschaltzeit ist die Verzögerung (Holdover Time) wenn bei einem Ausfall des aktuellen Masters auf eine andere Referenzquelle umgeschaltet werden soll. Bei einem „Precision“ Wert von Null wird sofort auf die nächste Referenzuhr in der Reihenfolge (Priorität) umgeschaltet. Ansonsten wird die Verzögerung nach der Formel „(new\_precision / old\_precision \* constant)“ berechnet.

Der Parameter „constant“ ist abhängig von der Genauigkeit des verwendeten internen Oszillators!

Beispiel: Das externe PPS Signal mit einer Genauigkeit von 100 Nanosekunden ist nicht mehr verfügbar. Es wird auf die nächste Referenz in der Prioritätenliste umgeschaltet, also in diesem Fall auf das IRIG Signal mit einer Genauigkeit von 10 Mikrosekunden (= 10000ns). Mit der Formel  $((10000\text{ns}/100\text{ns}) * 11.4 \text{ [s]})$  wird eine Umschaltzeit von 19 Minuten errechnet. Ist innerhalb dieser Zeit das PPS Signal wieder verfügbar, wird der Umschaltvorgang nicht durchgeführt.

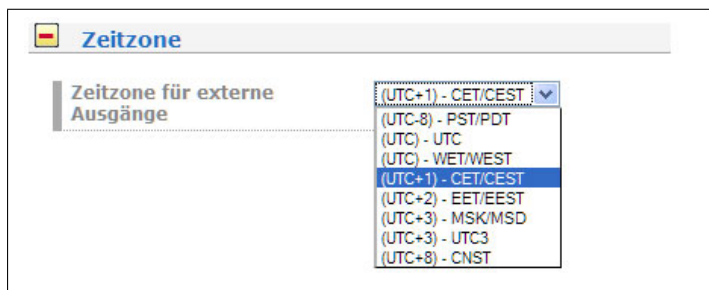
### 8.9.4 Synthesizer



Hier kann die Ausgangsfrequenz und Phase des eingebauten Synthesizers eingestellt werden. Frequenzen von 1/3 Hz bis zu 12 MHz sind durch Eingabe von vier Ziffern und einem Frequenzbereich einstellbar. Durch Eingabe der Frequenz 0 Hz kann der Synthesizer abgeschaltet werden.

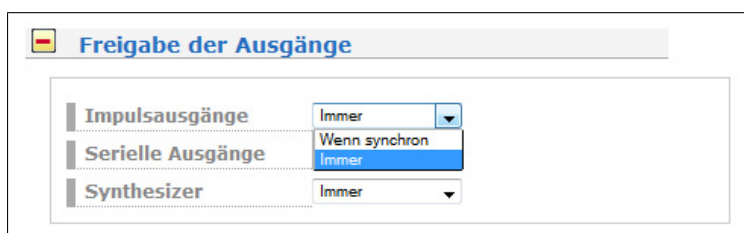
Mit Phase kann die Phasenlage der eingestellten Frequenz im Bereich  $-360^\circ$  bis  $+360^\circ$  mit einer Auflösung von  $0.1^\circ$  eingegeben werden. Bei Vergrößerung des Phasenwinkels wird das Ausgangssignal mehr verzögert. Falls eine Frequenz größer als 10 kHz eingestellt wurde, kann die Phase nicht geändert werden.

### 8.9.5 Zeitzone



Mit der DropDown Liste kann die Zeitzone für das Gerät ausgewählt werden. Die Liste kann im Menü „System -> Display -> Zeitzonentabelle bearbeiten“ noch um weitere Zonen erweitert werden.

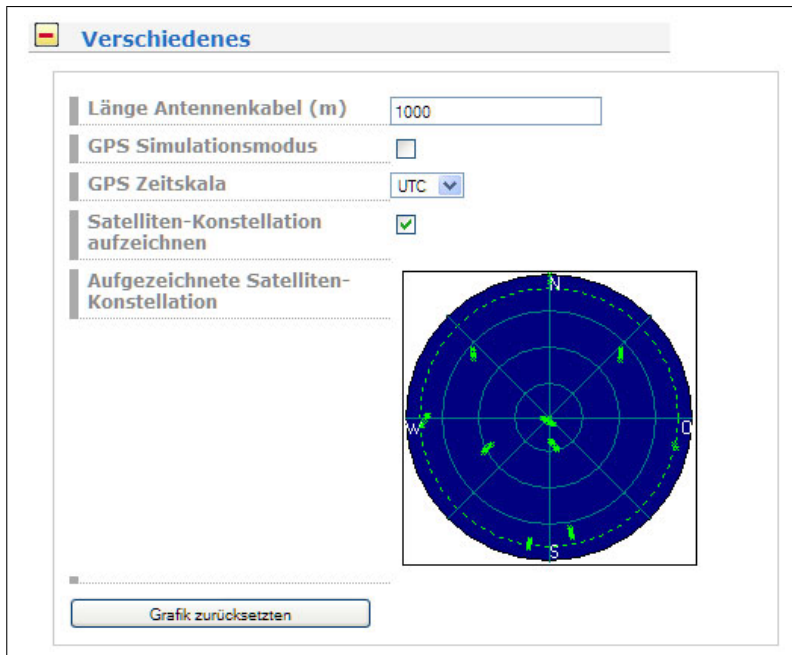
### 8.9.6 Freigabe der Ausgänge



Wahlweise können die Impuls- und seriellen Ausgänge so eingestellt werden, dass sie immer ein Signal liefern wenn das Gerät eingeschaltet ist, oder erst dann, wenn die interne Uhr synchron läuft.

## 8.9.7 Verschiedenes

### GPS Empfänger:



#### 1. Länge Antennenkabel

Die Signallaufzeit des Antennenkabels kann durch diesen Wert kompensiert werden. 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. Der maximale Eingabewert sollte 500m nicht überschreiten.

#### 2. GPS Simulationsmodus (GPS Empfänger)

Dieses Menü erlaubt es dem Benutzer, den Zeitserver 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 die Checkbox leer bleiben. Ist diese Box aktiviert, wird im Hauptmenü ein „\*“ hinter der Uhrzeit angezeigt.

#### 3. GPS Zeitskala (GPS Empfänger)

Folgende Werte können übernommen werden:

UTC - Koordinierte Weltzeit (Schaltsekunden sind eingerechnet)

GPS - seit 1. Januar 1980 - entspricht der TAI Zeitskala bis auf eine Konstante von 19 Sekunden (Schaltsekunden seit 1980)

TAI - seit 1. Januar 1900 - International Atomzeit (ohne Schaltsekunden)

#### 4. Satelliten Konstellation aufzeichnen (GPS Empfänger)

Ist dieser Punkt aktiv, wird eine Grafik generiert, auf der die Konstellation der sichtbaren Satelliten angezeigt wird.

## Init Receiver

### Warm Boot Modus (GPS Empfänger)

Dieses Menü erlaubt es dem Benutzer, den Empfänger in den WARM 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.

### Cold Boot Modus (GPS Empfänger)

Dieses Menü erlaubt es dem Benutzer alle GPS - Systemwerte zu initialisieren, d.h. alle gespeicherten Satellitendaten werden gelöscht. Bitte beachten Sie, dass der Receiver ungefähr 15 Minuten benötigt, um die Informationen der Satelliten neu einzulesen und den Cold Boot abzuschließen!

### Langwellenempfänger (DCF77, MSF, WWVB)

### Entfernung zum Sender

Der Menüpunkt „Entfernung zum Sender“ dient zur Eingabe der Senderentfernung in km und damit zur Laufzeitkompensation des eintreffenden PZF-Signals. Die Einstellung der Entfernung sollte möglichst präzise vorgenommen werden, da sie direkten Einfluss auf die absolute Genauigkeit des Zeitrasters hat.

### Simulationsmodus

Der LANTIME Zeitserver kann auch ohne Antenne betrieben werden. Normalerweise verliert der NTPD die Synchronisation zur Referenzuhr wenn das Eingangssignal abgezogen ist. 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 am LANTIME eingetragen wurden, an den NTPD zu übermitteln. Im Normalfall sollte dieser Punkt auf „disabled“ eingestellt sein. Ist diese Einstellung aktiviert, wird im Display - Hauptmenü „Simulations Mode“ im Status angezeigt.

### 8.9.8 Information des Empfängers

In diesem Menü werden alle wichtigen Informationen zur verwendeten Funkuhr und des internen Oszillators angezeigt.

 **Information des Empfängers**

Allgemeine Informationen des Empfängers

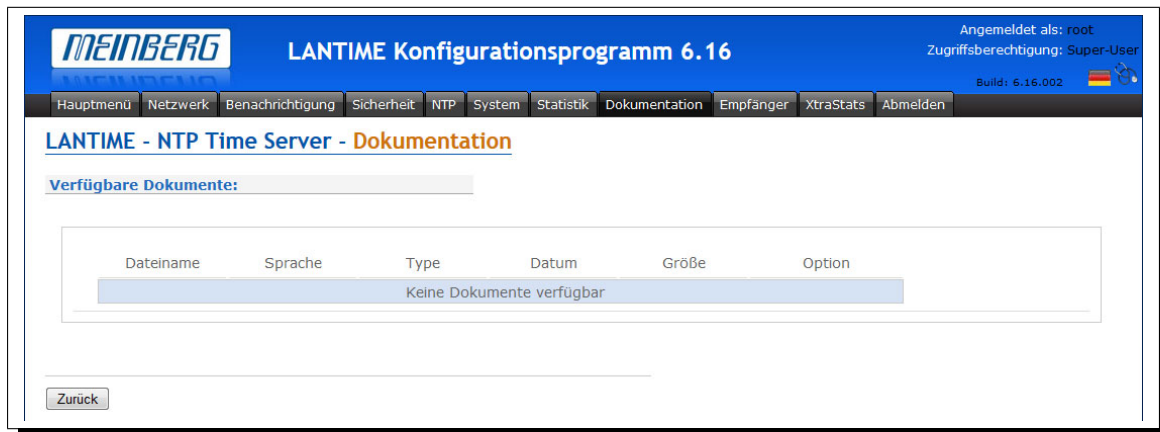
Name	Wert
Modell:	GPS170
Seriennummer:	029010012290
Software Revision:	ext. PPS sync
Oszillator Typ:	TCXO
Unterstützte Fähigkeiten:	Pulse Per Second, Pulse Per Minute, DCF77 Time Marks, Ignore Lock
Anzahl Programmierbarer Impulsausgänge:	0
Anzahl serieller Schnittstellen:	4

Spezielle Informationen des Empfängers

Name	Wert
GPS Status:	NORMAL OPERATION
GPS Position LLA:	Lat: 51.9828 Lon: 9.2258 Alt: 176m
GPS Position XYZ:	X:3885653m Y: 631133m Z:5001765m
Anzahl Satelliten in Sicht:	9
Anzahl brauchbarer Satelliten:	9
Verwendetes Satelliten-Set:	17 19 24 22



## 8.10 Konfiguration: Dokumentation



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.

**Verfügbare Dokumente:**

Dateiname	Sprache	Type	Datum	Größe	Option
m600_mrs_ptpv2	english	pdf	2011-12-07	5265.91kb	<a href="#">Anzeigen</a>
m600_mrs_ptpv2	german	pdf	2011-12-07	5869.14kb	<a href="#">Anzeigen</a>
2 Dokumente verfügbar					

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.

## 9 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.

## 9.1 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.

### 9.1.1 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](http://www.net-snmp.org)!

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

```
root@testhost:/# snmpwalk -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.

### 9.1.2 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.

### 9.1.3 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, HTTPS, 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 Benachrichtigungstypen 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).

### 9.1.4 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 Zeitserver
	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) aktiviert?
mbgLtCfgEMail	mbgLtCfgEMailTo	string (Liste von EMail-Adressen)	Eine oder mehrere EMail-Adressen(durch Semikolon getrennt), die Warnungen und Alarmmeldungen vom LANTIME per Mail empfangen sollen
	mbgLtCfgEMailFrom	string (EMail-Adresse)	Die EMail-Adresse, die als Absender der per Mail verschickten Warnungen und Alarmmeldungen verwendet wird
	mbgLtCfgEMailSmarthost	string (IPv4 oder IPv6-Adresse oder Hostname)	Der SMTP-Host, der für das Verschicken der per Mail verschickten Warnungen und Alarmmeldungen verwendet wird
mbgLtCfgSNMP	mbgLtCfgSNMPTrapReceiver1	string (IPv4 oder IPv6-Adresse oder Hostname)	Erster Rechner, der als SMTP-Traps verschickte Warnungen und Alarmmeldungen empfangen soll
	mbgLtCfgSNMPTrapReceiver1Community	string	Die SNMP Community, die beim Verschicken der SNMP-Traps an den ersten Rechner verwendet wird
	mbgLtCfgSNMPTrapReceiver2	string (IPv4 oder IPv6-Adresse oder Hostname)	Zweiter Rechner, der als SMTP-Traps verschickte Warnungen und Alarmmeldungen empfangen soll
	mbgLtCfgSNMPTrapReceiver2Community	string	Die SNMP Community, die beim Verschicken der SNMP-Traps an den zweiten Rechner verwendet wird
	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 Zeitserver
	mbgLtCfgSNMPLocation	string	Standortangaben (z.B. Gebäude/Raum) des Zeitserver
mbgLtCfgWinpopup	mbgLtCfgWMailAddress1	string	Erster Empfänger von per Windows Pop-up Messages verschickten Warnungen und Alarmmeldungen

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

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	mbgLtCfgEthernetIf0IPv4IP	string (IPv4 IP-Adresse)	IPv4-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0IPv4Netmask	string (IPv4 Netzmaske)	IPv4-Netzmaske des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0IPv4Gateway	string (IPv4 IP-Adresse)	IPv4-Adresse des Default Gateways des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0DHCPClient	integer (0 = disabled, 1 = enabled)	Konfiguration des ersten Netzwerkinterfaces des Zeitservers per DHCP aktiviert?
	mbgLtCfgEthernetIf0IPv6IP1	string (IPv6 IP-Adresse)	Erste IPv6-IP-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0IPv6IP2	string (IPv6 IP-Adresse)	Zweite IPv6-IP-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0IPv6IP3	string (IPv6 IP-Adresse)	Dritte IPv6-IP-Adresse des ersten Netzwerkinterfaces des Zeitservers
	mbgLtCfgEthernetIf0IPv6Autoconf	integer (0 = disabled, 1 = enabled)	IPv6 - Konfiguration des ersten Netzwerkinterfaces des Zeitservers per Autoconf aktiviert?
	mbgLtCfgEthernetIf0NetlinkMode	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.

## 9.2 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.

### 9.2.1 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.

# 10 Anhang: Technische Daten

## 10.1 Technische Daten LCES

GEHÄUSE:	Baugruppenträger, Schroff EUROPAC lab HF
EINGANGS- SPANNUNG:	100 ... 240 V AC (+/- 10%), 50/60Hz 100 ... 240 V DC (+/- 10%)
LEISTUNGS- AUFNAHME	max. 70 W
UMGEBUNGS- TEMPERATUR:	0 ... 50°C
SCHUTZART:	IP20
ABMESSUNGEN:	483mm x 132 mm x 275mm (B x H x T)

## 10.2 Front- und Rückwandanschlüsse

Bezeichnung	Steckverbindung	Art	Kabel / Verbindung
<b>Frontanschlüsse</b>			
Terminal	9pol. D-SUB Stecker	RS-232	Datenleitung geschirmt
USB	USB Port		USB-Stick
Netzwerk LAN	RJ-45	Ethernet	Datenleitung geschirmt
<b>Rückwandanschlüsse</b>			
Netzanschluss	Kaltger. Stecker	100-240 V AC	Kaltgeräteanschlusskabel
Refclock in	9pol. D-SUB Stecker	RS-232	Datenleitung geschirmt
PPS In	BNC Buchse	Pulse Per Second	Datenleitung geschirmt

## 10.3 LNE: Zusätzliche Ethernet-Schnittstellen für LANTIME Systeme

LANTIME Netzwerk Erweiterung LNE, zusätzliche Netzwerkschnittstellen für LANTIME Zeitserver

### Features

- Erweiterung des Lantime um zwei autarke Netzwerke 10/100MBIT
- Status-LEDs: Connect, Activity, Speed
- RJ45 Netzwerkanschlüsse in der Frontplatte

### Produktbeschreibung

Die Baugruppe LNE dient zur Erweiterung des NTP Timeservers Lantime um standardmäßig zwei (optional vier im Lantime/.../BGT) zusätzliche Netzwerkverbindungen. Somit stehen die Standardfunktionen des LANTIME weiteren physikalisch getrennten (autarken) Netzwerken zur Verfügung.

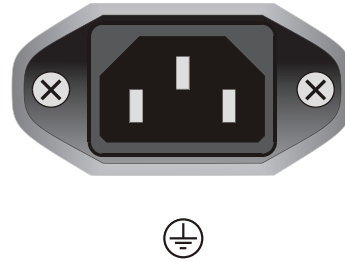
Auch für LANTIME - Modelle im 1HE Gehäuse kann bei Bestellung des Zeitservers eine LNE-Option mitbestellt werden, um zwei zusätzliche Ethernet-Schnittstellen zu erhalten. Die 1HE-LANTIMEs können somit mit maximal 3 Ethernet-Schnittstellen ausgerüstet werden.

Die zusätzlichen Netzwerkports können dazu genutzt werden, die Zeitsynchronisation in separaten Netzwerken zur Verfügung zu stellen. Es ist ebenfalls möglich, diese Ethernet-Ports per Bonding „zusammenzuschalten“, um eine redundante Netzwerkanbindung des Zeitservers zu erreichen (um diese Funktion zu nutzen, müssen die involvierten aktiven Netzwerk-Komponenten wie z.B. Switches diese Features unterstützen).



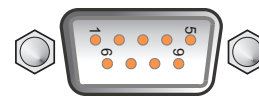
## 10.4 Anschluss Spannungsversorgung

<b>Eingangsspannung:</b>	100-240 V AC / 50-60Hz 100-240 V DC, (+/- 10%)
<b>Eingangsstrom:</b>	1 A <sub>max</sub>
<b>Sicherung:</b>	intern, T2.5 A / 250 V
<b>Anschluss:</b>	Netzseitig: IEC320 AC mit Zulentlastung



## 10.5 Refclock In

<b>Signal:</b>	Referenz, RS-232
<b>Steckverbinder:</b>	D-SUB Stecker 9pol.
<b>Kabel:</b>	Datenkabel (geschirmt) Verbindung PC: (Schnittstelle) 1:1
<b>Belegung:</b>	
Pin 1:	PPS (optional)
Pin 2:	TxD
Pin 5:	GND



Refclock In

## 10.6 PPS In

<b>Kabel:</b>	Koaxialkabel, geschirmt
<b>Impulslänge:</b>	5 $\mu$ s, active high
<b>Verbindungstyp:</b>	BNC-Buchse



PPS In

