



MANUAL

LANCPU

NTP Time Server Module

2010-07-22

Meinberg Radio Clocks GmbH & Co. KG

Table of Contents

1	Impressum	1
2	NTP Time Server Module	2
2.1	Technical Specifications LAN CPU	3
2.1.1	Rear Connector Pin Assignments LAN CPU	4
2.1.2	VGA, Keyboard Connector Pin Assignments	4
3	Network Time Protocol (NTP)	5
3.1	NTP Target	5
3.2	NTP-Client Installation	5
4	The graphical user interfaces	7
5	The WEB Interface	8
5.1	Configuration: Main Menu	8
5.2	Configuration: Ethernet	10
5.2.1	SYSLOG Server	10
5.3	Network interface specific configuration	11
5.3.1	IPv4 addresses and DHCP	11
5.3.2	IPv6 addresses and autoconf	12
5.3.3	High Availability Bonding	12
5.3.4	Additional Network Configuration	13
5.4	Configuration: Notification	14
5.4.1	Alarm events	14
5.4.2	E-mail messages	15
5.4.3	Windows Popup Messages	16
5.4.4	SNMP-TRAP messages	16
5.4.5	VP100/NET wall mount display	16
5.4.6	User defined Alarm scripts	16
5.4.7	NTP Client Monitoring	16
5.4.8	Alarm messages	17
5.5	Configuration: Security	18
5.5.1	Password	19
5.5.2	HTTP Access Control	19
5.5.3	SSH Secure Shell Login	19
5.5.4	Generate SSL Certificate for HTTPS	20
5.5.5	NTP keys and certificates	21
5.5.6	SNMP Parameter	21
5.6	Configuration: NTP	22
5.6.1	NTP Authentication	24
5.6.2	NTP AUTOKEY	25
5.7	Configuration: Local	28
5.7.1	Administrative functions	28
5.7.2	User Management	29
5.7.3	Administrative Information	30
5.7.4	Software Update	31
5.7.5	Automatic configuration check	32
5.7.6	Get Diagnostics Information	32
5.7.7	Web interface language	32
5.8	Configuration: Statistics	33
5.8.1	Statistical Information	33
5.9	Configuration: Manual	35

6	The Command Line Interface	36
6.1	CLI Ethernet	37
6.2	CLI Notification	39
6.3	CLI Security	41
6.4	CLI NTP Parameter	43
6.4.1	CLI NTP Authentication	44
6.5	CLI Local	44
7	SNMP Support	47
7.1	Configuration over SNMP	48
7.1.1	Examples for the usage of the SNMP configuration features	48
7.1.2	Further configuration possibilities	49
7.1.3	Send special timeserver commands with SNMP	49
7.1.4	Configuration of the timeserver with SNMP: Reference	51
7.2	SNMP Traps	55
7.2.1	SNMP Trap Reference	56

1 Impressum

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

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

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

Date: 2010-07-22

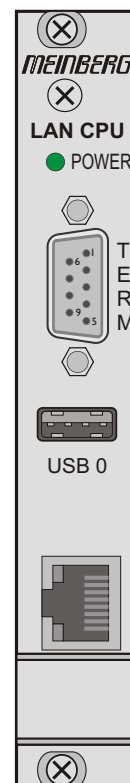
2 NTP Time Server Module

The Meinberg LANTIME CPU module transforms a Meinberg Radio Clock into a standalone "ready-to-run" NTP time server for TCP/IP networks, which comes with numerous possibilities for management and configuration: web interface (HTTP/HTTPS), text based setup (TELNET/SSH) and SNMP. To transfer files (e.g. Firmware-updates) to and from the device, FTP or SFTP/SCP can be used.

The IP address of the unit can be initially configured by using the front panel buttons of a GPS radio clock or by using a serial terminal connection. Alternatively, an integrated DHCP client allows assigning an IP address automatically.

The LANTIME CPU module can handle more than 1500 NTP requests per second, making it the first choice for providing accurate time information to large network with thousands of clients.

When developing the newest version, the main focus was on improvement of stability and security. Not only dealing with symmetric keys, the LANTIME CPU Module NTP server is also capable of using the autokey feature of NTP v4, providing the administrator with an easy way to maintain a reliable time source for large networks.



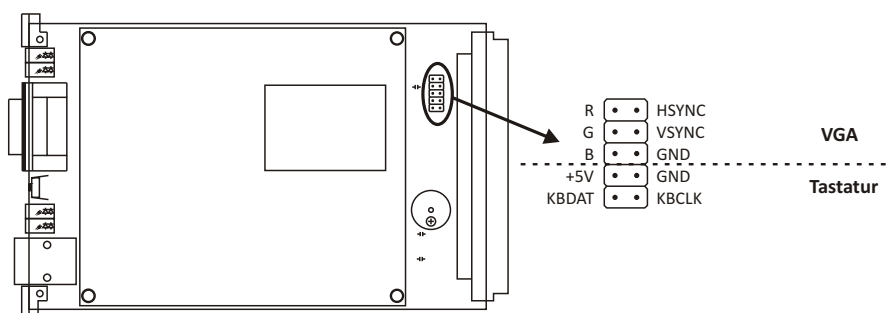
2.1 Technical Specifications LAN CPU

PROCESSOR:	Geode™ LX800 with 500 MHz
MAIN MEMORY:	128 MB
CACHE-MEMORY:	16 KB 2nd Level Cache
FLASHDISK:	512 MB
NETWORK CONNECTOR:	10/100 MBIT with RJ45-Jack
SERIAL - INTERFACE:	Four serial RS232-Ports 16550 compatible to FIFO <ul style="list-style-type: none">- RS232 9-pol. DSUB-male connector- three RS232 male connector according to DIN 41612, type C 96 (only TxD, RxD, DCD)
PARALLEL INTERFACE :	One LPT-Port male connector type C 96
VGA-CONNECTION:	10-pol pin contact strip
KEYBOARD CONNECTION:	10-pol pin contact strip
STATE LEDs:	<ul style="list-style-type: none">- power supply- 'Connect', 'Activity' and 'Speed' of the network connection
POWER REQUIREMENTS:	5 V +- 5 %, @ 1 A
FRONTPANEL:	3 HE / 4 TE (128 mm high x 20,3 mm wide)
CONNECTOR:	According to DIN 41612, type C 96, rows a+b+c (male) DSUB-plug (9-pol) RJ45-jack, USB Port
AMBIENT TEMPERATURE:	0 ... 50 °C
HUMIDITY:	85 % max.

2.1.1 Rear Connector Pin Assignments LAN CPU

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

2.1.2 VGA, Keyboard Connector Pin Assignments



3 Network Time Protocol (NTP)

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

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

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

3.1 NTP Target

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

<http://www.eecis.udel.edu/~ntp/>

You can find more information on our web page at:

<http://www.meinberg.de/english/sw/ntp.htm>

3.2 NTP-Client Installation

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

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

configure

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

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

make

While compiling the NTP daemon several warnings may appear. These warnings are mostly unimportant. In case of problems during the compilation read the system dependent notes in the subdirectory 'html'.

Afterwards the generated programs and tools have to be moved in the corresponding directories. Therefore type:

make install

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

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

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

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

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

Shows the last lines from the file `messages`. The status messages can also be redirected in a log file by using the following option:

ntpd -llogfile

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

e.g.: ntpq/ntpq

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

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

with the following meaning:

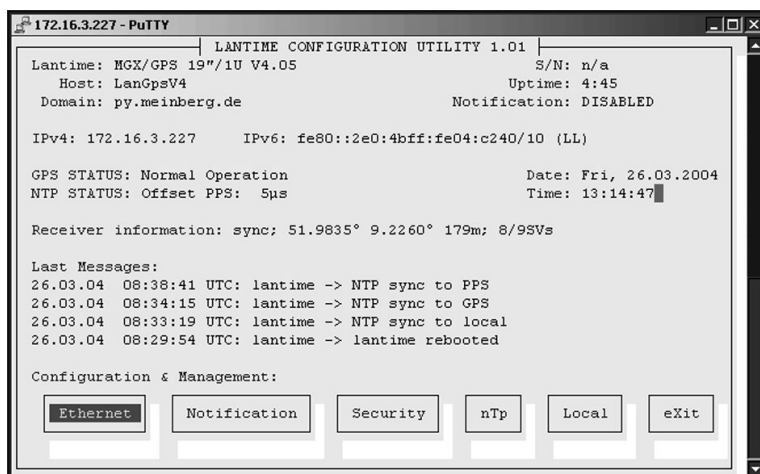
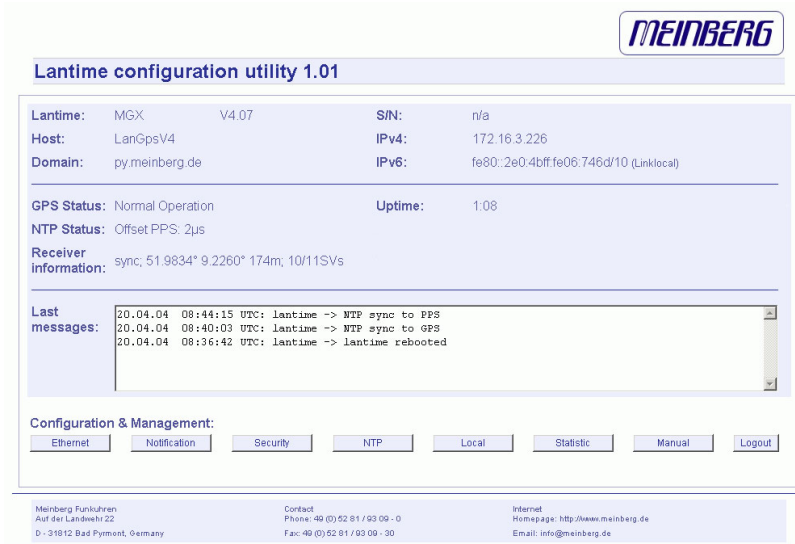
- remote: list of all valid time servers (ntp.conf)
- refid: reference number
- st: actual stratum value (hierarchy level)
- when: last request (seconds)
- poll: period of requesting the time server (seconds)
- reach: octal notation of the successful requests, shifted left
- delay: delay of the network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

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

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

4 The graphical user interfaces

The LANTIME offers three different options for configuration and status management: Web interface, Command Line Interface Setup and SNMP. In order to use the SNMP features of your LANTIME, you need special software like management systems or SNMP clients. In order to use the web interface, all you need is a web browser (LANTIME supports a broad range of browsers).



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

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

The above screen shots show the web interface and the Command Line Interface setup tool. The CLI setup tool cannot be used by more than one user at a time, the web interface can be used by more than one user in parallel, but the two or more running sessions may influence each other. We explicitly do not recommend the parallel usage of the configuration interfaces.

5 The WEB Interface

Connect to the web interface by entering the following address into the address field of your web browser:


<http://198.168.10.10>

(You need to replace 198.168.10.10 with the IP address of your LANTIME).

If you want to use an encrypted connection, replace the `http://` with `https://` in the above address. You may be prompted to accept the SSL certificate of your LANTIME the first time you are connecting to the system via HTTPS. In both HTTP and HTTPS mode, you will see the following login screen:

GPS controlled NTP time server

GPS:	NORMAL OPERATION	Time:	UTC 09:58:53
NTP:	Offs. PPS:-1us	Date:	Wed, 29.04.2009
Host:	LantimeV5	IP:	172.16.3.209
Contact:	Meinberg	Location:	Germany



Login for configuration and statistic

User:

Password: login

On this start page you see a short status display, which corresponds with the LC display on the front panel of the LANTIME unit. The upper line shows the operation mode of the receiver.

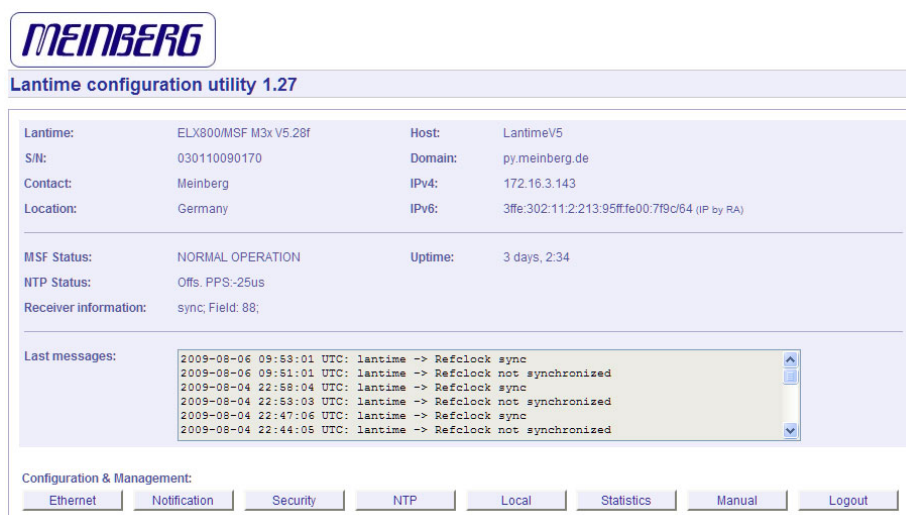
In the upper right corner of the LC display the time and time zone can be found, below that you will find the date and day of the week. On the second line the systems reports the NTP status. During the initial synchronisation process a "NTP: not sync" indicates that the NTP system is not synchronised with the receiver, this can also appear if the receiver loses synchronisation and the NTP switches back to its "LOCAL CLOCK" time source.

The receiver is connected to the LANTIME system internally by using a serial connection and additionally by using the second pulse. There are therefore 2 references used by NTPD, the receiver (GPS, PZF,...) and PPS time source. You will find the two time sources in the status information of the NTPD. After the NTP is synchronised, the display shows "NTP: Offset GPS [PZF,MSF,WWV,TCR]: x" or "NTP: Offset PPS: x" where "x" is the actual offset to the receiver or PPS time source.

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

5.1 Configuration: Main Menu

After entering the right password, the main menu page shows up. This page contains an overview of the most important configuration and status parameters for the system.



MEINBERG

Lantime configuration utility 1.27

Lantime:	ELX800/MSF M3x V5.28f	Host:	LantimeV5
S/N:	030110090170	Domain:	py.meinberg.de
Contact:	Meinberg	IPv4:	172.16.3.143
Location:	Germany	IPv6:	3ffe:302:11:2:213:95ff:fe00:7f9c/64 (IP by RA)

MSF Status:	NORMAL OPERATION	Uptime:	3 days, 2:34
NTP Status:	Offs. PPS-25us		
Receiver information:	sync; Field: 88;		

Last messages:

```

2009-08-06 09:53:01 UTC: lantime -> Refclock sync
2009-08-06 09:51:01 UTC: lantime -> Refclock not synchronized
2009-08-04 22:59:04 UTC: lantime -> Refclock sync
2009-08-04 22:53:03 UTC: lantime -> Refclock not synchronized
2009-08-04 22:47:06 UTC: lantime -> Refclock sync
2009-08-04 22:44:05 UTC: lantime -> Refclock not synchronized
  
```

Configuration & Management:

[Ethernet](#)
[Notification](#)
[Security](#)
[NTP](#)
[Local](#)
[Statistics](#)
[Manual](#)
[Logout](#)

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

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

The third section shows the last messages of the system, with a timestamp added. The newest messages are on top of the list. This is the content of the file `/var/log/messages`, which is created after every start of the system (and is lost after a power off or reboot).

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

5.2 Configuration: Ethernet

Ethernet configuration

Main network information:

Hostname:

Domainname:

Nameserver 1:

Nameserver 2:

Syslogserver 1:

Syslogserver 2:

Default Gateways:

IPv4 Gateway:

IPv6 Gateway:

Available network services:

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

Available internet protocols:

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

Available network interfaces: 2

Interface 0:

TCP/IP address:

Netmask:

DHCP-Client: ☒

Net link mode:

High availability bonding:

IP from DHCP:

Gateway from DHCP:

Netmask from DHCP:

Indicate Link on Front Panel LED: ☒

IPv6 1:

IPv6 2:

IPv6 3:

Autoconf: ☒

IP by Router Advertisement:

Link local:

Additional network configuration:

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

5.2.1 SYSLOG Server

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

to create entries. A Linux SYSLOGD can be told to do so by using the command “syslogd -r” when starting the daemon.

If you enter nothing in the SYSLOG server fields or specify 0.0.0.0 as the SYSLOG servers addresses, the remote SYSLOG service is not used on your LANTIME.

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

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

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

The third section allows you to select the IP protocol version 6. In this version the IPv4 protocol is mandatory and cannot be disabled, but as a workaround a standalone IPv6 mode can be achieved by entering an IPv4 address “0.0.0.0” and disabling the DHCP client option for every network interface of your LANTIME. By doing so, you ensure that the timeserver cannot be reached with IPv4. Please note that TELNET, FTP and NETBIOS cannot be used over IPv6 in this version. It is no problem to use IPv4 and IPv6 in a mixed mode environment on your LANTIME.

5.3 Network interface specific configuration

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

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

5.3.1 IPv4 addresses and DHCP

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

Example: 192.168.10.2

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

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

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

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

5.3.2 IPv6 addresses and autoconf

You can specify up to three IPv6 addresses for your LANTIME timeserver. Additionally you can switch off the IPv6 autoconf feature. IPv6 addresses are 128 bits in length and written as a chain of 16bit numbers in hexadecimal notation, separated with colons. A sequence of zeros can be substituted with "::" once.

Examples:

"::" is the address, which simply consists of zeros
 "::1" is the address, which only consists of zeros and a 1
 as the last bit. This is the so-called host local address
 of IPv6 and is the equivalent to 127.0.0.1 in the IPv4 world

"fe80::0211:22FF:FE33:4455" is a typical so-called link local
 address, because it uses the "fe80" prefix.

In URLs the colon interferes with the port section, therefore
 IPv6-IP-addresses are written in brackets in an URL.
 ("http://[1080::8:800:200C:417A]:80/" ;
 the last ":80" simply sets the port to 80, the default http port)

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

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

5.3.3 High Availability Bonding

The standard moniker for this technology is IEEE 802.3ad, although it is known by the common names of trunking, port trunking, teaming and link aggregation. The conventional use of bonding under Linux is an implementation of this link aggregation.

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

5.3.4 Additional Network Configuration

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

Ethernet configuration

Content of /mnt/flash/config/netconf.cmd:

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

Save file

Close

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

Ethernet configuration

Content of /mnt/flash/config/samba/smb.cnf:

```
# smb.conf is the main samba configuration file.  
[global]  
    workgroup = MEINBERG  
    map to guest = Bad User  
    os level = 2  
    time server = Yes  
    unix extensions = Yes  
    encrypt passwords = Yes  
    log level = 1  
    syslog = 0  
    printing = CUPS
```

Save file

Close

5.4 Configuration: Notification

Notification management

Email information:

To address:

Other recipients

From address:

Smarthost:

Windows messenger information (WinPopup):

Mail address 1:

Mail address 2:

SNMP information:

SNMP manager 1:
Community:

SNMP manager 2:
Community:

SNMP manager 3:
Community:

SNMP manager 4:
Community:

VP100/NET display information:

Display 1:
Serial number:

Display 2:
Serial number:

User defined notification:

Show user defined notification script
Edit user defined notification script

NTP client monitoring:

Show client list
Edit client list

NTP client offset limit:
10 ms
Show client status

NTP client stratum limit:
10

Notification conditions:

Condition:	Email	Wmail	SNMP	VP100/NET	User	Relais
Normal Operation	<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"/>
NTP stopped	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Server boot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receiver not responding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receiver not sync	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receiver sync	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Config changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTP client offset limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Edit messages

Save settings
Reset changes
Back

5.4.1 Alarm events

On this page you can set up different notification types for a number of events. This is an important feature because of the nature of a timeserver: running unobserved in the background. If an error or problem occurs, the timeserver is able to notify an administrator by using a number of different notification types.

The LANTIME timeserver offers different ways of informing the administrator or a responsible person about

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

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



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

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

- mbgLtTrapConfigChanged
- mbgLtTrapLeapSecondAnnounced
- mbgLtTrapServerBoot

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

5.4.2 E-mail messages

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

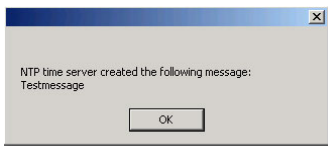
These settings cannot be altered with the LC display buttons of the front panel. Please note the following:

- The host name and domain name should be known to the SMTP smarthost
- A valid nameserver entry is needed
- The domain part of the "From:" address has to be valid

5.4.3 Windows Popup Messages

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

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



5.4.4 SNMP-TRAP messages

Up to two SNMP trap receiver hosts can be configured in this subsection, you may use IPv4 or IPv6 addresses or specify a hostname. Additionally you have to enter a valid SNMP community string for your trap receiving community. These can be unrelated to the SNMP community strings used for status monitoring and configuration access (see SNMP configuration on the "Security" page).

5.4.5 VP100/NET wall mount display

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

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

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

5.4.6 User defined Alarm scripts

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

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

5.4.7 NTP Client Monitoring

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

Notification management

Please insert up to 100 client address to monitor in a separate line

Content of /mnt/flash/config/clients_to_manage:

Save file

Close

You can monitor the current states of the configured clients:

5.4.8 Alarm messages

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

Notification management

Notification conditions: please adjust the messages to fulfill your needs

Condition:	Adjusted condition:
Normal Operation	
NTP not sync	
NTP stopped	
Server boot	
Receiver not responding	
Receiver not sync	
Receiver sync	
Config changed	
NTP client offset limit	
Default messages	

Save settings

Reset changes

Back

5.5 Configuration: Security

Security management

Login:

Config HTTP access control

Front Panel:

Lock Front Panel:
Deactivated

SSH key generation:

Generate SSH key
Show SSH key

HTTPS certificate generation:

Generate SSL certificate for HTTP
Show SSL certificate for HTTP

Durchsuchen...

Upload HTTPS certificate
Download HTTPS certificate

NTP autokey generation:

Generate new NTP public key
Generate groupkey

Durchsuchen...

Upload groupkey

NTP autokey password:

NTP symmetric keys:

Show NTP MD5 keys
Edit NTP MD5 keys

SNMP:

Read community String:
public

Read/Write community string:

SNMP contact:
Meinberg

SNMP location:
Germany
[Please edit these values on the local page](#)

User name:
root

Authentication passphrase:

Re-enter passphrase:
Change SNMP v3 authentication

Save settings
Reset changes
Back

5.5.1 Password

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

5.5.2 HTTP Access Control

Security management

HTTP access control:

Authorised TCP/IP addresses:

no access control currently configured

With this function you can restrict the access to the web interface and allow only a few hosts to login. Only the hosts you entered in the list are able to login to the HTTP/HTTPS server of your LANTIME.

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

GPS controlled NTP time server

Access denied - no authorization for log in from 172.16.3.20

GPS:	NORMAL OPERATION	Time:	UTC 10:00:52
NTP:	Offs. PPS: 2us	Date:	Fri, 21.08.2009
Host:	LantimeV5	IP:	172.16.3.153
Contact:	Meinberg	Location:	Germany

Login for configuration and statistic

User:

Password:

5.5.3 SSH Secure Shell Login

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

ssh root @ 192.168.16.111

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

Default Password: **timeserver**

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

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

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

Security management

Content of /tmp/ssh_key_output:

```
SSH V1 Host Key:
2048 35
2046797880213292523725036095625287622861135303504214341498207888544842325389250575506090209169422266
root@LantimeV5
-----
SSH V2 Host RSA Key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAzcXUTSvEQeWQ8qaGJLuj2E6+eDvzIV4cqruftCLJKexia3W6komT6gKt3kbG4yNf0Ni8R117
```

Close

5.5.4 Generate SSL Certificate for HTTPS

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

By using the button "Generate SSL certificate for HTTP" you can create a new certificate. Please enter your organisation, name, mail address and the location in the upcoming form and press "Generate SSL certificate" to finally generate it.

Generate HTTPS certificate

Please fill out the following fields:

Country Name(*): (2 letter code)

Locality Name(*):

Organization Name(*):

Organizational Unit:

Common Name(*):

Email Address(*):

☐ Generate Diffie-Hellman parameter

Fields marked with * are mandatory

Generate SSL certificate

Back

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

Security management

Content of /www/llnetmp:

```
-----BEGIN RSA PRIVATE KEY-----
MIICbwIBAAKBggQCM2KDSk88DvYv4RyISX2bcS1d3hEaf2heQPhetCqmBWqQh
dvd3qJlvyE3eaXk471o5EzExrxRhOIxKqHvRuU2T1v12uWQb1VohrLH+Vyd
jWzEO+zVQzSL2A1176688ZuP8og891XmM7aDMu+5WhZHQzrRy/Je+VbsewIDAQAB
AoQAMTEv46QvBBA2DvZ8m4s8Mjx+3a51zWU/4el69c1V198OT000b8e6
DCJcOFCt4M1aB+A0jz1F+DIHtP2W7v1z21GzrtcXNEJNqae1MzOh/86a5Y1SV3/
OKCdbdVGL5CGUo2nqf/OfoawA881ItvYJDIEChfXJYp9kCQQDtcK2kgLSf21ly
kgHactx4qlnA4g9SklyFKXQDgQz34h/epJOsoXmpICTY5vMcWbtp/Sh18TDkvf
rpJQRHnVAkAyroFOuP8JUTbvs06C80W1g9IC/m2h44dJOUscRu39wG2euzndM
QYUk4s8Paa8862QbWY8m5UULS7v87ZuJAEspHvvi5J6GjkgKfKmdDUT9CCSG
MkcK3FXbK11FaMnyGL2P187nR25uBuXrCNwupN2Axi1+A1JpXsSN3QUA2kc6
```

Close

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

5.5.5 NTP keys and certificates

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

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

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

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



5.5.6 SNMP Parameter

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

5.6 Configuration: NTP

NTP management

NTP configuration:

External NTP server address 1:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey
External NTP server address 2:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey
External NTP server address 3:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey
External NTP server address 4:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey
External NTP server address 5:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey
External NTP server address 6:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey
External NTP server address 7:	<input style="width: 90%;" type="text"/>	Key:	<input style="width: 90%;" type="text"/>	<input type="checkbox"/> use autokey

Stratum of local clock:

☐ disable local clock

Local trusted key:

NTP broadcast address: Key: ☐ use autokey

Broadcast interval: seconds

NTP trusttime: Days ☒ 0=Standard receiver trust time used (4 days)

	Autokey	PPS
Active:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Edit additional NTP parameter
Show current NTP configuration

Config NTP access control

Save settings
Reset changes
Back

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

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your LANTIME system and the GPS reference clock. The local clock is only chosen as the NTP time reference after the GPS clock lost its synchronisation. The stratum level of this local clock is set to 12, this ensures that clients recognise the switchover to the local clock and are able to eventually take further actions. The local clock can be disabled if the timeserver should not answer any more when the reference clock is out of order.

Because the reference clock is internally connected to the LANTIME system by using a serial connection, the accuracy using this way of synchronisation is around 1 ms. The high accuracy of the LANTIME timeserver (around 10 microseconds) is available by using the ATOM driver of the NTP subsystem, which is directly interpreting the PPS (pulse per second) of the GPS reference clock. The default configuration looks like this:

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

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

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

```
statistics loopstats
driftfile /etc/ntp.drift
```

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

By using the NTP configuration page, a number of additional parameters can be added to this default ntp.conf. In the upper section up to five external NTP servers can be set up to provide a high grade of redundancy for the internal reference clock. For each of these external NTP servers the AUTOKEY or symmetric key feature of NTP can be used to ensure the authentic of these time sources. The “Prefer” flag can be set for each external server. The internal refclock has set this flag by default. The “Prefer” flag is usefull if one of the refclocks are not available or out of sync.

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

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

If you want to use your LANTIME timeserver to send NTP broadcast packets to your network, you have to enter a valid broadcast address in “NTP broadcast address”. If you want to use IPv6 multicast mode, you have to enter a valid IPv6 multicast address in this field. Please note that NTP Version 4, which is used by the LANTIME timeserver, only permits authenticated broadcast mode. Therefore you have to set up the AUTOKEY feature or a symmetric key if you use a NTPv4 client and want to broadcast / multicast your time. A sample configuration of the NTP client for broadcast with symmetric keys looks like:

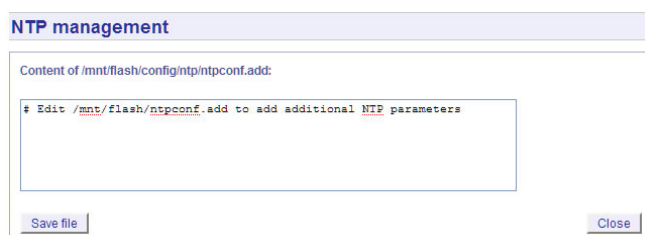
```
broadcastclient yes
broadcastdelay 0.05      # depends on your network
keys /etc/ntp/keys
trustedkey 6 15
requestkey 15
controlkey 15
```

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

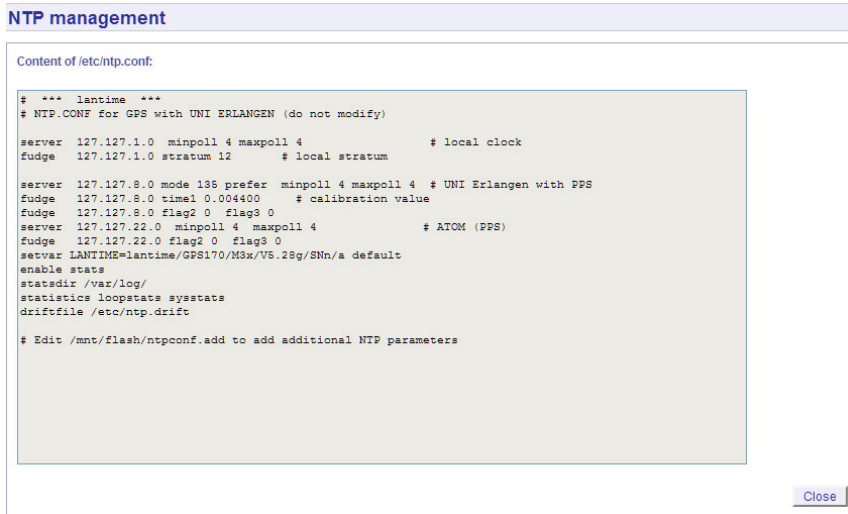
The NTP Trusttime will specify the time how long the NTP will trust the reference time if this is not synchronized (free running). This time will be set in seconds or minutes or hours. The value 0 will be select the default value for the specific reference clock. The default values are:

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

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



By choosing “Show current NTP configuration”, you can review the actual state of the `/etc/ntp.conf` file. The file cannot be changed on this page, see above for a description why editing this file is not reasonable.



5.6.1 NTP Authentication

NTP version 2 and version 3 support an authentication method using symmetric keys. If a packet is sent by the NTPD while using this authentication mode, every packet is provided with a 32 bit key ID and a cryptographic 64/128 bit checksum of the packet. This checksum is built with MD5 or DES, both algorithms offer a sufficient protection against manipulation of data.

Please note that the distribution of DES in the United States of America and Canada is subject to restrictions, while MD5 is not affected by that. With any of these algorithms the receiving NTP clients validate the checksum. Both parties (server and client) need to have the same crypto key with the same key ID.

In the authentication mode a party is marked “untrusted” and not suitable for synchronisation, whenever unauthorised packets or authorised packets with a wrong key are used. Please note that a server may recognise a lot of keys but uses only a few of them. This allows a timeserver to serve a client, who is demanding an authenticated time information, without “trusting” the client.

Some additional parameters are used to specify the key IDs used for validating the authentic of each partner. The configuration file `/etc/ntp.conf` of a server using this authentication mode may look like this:

```
# peer configuration for 128.100.100.7
# (expected to operate at stratum 2)
# fully authenticated this time

peer 128.100.49.105 key 22 # suzuki.ccie.utoronto.ca
peer 128.8.10.1 key 4 # umd1.umd.edu
peer 192.35.82.50 key 6 # lilben.tn.cornell.edu

keys /mnt/flash/ntp.keys # path for key file
trustedkey 1 2 14 15 # define trusted keys
requestkey 15 # key (mode 6) for accessing server variables
controlkey 15 # key (mode 7) for accessing server variables
```

The “keys” parameter indicates the location of the file, in which all symmetric keys are stored. The “trustedkey” line identifies all key IDs, which have to be considered “trusted” or “uncompromised”. All other keys defined in the keyfile are considered “compromised”. This allows to re-use already owned keys by just adding their respective key ID to the “trustedkey” parameter. If a key needs to be “switched off”, it can be removed from this line without actually removing it from the system. This ensures an easy way to re-activate it later without actually transferring

the key again.

The line “requestkey 15” declares the key ID for mode-6 control messages (as described in RFC-1305), which are used by the ntpq utility for example. The “controlkey” parameter is specifying the key used for mode-7 private control messages, for example used by the ntpdc utility. These keys protect the ntpd variables against unauthorised modification.

The ntp.keys file mentioned above holds a list of all keys and their respective ID known by the server. This file should not be world-readable (only root should be able to look into this) and it may look like this:

ntp keys file (ntp.keys)

```

1      N 29233E0461ECD6AE      # des key in NTP format
2      M Rlrop8KPPvQvYotM      # md5 key as an ASCII random string
14     M sundial                # md5 key as an ASCII string
15     A sundial                # des key as an ASCII string
                                # the following 3 keys are identical
10     A SeCReT
10     N d3e54352e5548080
10     S a7cb86a4cba80101
```

The first column holds the key ID (used in the ntp.conf file), the second column defines the format of the key, which is following in column three. There are four different key formats:

- “**A**” means DES key with up to eight 7-bit ASCII characters, where each character is standing for a key octet (this is used by Unix passwords, too).
- “**S**” is a DES key written in hexadecimal notation, where the lowest bit (LSB) of each octet is used as the odd parity bit.
- If the key format is specified as “**N**”, it also consists of a hexadecimal string, but in NTP standard format by using the highest bit (HSB) of each octet used as the odd parity bit.
- A key defined as “**M**” is a MD5 key with up to 31 ASCII characters.
- The LANTIME supports MD5 authentication only.
- Please be aware of the following restrictions: No “**#**”, “**t**” (**tab**), “**n**” (**newline**) and “**0**” (**null**) are allowed in a DES or MD5 ASCII key. The key ID 0 is reserved for special purposes and should not appear in the keys file.

5.6.2 NTP AUTOKEY

NTP Version 4 supports symmetric keys and additionally provides the so-called AUTOKEY feature. The authentic of received time at the NTP clients is sufficiently ensured by the symmetric key technique. In order to achieve a higher security, e.g. against so-called replay attacks, it is important to change the used crypto keys from time to time.

In networks with a lot of clients, this can lead to a logistic problem, because the server key has to be changed on every single client. To help the administrator to reduce this work (or even eliminate it completely), the NTP developers invented the AUTOKEY feature, which works with a combination of group keys and public keys. All NTP clients are able to verify the authentic of the time they received from the NTP servers of their own AUTOKEY group by using this AUTOKEY technique.

The AUTOKEY features works by creating so-called secure groups, in which NTP servers and clients are combined. There are three different kinds of members in such a group:

a) Trusted Host

One or more trusted NTP servers. In order to become a “trusted” server, a NTP server must own a self-signed certificate marked as “trusted”. It is good practice to operate the trusted hosts of a secure group at the lowest stratum level (of this group).

b) Host

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

c) Client

One or more NTP client systems, which in contrast to the above mentioned servers do not provide accurate time to other systems in the secure group. They only receive time.

All members of this group (trusted hosts, hosts and clients) have to have the same group key. This group key is generated by a so-called trusted authority (TA) and has to be deployed manually to all members of the group by secure means (e.g. with the UNIX SCP command). The role of a TA can be fulfilled by one of the trusted hosts of the group, but an external TA can be used, too.

The used public keys can be periodically re-created (there are menu functions for this available in the web interface and also in the CLI setup program, see “Generate new NTP public key” in section “NTP Autokey” of the “Security Management” page) and then distributed automatically to all members of the secure group. The group key remains unchanged, therefore the manual update process for crypto keys for the secure group is eliminated. A LANTIME can be a trusted authority / trusted host combination and also a “non-trusted” host in such a secure group.

To configure the LANTIME as a TA / trusted host, enable the AUTOKEY feature and initialise the group key via the HTTPS web interface (“Generate groupkey”) or CLI setup program. In order to create such a group key, a crypto password has to be used in order to encrypt / decrypt the certificate. This crypto password is shared between all group members and can be entered in the web interface and CLI setup program, too. After generating the group key, you have to distribute it to all members of your secure group (and setup these systems to use AUTOKEY, too). In the ntp.conf file of all group members you have to add the following lines (or change them, if they are already included):

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

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

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

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

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

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

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

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

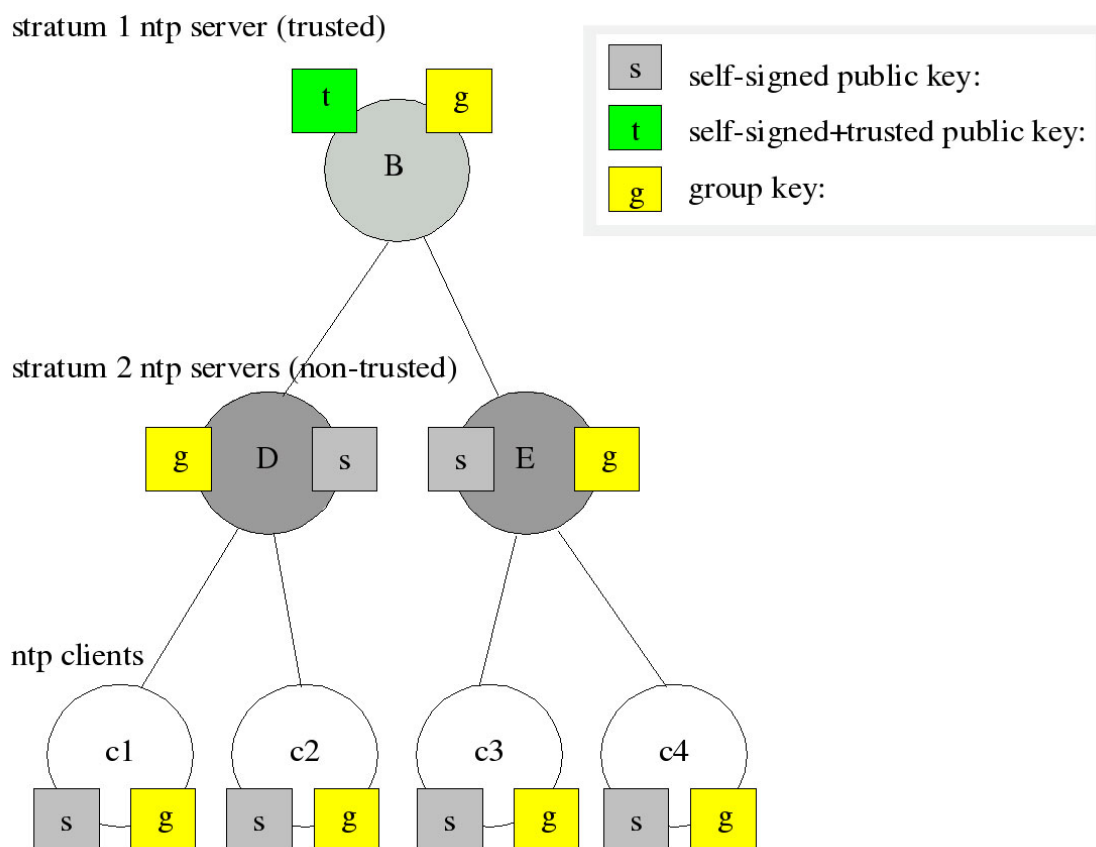
Here, too, “cryptosecret” is the crypto password used in the ntp.conf entry. Then you have to copy the new ntpkeys to the flash disk with:

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

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

Example:

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



D and E are NTP servers, which are “non-trusted” hosts of the group, they hold the group key and a self-signed certificate which lacks the “trusted” mark. The clients also hold the group key and a self-signed certificate. In order to distribute new public keys to the whole group, the administrator only has to generate a new “t” key, which will be distributed automatically to the two hosts D and E. Because these two servers can now present a unbroken chain of certificates to a trusted host, they can be considered “trusted” by the clients as well.

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

5.7 Configuration: Local

Local configuration

Lantime services:

Reboot device

Manual configuration

Send test notification

Save NTP drift file

Reset to factory defaults

Download SNMP MIB files

Reset Error Relais

Lantime User Management:

User administration

Show Lantime information:

List all messages

List detailed version information

List device options

Lantime firmware update:

Durchsuchen...

Start firmware update

View logfile of last update

Lantime configuration:

Check configuration

Get diagnostics information

Receiver:

List detailed GPS information

General Information:

Contact:

Location:

Web interface language:

Save settings

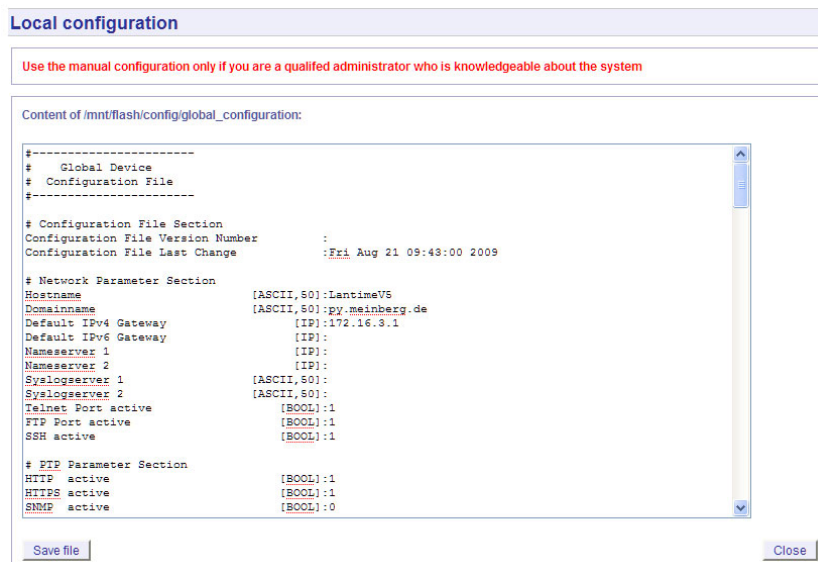
Reset changes

Back

5.7.1 Administrative functions

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

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



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

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

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

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

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

5.7.2 User Management

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

Local configuration

Change Current User Password:

New password:

Re-enter:

Change password

User Management:

Add new User:

Password:

Group membership:

☐ Super-User
 ☐ Administrator
 ☐ Info

Create User

Available User:

Username	Group membership	Option
root	Super-User	

Close

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

5.7.3 Administrative Information

The button “List all messages” displays the SYSLOG of the LANTIME completely. In this log all subsystems create their entries, even the OS (upper case) kernel. The SYSLOG file /var/log/messages is only stored in the system’s ram disk, therefore it is lost after a power off or restart. If you configured an external SYSLOG server, all LANTIME syslog entries will be duplicated on this remote system and can be saved permanently this way.

```

Mar 15 13:35:17 LanGpsV4 ntpd[12948]: ntpd 4.2.0@1.1161-r Fri Mar 5 15:58:48 CET 2004 (3)
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: signal_no_reset: signal 13 had flags 4000000
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: precision = 3.000 usec
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: kernel time sync status 2040
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: frequency initialized 45.212 PPM from /etc/ntp.drift
Mar 15 13:38:36 LanGpsV4 lantime[417]: NTP sync to GPS
Mar 15 13:38:36 LanGpsV4 lantime[417]: NTP restart
Mar 15 13:45:36 LanGpsV4 proftpd[14061]: connect from 172.16.3.2 (172.16.3.2)
Mar 15 14:01:11 LanGpsV4 login[15711]: invalid password for 'root' on 'tty1' from '172.16.3.45'
Mar 15 14:01:17 LanGpsV4 login[15711]: root login on 'tty1' from '172.16.3.45'

```

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

Local configuration

Content of /device_version:

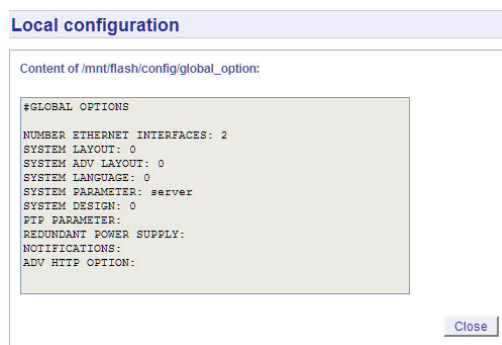
```

ID: lantime ELX800 GPS170 M3x VS.28g
S/N: n/a
GPS170 v1.19 S/N: 10012290
Oscillator type: TCXO HQ
NTP Version: 4.2.0b$1.1438-o Mon Oct 6 13:18:28 UTC 2008 (1)
Kernel Version: 2.6.15.1
System Version: 528
ETH0: HWaddr 00:13:95:02:C2:FA

```

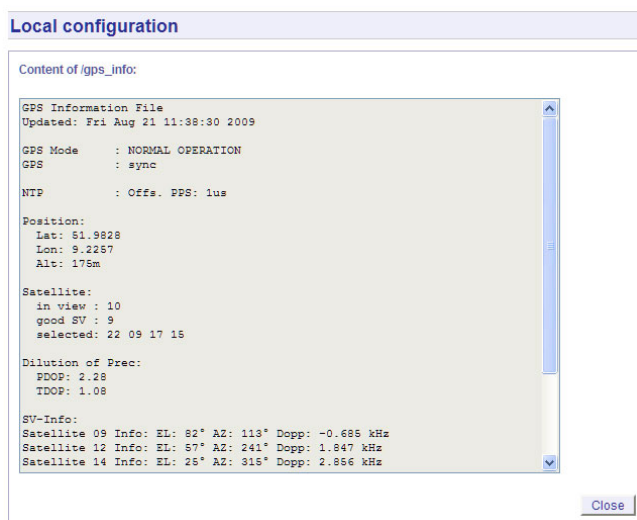
Close

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



Using the button “List detailed GPS information” gives you the possibility to check detailed GPS status information. The first parameter indicates the time and date of the last update of the shown parameters. Next you find the GPS receiver status and the NTP status, followed by the GPS position data. The position uses the Latitude / Longitude / Altitude format. Latitude and Longitude are shown in degrees, minutes and seconds, Altitude is shown in meters above WGS84 ellipsoid.

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



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

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

5.7.4 Software Update

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

The chosen file will be uploaded to the LANTIME, afterwards you are prompted to confirm the start of the update process. The scope of the update only depends on the chosen file.

5.7.5 Automatic configuration check

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

Local configuration

Checking the configuration

Ethernet:

Hostname: LantimeV5

IPv4 Gateway: 172.16.3.1

ok

ok

Ethernet interface 0:

TCP/IP address: 0.0.0.0

Netmask: 255.255.255.000

ok

ok

Ethernet interface 1:

TCP/IP address: 0.0.0.0

Netmask: 255.255.255.000

ok

ok

Notification:

To address: jens.bal@meinberg.de

From address: jens.bal@meinberg.de

ok

ok

Checking the reachability of configured ip-addresses or hostnames

Ethernet:

IPv4 Gateway: 172.16.3.1

reacha

Notification:

Back

5.7.6 Get Diagnostics Information

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

5.7.7 Web interface language

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

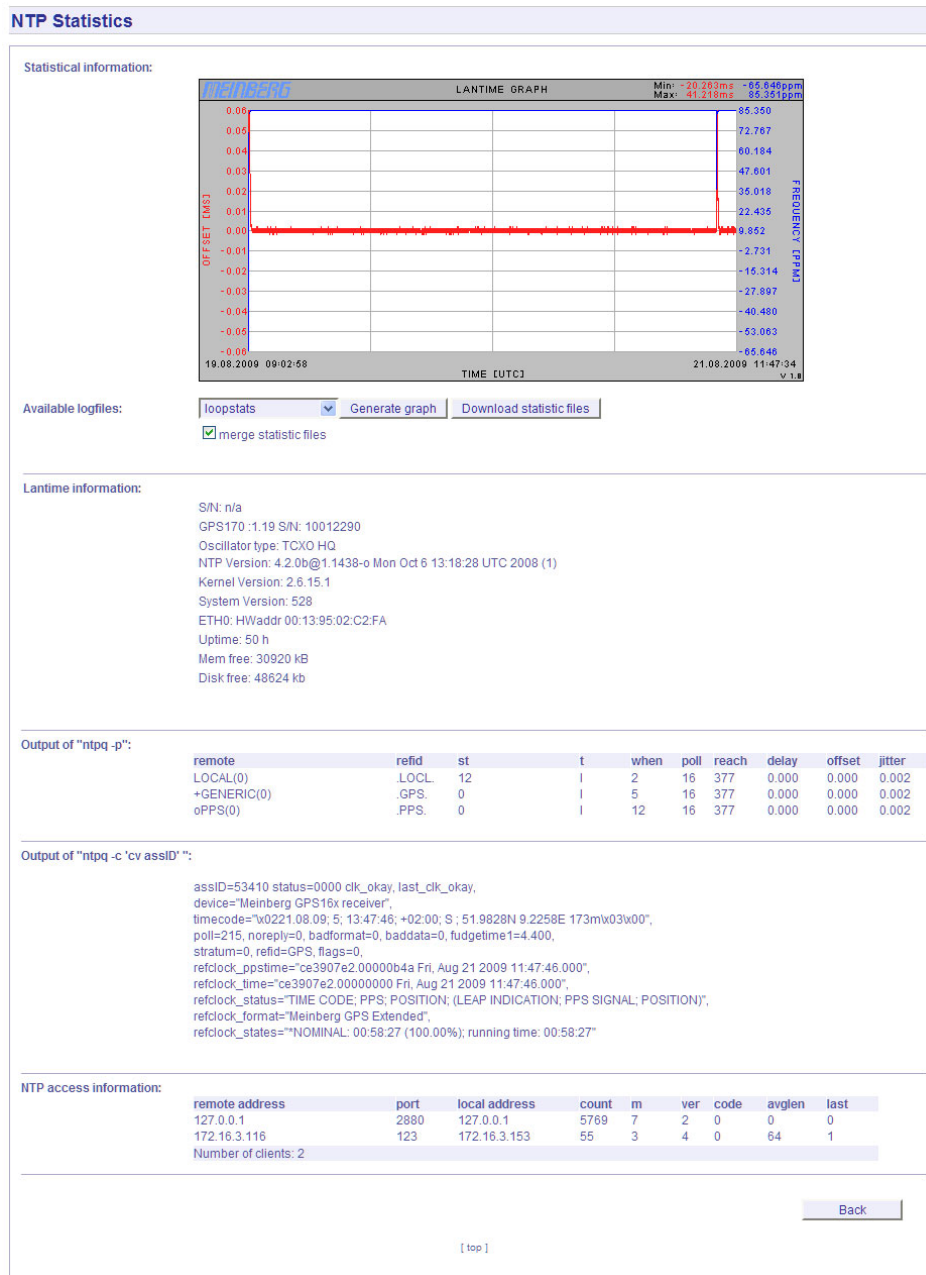
Web interface language:

English

English

German

5.8 Configuration: Statistics



5.8.1 Statistical Information

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

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

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

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

with the following meaning:

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

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

5.9 Configuration: Manual

Manual

Available documents:

Filename	Language	Type	Date	Size	Option
1he_langps_etv_v5_e	english	pdf	2009-02-27	1647.40kb	open
1he_langps_etv_v5	german	pdf	2009-02-27	1745.07kb	open

2 documents available

You need Adobe's Acrobat Reader to open most of the documents [open](#)

Customer notes:

Filename	Language	Type	Date	Size	Options
no notes available	n/a	n/a	n/a	n/a	n/a

Add note

Back

This page gives you access to the documents stored on your LANTIME, especially the manuals and your own notes. The two lists include filename, language, file type, date and size of the documents/notes.

The LANTIME documents can be downloaded from here in order to read / print them on your workstation. The customer notes are a way of storing small pieces of information on your LANTIME, for example if you want to keep track of configuration changes and want to comment them, you can create a note called "config_changes" and show or edit it from here. If you want to get rid of one of your notes, you are able to delete it by choosing the appropriate button.

Manual

Content of /www/manual/customer/english/history.txt:

```

12.08.2009 - Start LANTIME Time Service
20.08.2009 - Firmware Update

```

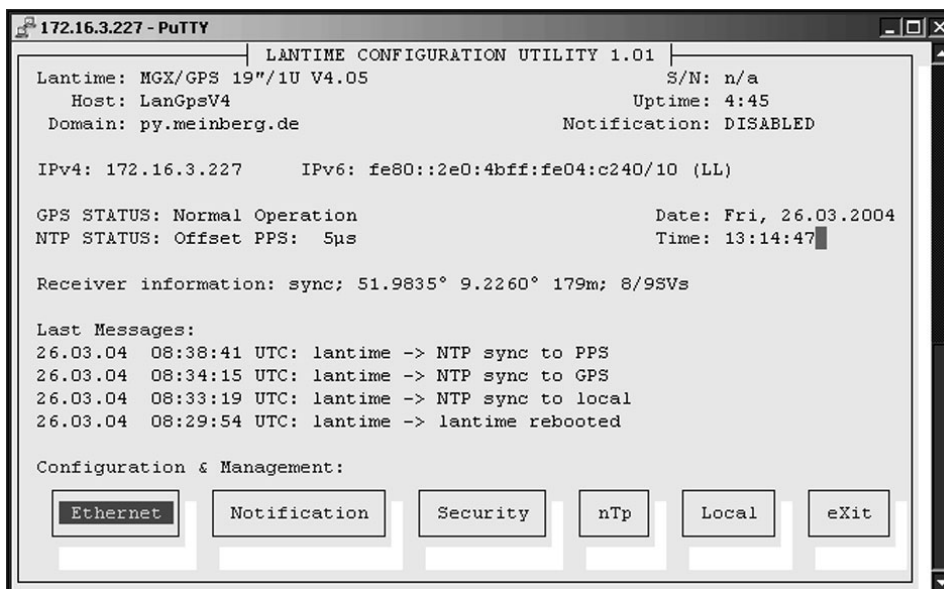
Save file

Close

If you want to add a note (you can maintain more than one note on your LANTIME), after choosing the button "add note" you have to enter a filename (without a directory path, all notes are stored in a fixed directory on the flash disk of your LANTIME) and the language of your note first. After you confirmed these parameters with "Add document", you are able to edit the text of your new note.

6 The Command Line Interface

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



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

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

The third section shows the last messages of the system, each with a timestamp added. The newest messages are placed at the top of the list. This reflects the content of the file `/var/log/messages`, which is created after every start of the system (and is lost after a power off or reboot, see “Syslog server” to learn how to save the entries of your SYSLOG).

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

6.1 CLI Ethernet

The screenshot shows a window titled "ETHERNET CONFIGURATION". It contains several fields for configuration:

- <Hostname>**: LantimeV4
- <Domainname>**: py.meinberg.de
- <Nameserver 1>**: 172.16.3.1
- <Nameserver 2>**: (empty)
- <Syslogserver 1>**: (empty)
- <Syslogserver 2>**: (empty)
- <IPv4 Default Gateway>**: 172.16.3.1
- <IPv6 Default Gateway>**: (empty)
- Protocol Status Table**:

<Telnet>	ENABLED	<SSH>	ENABLED
<FTP>	ENABLED	<HTTPS>	ENABLED
<HTTP>	ENABLED	<SMB>	DISABLED
<IPv6 protocol>	ENABLED	<SNMP>	ENABLED
- Ethernet 0**: (button)
- SAVE** and **CLOSE** buttons.

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

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

If you enter nothing in the SYSLOG server fields or specify 0.0.0.0 as the SYSLOG server's addresses, the remote SYSLOG service is not started on your LANTIME.

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

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

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

The third section allows you to select the IP protocol 6. In this version the IPv4 protocol is mandatory and cannot be disabled, but a standalone IPv6 mode can be reached by entering an IPv4 address "0.0.0.0" and disabling the DHCP client option for every network interface of your LANTIME. By doing so, you ensure that the timeserver cannot be reached with IPv4. Please note that TELNET, FTP and NETBIOS cannot be used over IPv6 in this version. IPv4 and IPv6 can be used together on one LANTIME.

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

ETHERNET CONFIGURATION LINE 0	
IPv4:	<TCP/IP address> 172.16.3.226
	<Netmask> 255.255.255.0
	<Gateway> 172.16.3.1
	<DHCP Client> DISABLED
IPv6:	<IP 1>
	<IP 2>
	<IP 3>
	<Autoconf> ENABLED
	<Net Link Mode> Auto
	<High availability bonding> single connection
IPv6: IP Router Advert.:	
	Link local: fe80::2e0:4bff:fe04:c240/10
<input type="button" value="BACK"/>	

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

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

Example: 192.168.10.2

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

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

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

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

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

You can specify up to three IPv6 addresses for your LANTIME timeserver. Additionally you can switch off the IPv6 AUTOCONF feature. IPv6 addresses are 128 bits in length and written as a chain of 16 bit numbers in hexadecimal notation, separated with colons. A sequence of zeros can be substituted with “:” once.

Examples:

“::” is the address, which simply consists of zeros

“::1” is the address, which only consists of zeros and a 1 as the last bit.

This is the so-called host local address of IPv6 and is the equivalent to 127.0.0.1 in the IPv4 world

“fe80::0211:22FF:FE33:4455” is a typical so-called link local address, because it uses the “fe80” prefix.

In URLs the colon interferes with the port section, therefore IPv6-IP-addresses are written in brackets in an URL: “http://[1080::8:800:200C:417A]:80/”; the last “:80” simply sets the port to 80, the default http port)

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

The next parameter in this sub section is “Netlink mode”. This controls the port speed and duplex mode of

the selected Ethernet port. Under normal circumstances, you should leave the default setting ("autosensing") untouched, until your network administrator tells you to change it.

The standard moniker for this technology is IEEE 802.3ad, although it is known by the common names of trunking, port trunking, teaming and link aggregation. The conventional use of bonding under Linux is an implementation of this link aggregation. Only one link is used at any given time. At least two physical Ethernet ports must be linked to one bonding group to activate this feature. The first Ethernet Port in one bonding group provides the IP-Address and the net mask of this new virtual device. The implementation of the LANTIME Bonding feature will not replace the MAC address of the active ethernet port. Depending on the LINK state of the ETH-port the IP address of the first port in the bonding group will be set to the next ethernet port. All services will be restarted automatically.

At this menu point it is possible to add each Ethernet port to a bonding group. At least two physical Ethernet ports must be linked to one bonding group to activate this feature. The first Ethernet Port in one bonding group provides the IP Address and the net mask of this new virtual device.

6.2 CLI Notification

```

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

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

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

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

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

            <Notification conditions>      <SAVE>      <CLOSE>

```

Alarm events

On this page you can set up different notification types for a number of events. This is an important feature because of the nature of a timeserver: running in the background. If an error or problem occurs, the timeserver is able to notify an administrator by using a number of different notification types.

The LANTIME timeserver offers four different ways of informing the administrator or a responsible person about nine different events: EMAIL send an e-mail message to a specified e-mail account, SNMP-TRAP sends a SNMP trap to one or two SNMP trap receivers, WINDOWS POPUP MESSAGE sends a Winpopup message to one or two different computers and DISPLAY shows the alarm message on a wall mount display model VP100/NET, that is an optional accessory you can obtain from us.

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

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

E-mail messages

You can specify the e-mail address which is used as the senders address of the notification e-mail (From: address), the e-mail address of the receiver (To: address) and a SMTP smarthost, that is a mail server who is forwarding your mail to the receiver. If your LANTIME system is connected to the internet, it can deliver those e-mails itself. Additional e-mail recipients can be configured with the button “CC recipients”. These settings cannot be altered with the LC display buttons of the front panel.

Please note the following:

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

Condition:	EMail	SNMP	WinMail	Display
NTP not sync	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTP stopped	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Server boot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receiver not responding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receiver not sync	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Antenna faulty	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Antenna reconnect	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Config changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Leap Second announced	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

BACK

Windows Popup Messages

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



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

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

SNMP-TRAP messages

Up to two SNMP trap receiver hosts can be configured in this subsection, you may use IPv4 or IPv6 addresses or specify a hostname. Additionally you have to enter a valid SNMP community string for your trap receiving community. These are mostly independent from the SNMP community strings used for status monitoring and configuration (see SNMP configuration on the “Security” page).

VP100/NET wall mount display

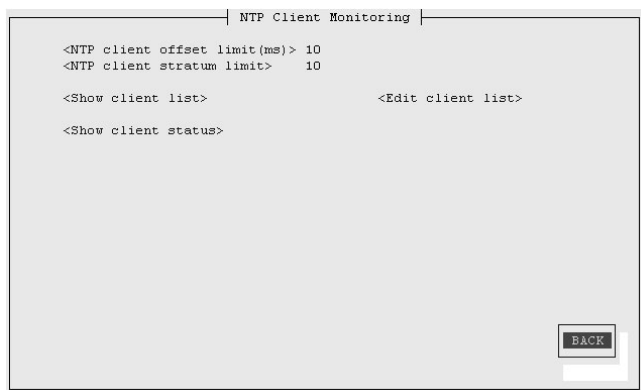
The VP100/NET wall display is an optional accessory for the LANTIME timeserver, it has an own integrated Ethernet port (10/100 Mbit) and a SNTP client. The time of the display can be received from any NTP server using the SNTP protocol, additionally the display is able to show text messages, which are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

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

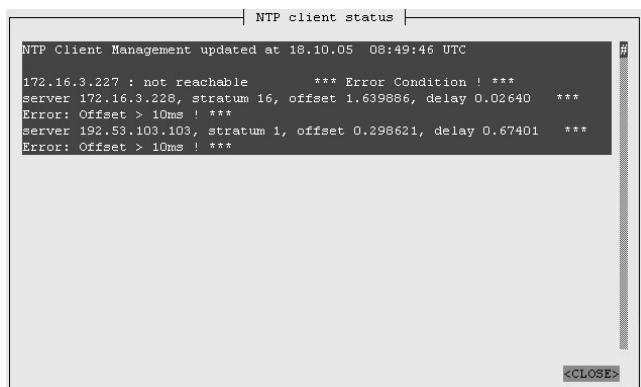
If you want to use the display for other purposes, you can send text messages to it by using our command line tool send2display, which can be found on the LANTIME. This allows you to use the display by CRON jobs or your own shell scripts etc. If you run the tool without parameters, a short usage screen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

NTP Client Monitoring

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

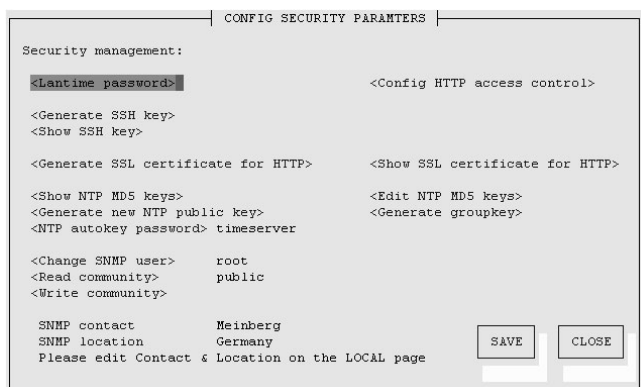


You can monitor the current states of the configured clients:



6.3 CLI Security

On the “Security” page you can manage all security relevant parameters for your timeserver. In the first section “Login” the administration password can be changed, which is used for SSH, TELNET, FTP, HTTP and HTTPS access.



The password is stored encrypted on the internal flash disk and can only be reset to the default value “timeserver”

by a “factory reset”, changing all settings back to the factory defaults. Please refer to the LCD configuration section in this manual.

SSH Secure Shell Login

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

```
ssh root @ 192.168.16.111
```

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

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

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

Generate SSL Certificate for HTTPS

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

By using the button “Generate SSL certificate for HTTP” you can create a new certificate. Please enter your organisation, name, mail address and the location in the upcoming form and press “Generate SSL certificate” to finally generate it.

NTP keys and certificates

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

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

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

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

6.4 CLI NTP Parameter

```

CONFIG NTP PARAMETERS

<Config External NTP Server>

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

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

  <PPS> ENABLED
  <Autokey> DISABLED

  <Trusted key>

  <NTP trust time> 0    hour(s)

  <Edit additional NTP Parameter>    <Show current NTP configuration>

  [SAVE] [CLOSE]

```

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

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your LANTIME system and the GPS reference clock. The local clock is only chosen as the NTP time reference after the GPS clock lost its synchronisation. The stratum level of this local clock is set to 12, this ensures that clients recognise the switchover to the local clock and are able to eventually take further actions. The local clock can be disabled.

Because the GPS reference clock is internally connected to the LANTIME system by using a serial connection, the accuracy using this way of synchronisation is around 1 ms. The high accuracy of the LANTIME timeserver (around 10 microseconds) is available by using the ATOM driver of the NTP subsystem, which is directly interpreting the PPS (pulse per second) of the GPS reference clock. The default configuration looks like this:

```

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

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

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

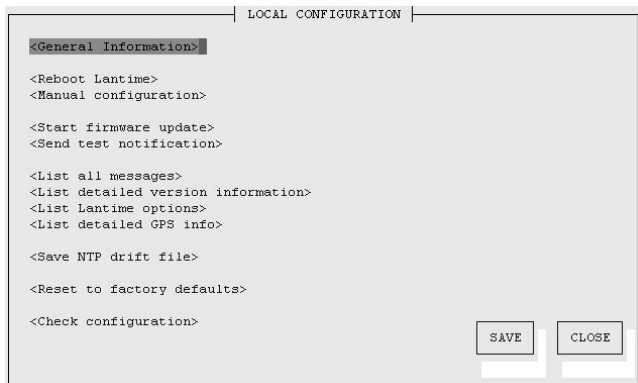
# Edit /mnt/flash/ntpconf.add to add additional NTP parameters

```

6.4.1 CLI NTP Authentication

Please see the corresponding chapter in the web interface description.

6.5 CLI Local



Administrative functions

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

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

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

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

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

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

User Management

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

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

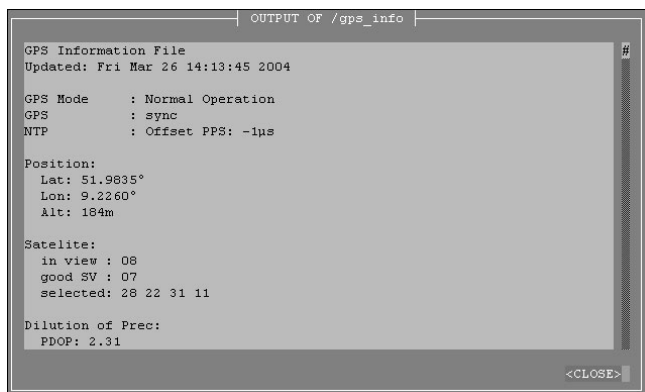
Administrative information

The button "List all messages" displays the SYSLOG of the LANTIME completely. In this log all subsystems create their entries, even the OS kernel. The SYSLOG file /var/log/messages is only stored in the system's ram disk, therefore it is lost after a power off or restart. If you configured an external SYSLOG server, all LANTIME SYSLOG entries will be duplicated on this remote system and can be saved permanently this way.

```
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: ntpd 4.2.0@1.1161-r Fri Mar 5 15:58:48 CET 2004 (3)
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: signal_no_reset: signal 13 had flags 4000000
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: precision = 3.000 usec
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: kernel time sync status 2040
Mar 15 13:35:17 LanGpsV4 ntpd[12948]: frequency initialized 45.212 PPM from /etc/ntp.drift
Mar 15 13:38:36 LanGpsV4 lantime[417]: NTP sync to GPS
Mar 15 13:38:36 LanGpsV4 lantime[417]: NTP restart
Mar 15 13:45:36 LanGpsV4 proftpd[14061]: connect from 172.16.3.2 (172.16.3.2)
Mar 15 14:01:11 LanGpsV4 login[15711]: invalid password for 'root' on 'tty1' from '172.16.3.45'
Mar 15 14:01:17 LanGpsV4 login[15711]: root login on 'tty1' from '172.16.3.45'
```

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

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



Using the button "List detailed GPS information" gives you the possibility to check detailed GPS status information. The first parameter indicates the time and date of the last update of the shown parameters. Next you find the GPS receiver status and the NTP status, followed by the GPS position data. The position uses the Latitude / Longitude / Altitude format. Latitude and Longitude are shown in degrees, minutes and seconds, Altitude is shown in meters above WGS84 ellipsoid.

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

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

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

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

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

Software Update

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

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

7 SNMP Support

The Simple Network Management Protocol (SNMP) has been created to achieve a standard for the management of different networks and the components of networks. SNMP is operating on the application layer and uses different transport protocols (like TCP/IP and UDP), so it is network hardware independent.

The SNMP design consists of two types of parties, the agent and the manager. SNMP is a client-server architecture, where the agent represents the server and the manager represents the client.

The LANTIME has an integrated SNMP agent, who is designed especially to handle SNMP requests for LANTIME specific status information (including status variables for the internal reference clock). The LANTIME SNMP agent is also capable of handling SET requests in order to manage the LANTIME configuration via SNMP, if your SNMP management software is also supporting this feature.

The elements (objects / variables) are organised in data structures called Management Information Base (MIB). The LANTIME includes the standard NET-SNMP MIB and is based on SNMPv1 (RFC 1155, 1157), SNMPv2 (RFC 1901-1908) and SNMPv3.

The following SNMP version is installed on the timeserver:

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

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

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

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

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

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

...mbgLtRefclock.mbgLtRefClockModeVal.0 = 1
```

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

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

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

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

7.1 Configuration over SNMP

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

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

- a) SNMP has to be activated in the timeservers setup by setting up a RWCOMMUNITY
- b) In the SNMP configuration the read-write-access needs to be activated
- c) The timeserver-specific MIB files must be present on the clients, they have to be included in the SNMP setup of the client software

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

Afterwards, copy all MIB files to the MIB directory on your client(s) and configure your SNMP client software to use them.

7.1.1 Examples for the usage of the SNMP configuration features

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

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

```
root@testhost:/# snmpwalk -v 2c -c public timeserver.meinberg.de mbgLtCfg
```

```

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

```

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

```

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

```

```

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

```

```

root@testhost:/#

```

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

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

```

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

```

```

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

```

```

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

```

```

root@testhost:/#

```

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

7.1.2 Further configuration possibilities

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

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

If you need to customize the configuration of the timeservers SNMPD (for setting up detailed access control rights for example), you may edit /mnt/flash/packages/snmp/etc/snmpd_conf.default (which is the mentioned template file). Please note that some lines are appended to this file (as described above), before it is used as /usr/local/share/snmp/snmpd.conf by the snmpd process.

7.1.3 Send special timeserver commands with SNMP

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

Reboot(1)

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

FirmwareUpdate(2)

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

ReloadConfig(3)

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

GenerateSSHKey(4)

A new SSH key will be generated.

GenerateHTTPSKey(5)

A new HTTPS key will be generated.

ResetFactoryDefaults(6)

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

GenerateNewNTPAutokeyCert(7)

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

SendTestNotification(8)

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

A few examples:

(we are again using the `snmpset` command which comes with the `net-snmp` tools).

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

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

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

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

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

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

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

7.1.4 Configuration of the timeserver with SNMP: Reference

The MIB of the timeserver includes the following parts:

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

Further detailed information can be found in the Meinberg MIB files.
Reference of LANTIME SNMP configuration variables:

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

SNMP branch	Variable	Data type	Description
	mbgLtCfgSambaAccess	integer (0 = disabled, 1 = enabled)	LANManager-access activated?
	mbgLtCfgIPv6Access	integer (0 = disabled, 1 = enabled)	IPv6-protocol enabled?
	mbgLtCfgSSHAccess	integer (0 = disabled, 1 = enabled)	SSH-access activated?
mbgLtCfgNTP	mbgLtCfgNtpServer1IP	string (IPv4 or IPv6-address or hostname)	First external NTP-server
	mbgLtCfgNtpServer1KEY	integer	Link to the key which should be used for the first NTP-server
	mbgLtCfgNtpServer2IP	string (IPv4 or IPv6-address or hostname)	Second external NTP-server
	mbgLtCfgNtpServer2KEY	integer	Link to the key which should be used for the second NTP-server
	mbgLtCfgNtpServer3IP	string (IPv4 or IPv6-address or hostname)	Third external NTP-server
	mbgLtCfgNtpServer3KEY	integer	Link to the key which should be used for the third NTP-server
	mbgLtCfgStratumLocal Clock	integer(0..15)	Stratum-value of the internal system clock of the timeserver
	mbgLtCfgNTPTrustedKey	integer	Link to the key which should be used for the internal reference time source
	mbgLtCfgNTPBroadcastIP	string (IPv4 or IPv6-address)	IP-address, which has to be used for NTP-broadcasts (or multicasts)
	mbgLtCfgNTPBroadcast Key	integer	Link to the key which should be used for outgoing NTP-broadcasts
	mbgLtCfgNTPBroadcast Autokey	integer (0 = disabled, 1 = enabled)	Use autokey for NTP broadcasts?
	mbgLtCfgAutokeyFeature	integer (0 = disabled, 1 = enabled)	Use autokey feature of the NTP server?

SNMP branch	Variable	Data type	Description
	mbgLtCfgAtomPPS	integer (0 = disabled, 1 = enabled)	Atom PPS (pulse per second) activated?
mbgLtCfgEMail	mbgLtCfgEMailTo	string (Liste von EMail-addressen)	One or more (semicolon separated) email address(es). which should receive warnings and alarm notifications from the timeserver
	mbgLtCfgEMailFrom	string (EMail-address)	The EMail-address which is used as the senders address for email notifications
	mbgLtCfgEMailSmarthost	string (IPv4 or IPv6-address or hostname)	The SMTP-host, which is used for sending mails
mbgLtCfgSNMP	mbgLtCfgSNMPTrapReceiver1	string (IPv4 or IPv6-address or hostname)	First host, which receives notifications sent as SMTP-traps
	mbgLtCfgSNMPTrapReceiver1Community	string	The SNMP community used when sending SNMP-Traps to the first host
	mbgLtCfgSNMPTrapReceiver2	string (IPv4 or IPv6-address or hostname)	Second host, which receives notifications sent as SMTP-traps
	mbgLtCfgSNMPTrapReceiver2Community	string	The SNMP community used when sending SNMP-Traps to the second host
	mbgLtCfgSNMPROCommunity	string	The SNMP community, which has read-only access and therefore can be used to only monitor status variables or configuration values (SNMP V2c)
	mbgLtCfgSNMPRWCommunity	string	The SNMP community, which has read-write access and there for can be used to monitor status variables and get/set configuration values (SNMP V2c)
	mbgLtCfgSNMPContact	string	Contact information (e.g. name of a contact person) of the timeserver
	mbgLtCfgSNMPLocation	string	Location (e.g. building/room number) of the timeserver
mbgLtCfgWinpopup	mbgLtCfgWMailAddress1	string	First receiver of notifications sent as windows popup messages
	mbgLtCfgWMailAddress2	string	Second receiver of notifications sent as windows popup messages

SNMP branch	Variable	Data type	Description
mbgLtCfgWalldisplay	mbgLtCfgVP100Display1IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the first wall-mount display used for showing notifications
	mbgLtCfgVP100Display1SN	string (Hexstring)	The serial number of the first wall mount display used for showing notifications (can be found in the setup menu of the display)
	mbgLtCfgVP100Display2IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the second wall mount display used for showing notifications
	mbgLtCfgVP100Display2SN	string (Hexstring)	The serial number of the first wall mount display used for showing notifications (can be found in the setup menu of the display)
mbgLtCfgNotify	mbgLtCfgNotifyNTPNotSync	string(combination)	Exactly one, none or a combination of the following notification types: email = sending an email wmail = sending a winpopup-message snmp = sending a SNMP-trap, disp = showing on wall mount display, syslog = sending a syslog-entry for the event „NTP not synchronized“
	mbgLtCfgNotifyNTPStopped	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „NTP Daemon stopped“
	mbgLtCfgNotifyServerBoot	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Timeserver reboot“
	mbgLtCfgNotifyRefclockNotResponding	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not ready“
	mbgLtCfgNotifyRefclockNotSync	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not synchron“
	mbgLtCfgNotifyAntennaFaulty	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna not connected or damaged“
	mbgLtCfgNotifyAntennaReconnect	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna reconnected“
	mbgLtCfgNotifyConfigChanged	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Configuration changed“
	mbgLtCfgNotifyLeapSecondAnnounced	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Leap second announced“

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

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

7.2 SNMP Traps

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

The following SNMP-traps are available:

"NTP not sync"	NTP not synchronised to refclock	"NTP stopped"
NTP stopped	"Server boot"	System has rebooted
"Receiver not responding"	no answer from GPS	"Receiver not sync"
GPS receiver not synchronised	"Antenna faulty"	GPS antenna not connected
"Antenna reconnect"	GPS antenna reconnected	"Config changed"
System parameter changed by user	„Leap second announced“	Leap second announced

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

7.2.1 SNMP Trap Reference

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

Here is a list of all traps the timeserver knows:

- **mbgLtTrapNTPNotSync (mbgLtTraps.1):** Whenever the NTP daemon (ntpd) loses sync, it will generate this trap and send it to the configured SNMP trap receivers.
- **mbgLtTrapNTPStopped (mbgLtTraps.2):** This trap is sent when the NTP daemon stopped, manually or because of an error condition.
- **mbgLtTrapServerBoot (mbgLtTraps.3):** After finishing the boot process, this trap is generated.
- **mbgLtTrapReceiverNotResponding (mbgLtTraps.4):** Trap to be sent when the internal receiver of the timeserver is not responding.
- **mbgLtTrapReceiverNotSync (mbgLtTraps.5):** If the internal receiver loses sync, the SNMP trap receivers will receive this trap.
- **mbgLtTrapAntennaFaulty (mbgLtTraps.6):** This trap will be sent whenever the timeserver recognises a broken connection to the antenna of the receiver.
- **mbgLtTrapAntennaReconnect (mbgLtTraps.7):** After the connection to the antenna has been re-established, this trap is sent.
- **mbgLtTrapConfigChanged (mbgLtTraps.8):** After reloading its configuration, the timeserver generates this trap.
- **mbgLtTrapLeapSecondAnnounced (mbgLtTraps.9):** If a leap second has been announced by the internal GPS receiver, this trap will be sent.
- **mbgLtTrapTestNotification (mbgLtTraps.99):** This trap is sent whenever you are requesting a test notification; it is only used for testing the connection between the timeserver and your SNMP trap receivers.