MANUAL

LCES

NTP/RPS/BGT

8th February 2016

Meinberg Radio Clocks GmbH & Co. KG

Table of Contents

1 Imprint

Meinberg Funkuhren 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: 2015-07-27

2 Safety instructions for building-in equipment

This building-in equipment has been designed and tested in accordance with the requirements of Standard IEC 60950-1 "Safety of Information Technology Equipment, including Electrical Business Equipment".

During installation of the building-in equipment in an end application (i.e. rack) additional requirements in accordance with Standard IEC 60950-1 have to be taken into account.

General Safety instructions

- The building-in equipment has been evaluated for use in office environment (pollution degree 2) and may be only used in this environment. For use in rooms with a higher pollution degree more stringent requirements are applicable.
- The equipment/building-in equipment was evaluated for use in a maximum ambient temperature of 40°C.
- The building-in equipment may not be opened.
- Protection against fire must be assured in the end application.
- The ventilation opening may not be covered.

For AC Supply 100-240VAC

- The building-in equipment is a class 1 - equipment and must be connected to an earthed outlet (TN Power System).
- For safe operation the building-in equipment must be protected by max 16 A fuse in the power installation system.
- Disconnection of the equipment from mains is done by pulling the mains plug at the outlet. Don't use the connector at the module for disconnection from mains.

For DC Supply 100-240VDC

- The device can be disconnected outside the unit in accordance with the regulations as in EN 60950 (e.g. through primary side line protection).
- Assembling and disassembling of the power connector is only allowed if the device is disconnected from power supply (e.g. trough primary side line protection).
- All feed lines are sufficiently protected and dimensioned.

Fuse:	T3A
Connector Diameter:	1mm^2 - 2,5mm^2 / 17AWG - 13AWG

2.1 Additional Safety Hints

⚠

This manual contains important information for the installation and operation of this device as well as for your safety. Make sure to read carefully before installing and commissioning the device.

Certain operating conditions may require the observance of additional safety regulations not covered by this manual. Nonobservance of this manual will lead to a significant abatement of the security provided by this device. Security of the facility where this product is integrated lies in the responsibility of the installer.

The device must be used only for purpose named in this manual, any other use especially opteration above the limits specified in this document is considered as improper use.

Keep all documents provided with the device for later reference.

This manual is exclusively for qualified electricians or by a qualified electrician trained personnel who are familiar with the applicable national standards and specifications, in particular for the construction of high voltage devices.

2.2 Supply Voltage

WARNING!
This device is powered by a dangerous voltage. Nonobservance of the safety instructions of this manual may lead to serious damage to persons and property and to danger to life! Installtion, commissioning, maintenance and operation of this device are to be carried out by qualified personnel only.

The general safety instructions and standards (e.g. IEC, DIN, VDE, EN) for installation and work with high voltage equipment as well as the respective national standards and laws must be observed.

NONOBSERVANCE MAY LEAD TO SERIOUS DAMAGE TO PERSONS AND PROPERTY AND TO DANGER TO LIFE!

The device may not be opened. Repair services may only be carried out by the manufaturer.

Supply lines for this decice must be equipped via an appropriate switch that must be mounted close to the device and must be marked as a mains switch for the device.

To ensure safe operation supply mains connected to this decice must be equipped with a fuse and a fault-current circuit breaker according to the applicable national standards for safe operation.

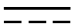
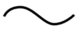
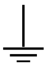
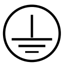
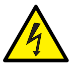
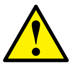
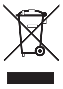
The device must be connected to a protective earth with low grounding resistance according to the applicable national rules.

2.3 Cabling

WARNING!
DANGER TO LIFE BY ELECTRICAL SHOCK! NO LIVE WORKING!
Wiring or any other work done the connectors particularly when connectors are opened may never be carried out when the installation is energized. All connectors must be covered to prevent from accidental contact to life parts.

ALWAYS ENSURE A PROPER INSTALLATION!

2.4 Used Symbols

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

CE marking
This device follows the provisions of the directives 93/68/EEC

CE

3 LANTIME Basic Configuration Wizard

After running up the device, one can connect with a serial port (TERM) of the LANTIME with a PC using a NULL MODEM cable. Start a Terminal program (e.g. Putty) shipped with your Windows operating system. The proper serial interface settings are 38400 Baud, 8 Databits, no parity and 1 Stopbit (38400 8N1). For computers where no serial interface is available a “Serial-to-USB” cable converter should be used instead.

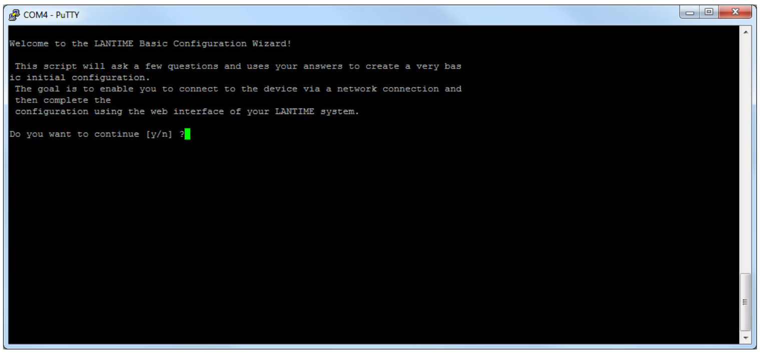
After the connection is successfully established use your login credentials in the welcome screen to enter a console.

Welcome to Meinberg LANTIME
login: _

Default settings are:
Login: **root**,
Password: **timeserver**.
(It may be the case to press a RETURN button again).

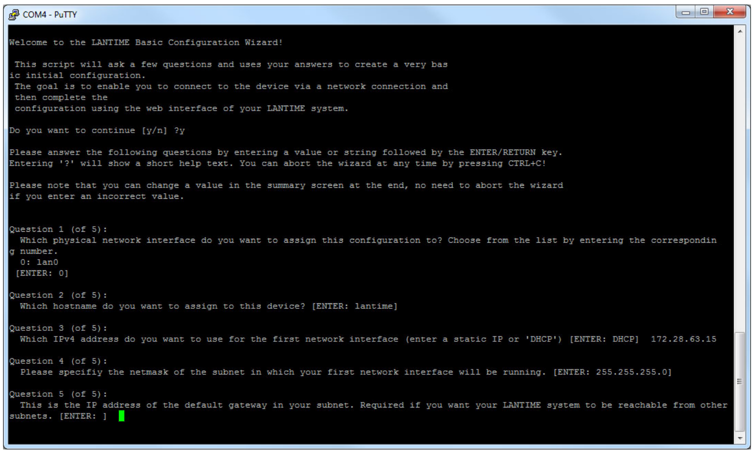
After successful registration change the current path to */wizard/*. Start now the LANTIME Basic Configuration Wizard with “startwizard”.

The following Wizard Welcome screen is now displayed:



```
Welcome to the LANTIME Basic Configuration Wizard!

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

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

Confirm with "y" to start the configuration for all the following settings.

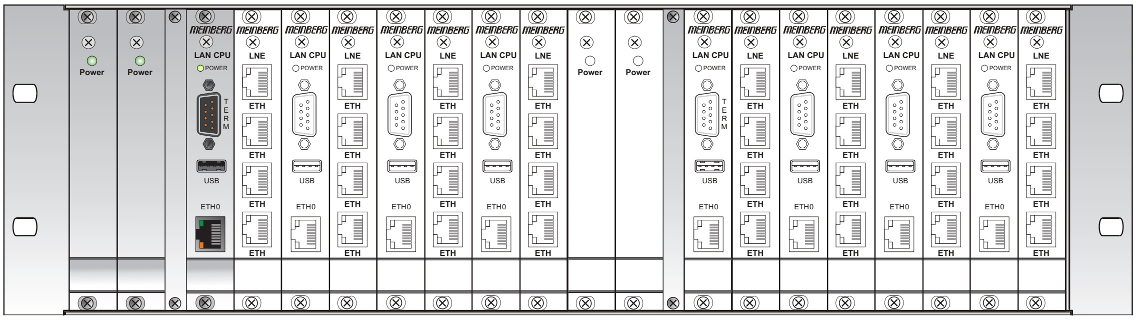


```
Welcome to the LANTIME Basic Configuration Wizard!

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

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

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

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


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

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

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

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

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

At the end please confirm your configuration.

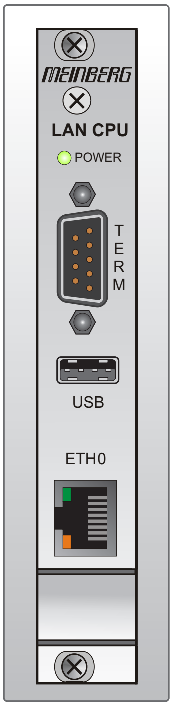
4 The Modular System LCES-NTP

LCES-NTP is a set of equipment composed of a LAN-CPU, LNE-cards together with power supply units (see chapter power supply), both installed in a metal 19" Modular chassis and ready to operate. The interfaces provided by LCES are accessible via connectors in the rear panel of the case. Details of the components are described below.



5 LAN CPU Time Server Module

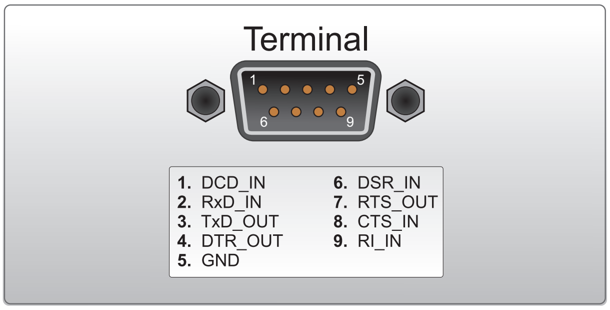
The Meinberg LANTIME CPU module transforms a Meinberg Radio Clock into a standalone "ready-to-run" NTP time server for TCP/IP networks, which comes with numerous possibities for management and configuration: web interface (HTTP/HTTPS), text based setup (TELNET/SSH) and SNMP. To transfer files (e.g. Firmware-updates)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



Technical specifications LAN CPU

PROCESSOR:	Geode^{TM} LX800 with 500 MHz
MAIN MEMORY:	256 MB
CACHE-MEMORY:	16 KB 2nd Level Cache
FLASHDISK:	1 GB
NETWORK CONNECTOR:	10/100 MBIT with RJ45-Jack
SERIAl - INTERFACE:	Four serial RS232-Ports 16550 compatible to FIFO - RS232 9-pol. DSUB-male connector - three RS232 male connector according to DIN 41612, type C 96 (only TxD, RxD, DCD)

To connect a serial terminal use the 9 pin SUBD RS232 connector in the front panel. Via the serial terminal connection it is possible to configure the parameters with a terminal program. To establish a connection between the LANTIME and a PC, use a NULL-MODEM cable. Configure your terminal program with 38400 Baud, 8 Databits, no parity and one Stopbit ((8N1). The terminal emulation has to be set to VT100. After connecting to the time server the login message will be displayed. Enter user name and password:



Default User: *root*; Password: *timeserver*

6 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, satelliet 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.

6.1 NTP Clients

The NTP software package was tested on different UNIX systems. Almost all UNIX-like systems come with a pre-installed NTP client software. In order to use the LANTIME as an NTP server, it is required to add its IP address to the client configuration. NTP client software are available for most other operating systems like Microsoft Windows or MAC OS.

The following WEB site is recommended to get the latest version of NTP:
http://www.ntp.org

You can find more information on our web page at: https://www.meinbergglobal.com/english/sw/ntp.htm

7 Introduction: Configuration LANTIME

There are several ways to configure the LANTIME parameters:

TELNET
SSH
HTTP Interface
Secure HTTP Interface (HTTPS)
Terminal in front panel (38400/8N1/VT100)
SNMP Management

In order to be able to configure the time server via the web interface or a telnet/SSH connection, an IP address has to be assigned via the front panel keys and LC/VF display (for automatic assignment possibilities please refer to: DHCP IPv4 or AUTOCONF IPv6). Once the IPv4 address, net mask and IPv4 GATEWAY have been set up or the network interface has been automatically configured with DHCP/Autoconf, further configuration changes can be done via a network connection:

Note: If the system doesn't has a display feature (e.g. LANTIME M100), goto chapter LANTIME Setup Wizard in this manual.

To set up a TELNET connection the following commands are entered:
telnet 198.168.10.10 // LANTIME IP
Default User: root
Default Password: timeserver

To set up a SSH connection the following commands are entered:
ssh root@198.168.10.10 // LANTIME IP
Default Password: timeserver

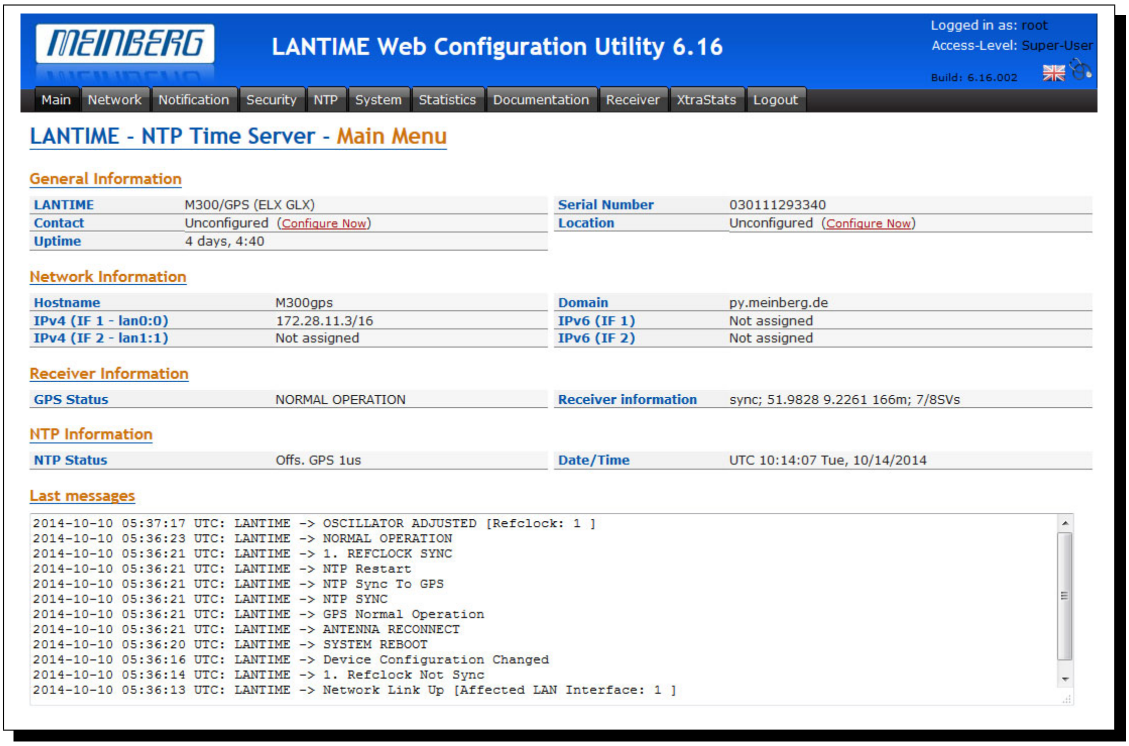
To set up a HTTP connection the following address is to enter in a web browser:
http://198.168.10.10 // LANTIME IP
Default User: root
Default Password: timeserver

To set up a Secure HTTP (HTTPS) connection the following address is entered in a web browser:
https://198.168.10.10 // LANTIME IP
Default User: root
Default Password: timeserver

8 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).

8.1 Configuration: Main Menu



LANTIME Web Configuration Utility 6.16

Logged in as: root
Access-Level: Super-User
Build: 6.16.002

LANTIME - NTP Time Server - Main Menu

General Information

LANTIME	M300/GPS (ELX GLX)	Serial Number	030111293340
Contact	Unconfigured (Configure Now)	Location	Unconfigured (Configure Now)
Uptime	4 days, 4:40		

Network Information

Hostname	M300gps	Domain	py.meinberg.de
IPv4 (IF 1 - lan0:0)	172.28.11.3/16	IPv6 (IF 1)	Not assigned
IPv4 (IF 2 - lan1:1)	Not assigned	IPv6 (IF 2)	Not assigned

Receiver Information

GPS Status	NORMAL OPERATION	Receiver information	sync; 51.9828 9.2261 166m; 7/8SVs

NTP Information

NTP Status	Offs. GPS 1us	Date/Time	UTC 10:14:07 Tue, 10/14/2014

Last messages

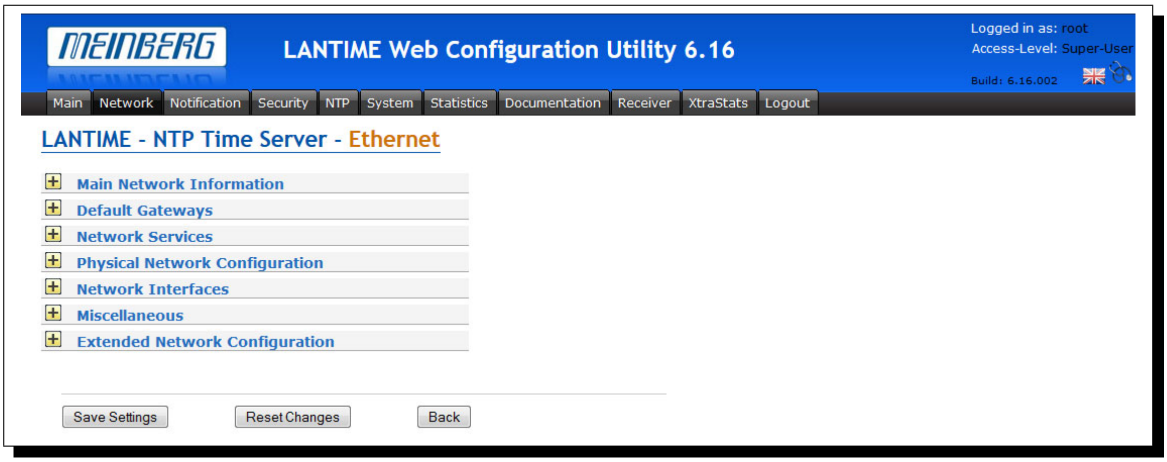
```
2014-10-10 05:37:17 UTC: LANTIME -> OSCILLATOR ADJUSTED [Refclock: 1 ]
2014-10-10 05:36:23 UTC: LANTIME -> NORMAL OPERATION
2014-10-10 05:36:21 UTC: LANTIME -> 1. REFCLOCK SYNC
2014-10-10 05:36:21 UTC: LANTIME -> NTP Restart
2014-10-10 05:36:21 UTC: LANTIME -> NTP Sync To GPS
2014-10-10 05:36:21 UTC: LANTIME -> NTP SYNC
2014-10-10 05:36:21 UTC: LANTIME -> GPS Normal Operation
2014-10-10 05:36:21 UTC: LANTIME -> ANTENNA RECONNECT
2014-10-10 05:36:20 UTC: LANTIME -> SYSTEM REBOOT
2014-10-10 05:36:16 UTC: LANTIME -> Device Configuration Changed
2014-10-10 05:36:14 UTC: LANTIME -> 1. Refclock Not Sync
2014-10-10 05:36:13 UTC: LANTIME -> Network Link Up [Affected LAN Interface: 1 ]
```

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.

- Information about LANTIME model and software
- Network information - first interface
- Receiver status
- NTP status
- PTP status (option)
- Last messages

The field in the lower 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 navigation on top of the page you can reach a number of configuration menus, which are described in the following chapters.

8.2 Configuration: Network



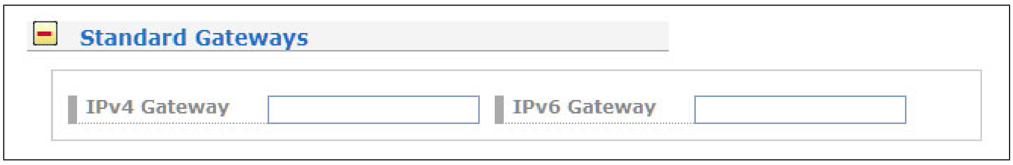
Logged in as: root
Access-Level: Super-User
Build: 6.16.002

LANTIME - NTP Time Server - Ethernet

In the network configuration all parameters related to the network interfaces can be changed. In the first section you can edit the hostname and domain name. You can also specify two nameserver - in the nameserver field you may enter an IPv4 or IPv6 address.

8.2.1 Network interface specific configuration

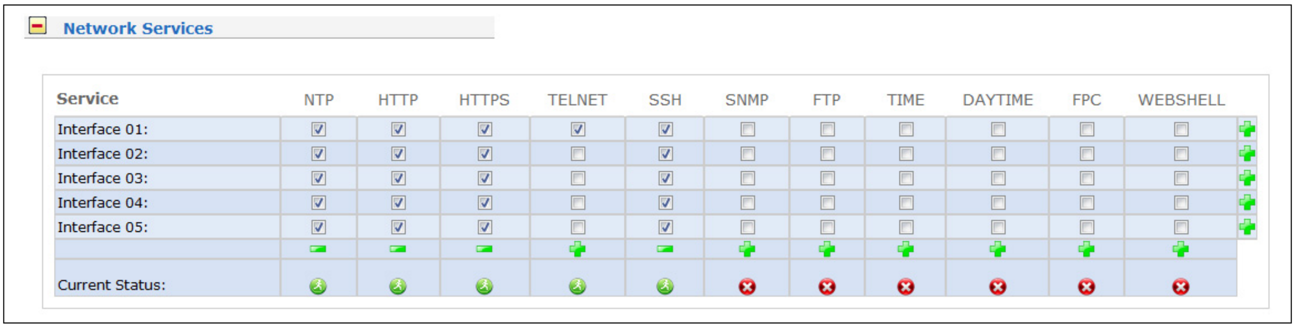
Standard Gateways:



IPv4 Gateway		IPv6 Gateway	

In this Subsection you can enter a Default Gateway for IPv4 and IPv6

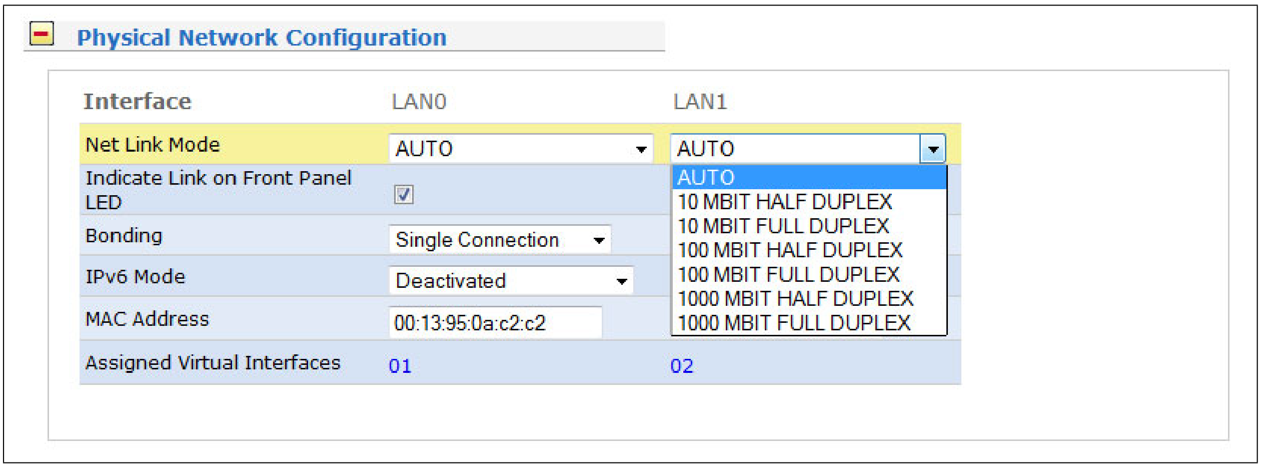
Network Services



Service	NTP	HTTP	HTTPS	TELNET	SSH	SNMP	FTP	TIME	DAYTIME	FPC	WEBSHELL	
Interface 01:	☑	☑	☑	☑	☑	□	□	□	□	□	□	+
Interface 02:	☑	☑	☑	□	☑	□	□	□	□	□	□	+
Interface 03:	☑	☑	☑	□	☑	□	□	□	□	□	□	+
Interface 04:	☑	☑	☑	□	☑	□	□	□	□	□	□	+
Interface 05:	☑	☑	☑	□	☑	□	□	□	□	□	□	+
	−	−	−	+	−	+	+	+	+	+	+	
Current Status:	●	●	●	●	●	✗	✗	✗	✗	✗	✗	

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

Physical Network Configuration



Physical Network Configuration

Interface	LAN0	LAN1
Net Link Mode	AUTO	AUTO
Indicate Link on Front Panel LED	☑	
Bonding	Single Connection	
IPv6 Mode	Deactivated	
MAC Address	00:13:95:0a:c2:c2	
Assigned Virtual Interfaces	01	02

The "Net Link Mode" controls the port speed and duplex mode of the selected Ethernet port. Under normal circumstances, you should leave the default setting (AUTO) untouched, until your network administrator tells you to change it.

Possible values are:
AUTO — Autonegotiation or Autosensing - the link mode is set up automatically..

10 MBIT HALF DUPLEX
100 MBIT HALF DUPLEX
1000 MBIT HALF DUPLEX — Transmission of information in both direction of the channel - but not at the same time, only alternate.

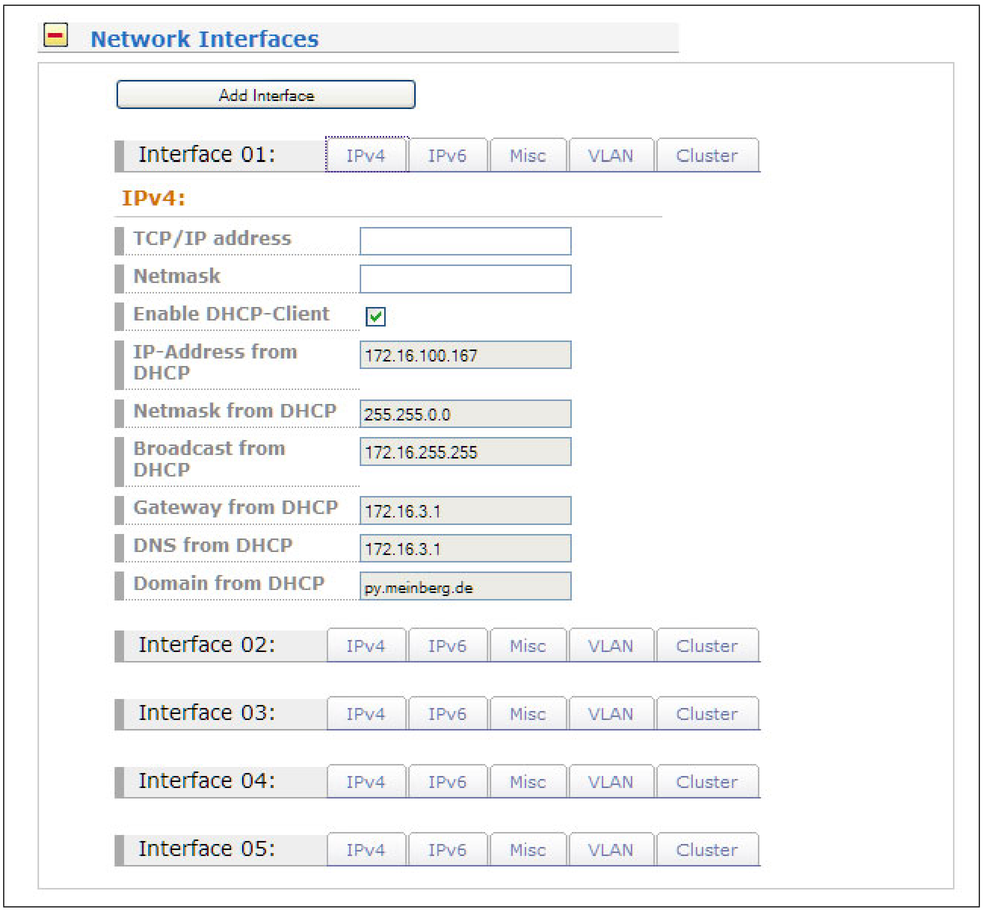
10 MBIT FULL DUPLEX
100 MBIT FULL DUPLEX
1000 MBIT FULL DUPLEX — The simultaneous transmission of data in both directions is possible in Full Duplex mode.

Further configurations:
With the checkbox you can activate the Network LED at the front panel of your LANTIME for the corresponding physical network interface and you can activate/deactivate IPv6 mode in the drop down list.

Network Interfaces:

Here you can edit/select parameters for IPv4 and IPv6. 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 and FTP 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.

For each physical network interface you find a seperate submenu after first start of the device. The parameters of the interfaces are editable with the context menu (see chapter "IPv4 addresses and DHCP").



Interface 01:

IPv4:

TCP/IP address

Netmask

Enable DHCP-Client ☑

IP-Address from DHCP 172.16.100.167

Netmask from DHCP 255.255.0.0

Broadcast from DHCP 172.16.255.255

Gateway from DHCP 172.16.3.1

DNS from DHCP 172.16.3.1

Domain from DHCP py.meinberg.de

Interface 02:

Interface 03:

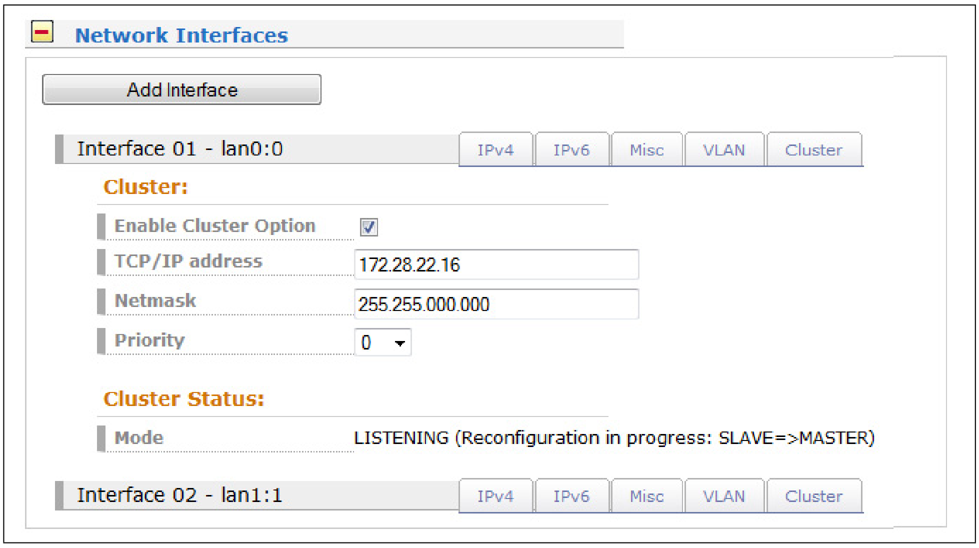
Interface 04:

Interface 05:

NTP Cluster

To enable NTP redundancy for network clients, which can only communicate with one time server, multiple time servers can be assigned to a cluster.

For this purpose, the selected interfaces of the involved time servers are assigned to a common cluster-IP. The NTP-clients can send their NTP-requests to this cluster-IP. The current master sends its NTP packets via this IP to the clients.



Interface 01 - lan0:0

Cluster:

Enable Cluster Option ☑

TCP/IP address 172.28.22.16

Netmask 255.255.000.000

Priority 0

Cluster Status:

Mode LISTENING (Reconfiguration in progress: SLAVE=>MASTER)

Interface 02 - lan1:1

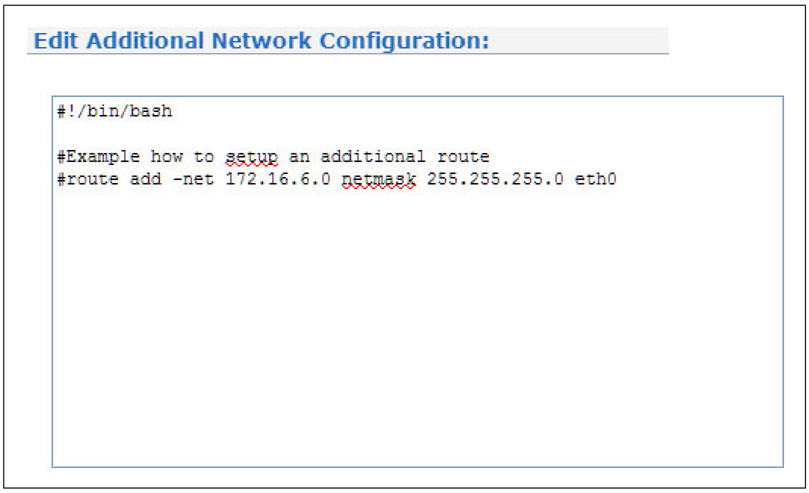
In our example, we will choose the virtual port 01 (assigned to the physical interface LAN 0 of this time server) as cluster port. The cluster tag of this interface is selected and the corresponding fields are filled with the cluster-IP and subnet-mask, as shown in the dialog screen above.

The same cluster IP configuration is entered on all involved NTP servers in the cluster. If you want to set the priority of a particular server as master, then the priority value in the list must be set to a smaller value than the value of the other servers in the cluster.

The MASTER server is chosen according to parameters in the following order:
1. NTP status (sync, not sync);
2. Priority (user configurable, the lower value the higher priority, default value is 0
3. Ref Clock Type - GNSS receiver has the highest rating
4. Ref Clock Status (sync, not sync)

Extended Network Configuration

With the submenu "Extended 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.


Edit Additional Network Configuration:

```
#!/bin/bash

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

8.2.2 IPv4 addresses and DHCP

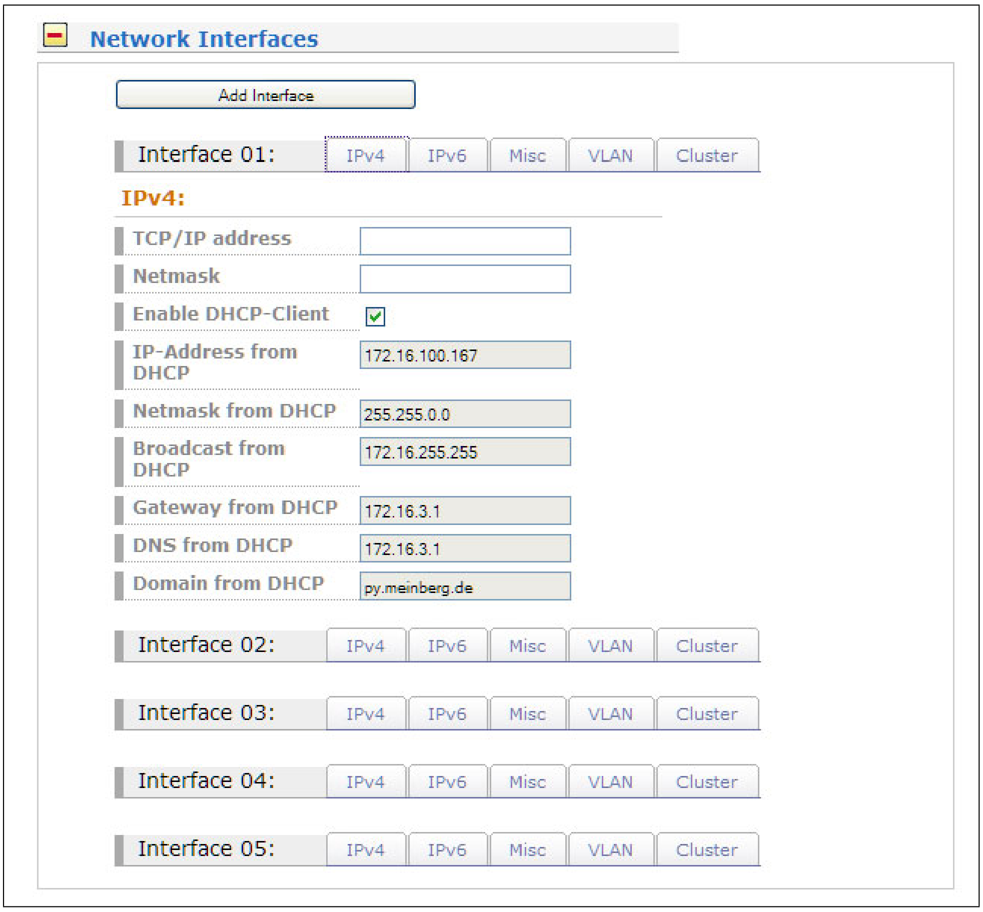
IPv4 addresses are built of 32 bits, which are grouped in four octets, each containing 8 bits. You can specify an IP address in this mask by entering four decimal numbers, separated by a point ".".

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.



Network Interfaces

Interface 01:

IPv4:

TCP/IP address	
Netmask	
Enable DHCP-Client	☑
IP-Address from DHCP	172.16.100.167
Netmask from DHCP	255.255.0.0
Broadcast from DHCP	172.16.255.255
Gateway from DHCP	172.16.3.1
DNS from DHCP	172.16.3.1
Domain from DHCP	py.meinberg.de

Interface 02:

Interface 03:

Interface 04:

Interface 05:

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

8.2.3 IPv6 addresses and autoconf

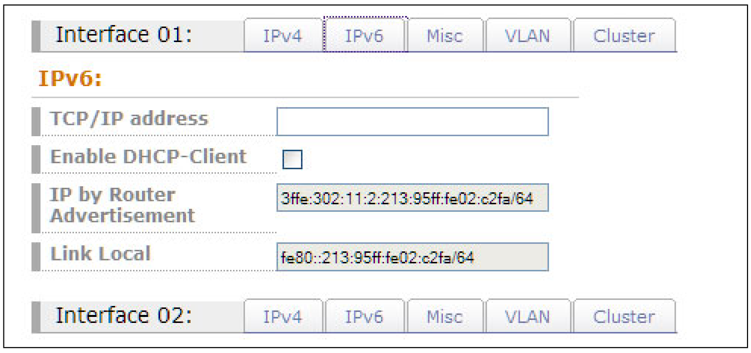
You can specify up to three IPv6 addresses for your LANTIME timeserver. Additionally you can switch off the IPv6 autoconf feature. IPv6 addresses are 128 bits in length and written as a chain of 16bit numbers in hexadecimal notation, separated with colons. A sequence of zeros can be substituted with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



IPv6:

TCP/IP address

Enable DHCP-Client □

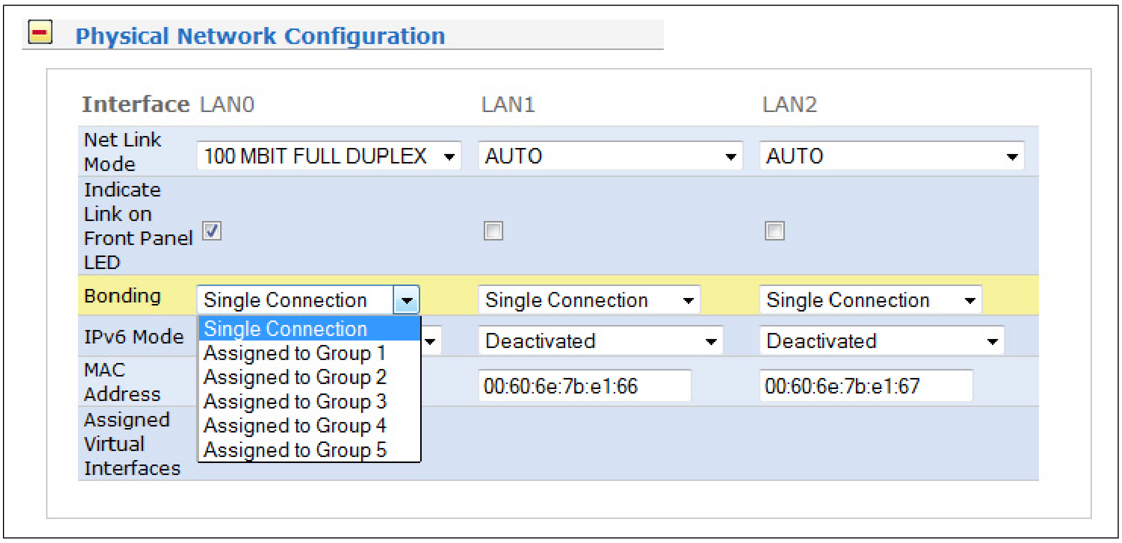
IP by Router Advertisement 3ffe:302:11:2:213:95ff:fe02:c2fa/64

Link Local fe80::213:95ff:fe02:c2fa/64

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.

8.2.4 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.

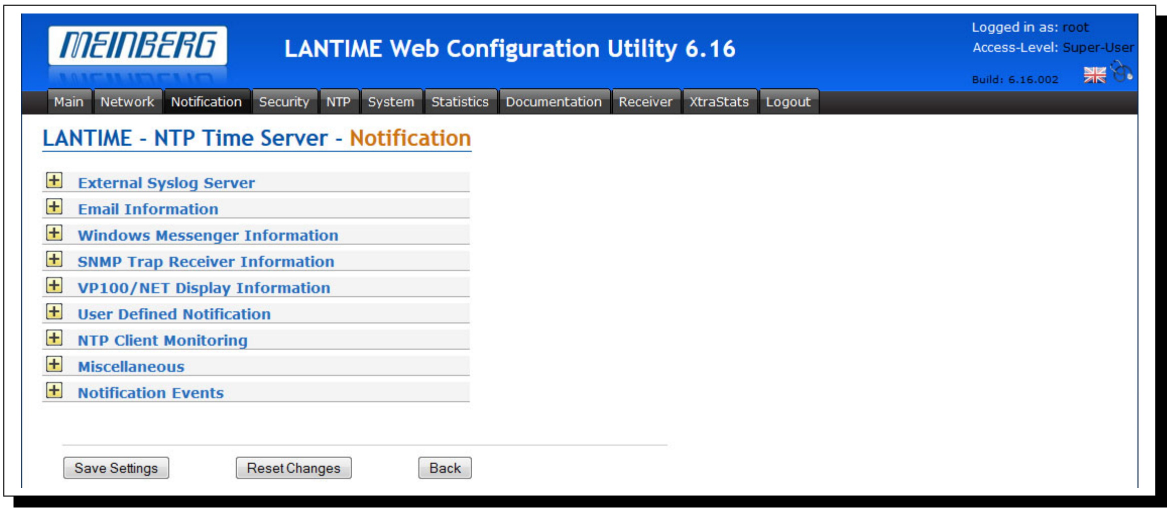


Physical Network Configuration

Interface	LAN0	LAN1	LAN2
Net Link Mode	100 MBIT FULL DUPLEX	AUTO	AUTO
Indicate Link on Front Panel LED	☑	□	□
Bonding	Single Connection	Single Connection	Single Connection
IPv6 Mode		Deactivated	Deactivated
MAC Address		00:60:6e:7b:e1:66	00:60:6e:7b:e1:67
Assigned Virtual Interfaces			

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.

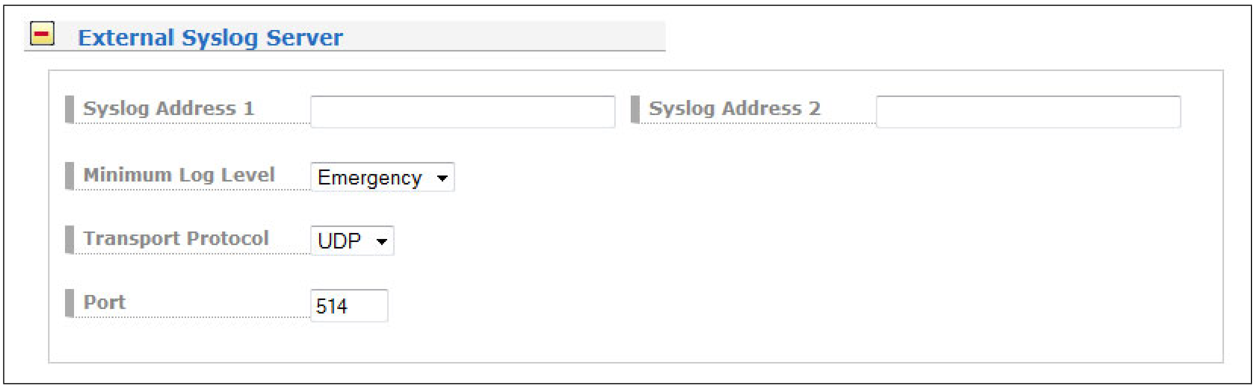
8.3 Configuration: Notification



8.3.1 SYSLOG Server

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

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



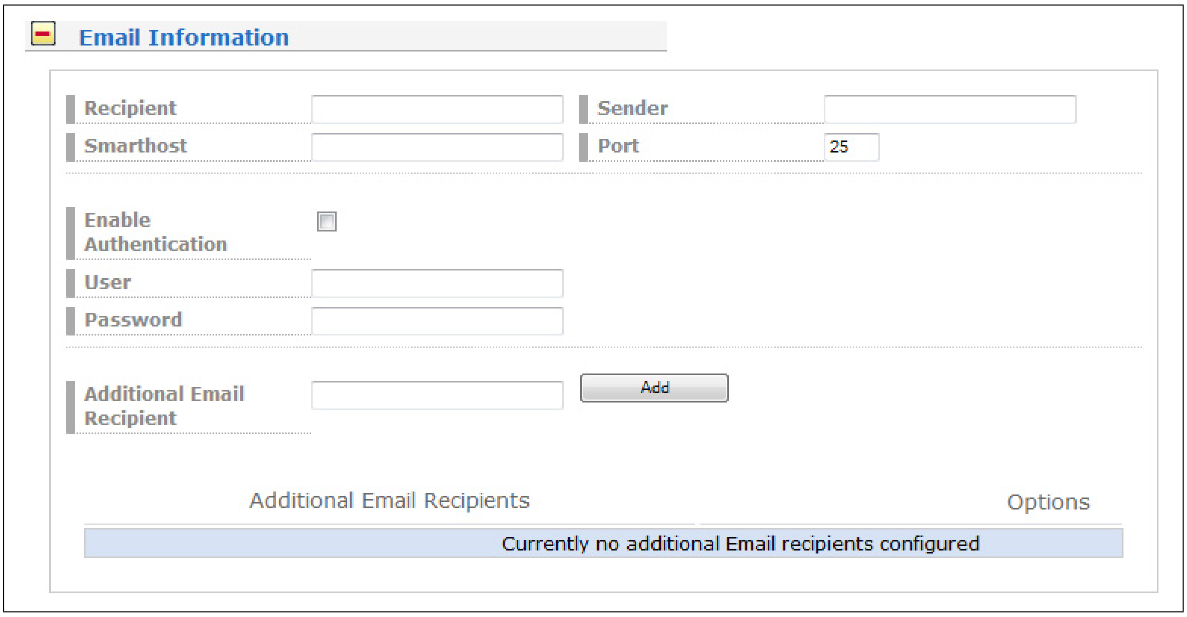
Syslog Address 1:
Syslog Address 2:
Minimum Log Level: Emergency
Transport Protocol: UDP
Port: 514

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.

8.3.2 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.



Email Information

Recipient		Sender	
Smarthost		Port	25

Enable Authentication □

User

Password

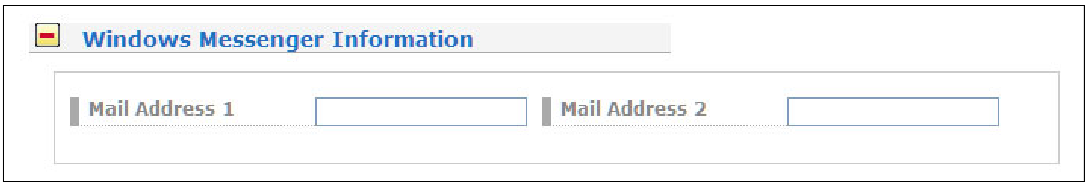
Additional Email Recipient

Additional Email Recipients	Options
Currently no additional Email recipients configured	

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

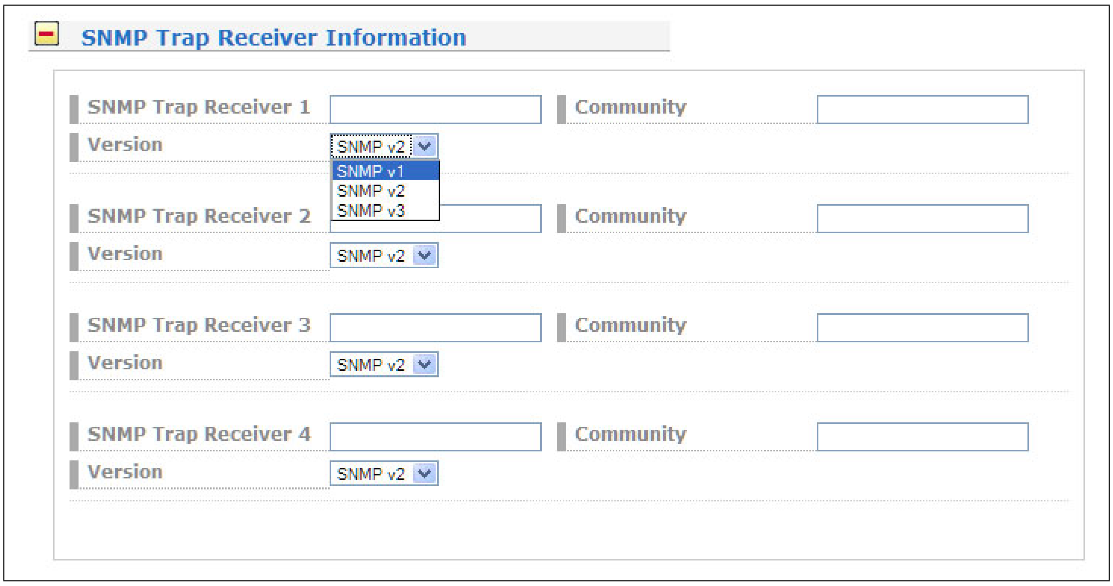
8.3.3 Windows Messenger Information



Windows Messenger Information

Mail Address 1		Mail Address 2	

8.3.4 SNMP-TRAP messages



SNMP Trap Receiver Information

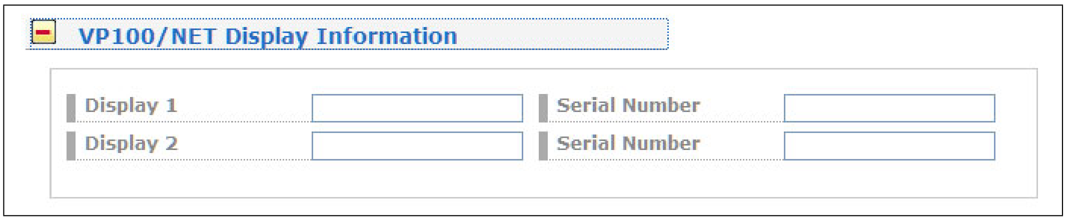
SNMP Trap Receiver 1		Community	
Version	SNMP v2		
SNMP Trap Receiver 2		Community	
Version	SNMP v2		
SNMP Trap Receiver 3		Community	
Version	SNMP v2		
SNMP Trap Receiver 4		Community	
Version	SNMP v2		

Up to four independent 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).

8.3.5 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.



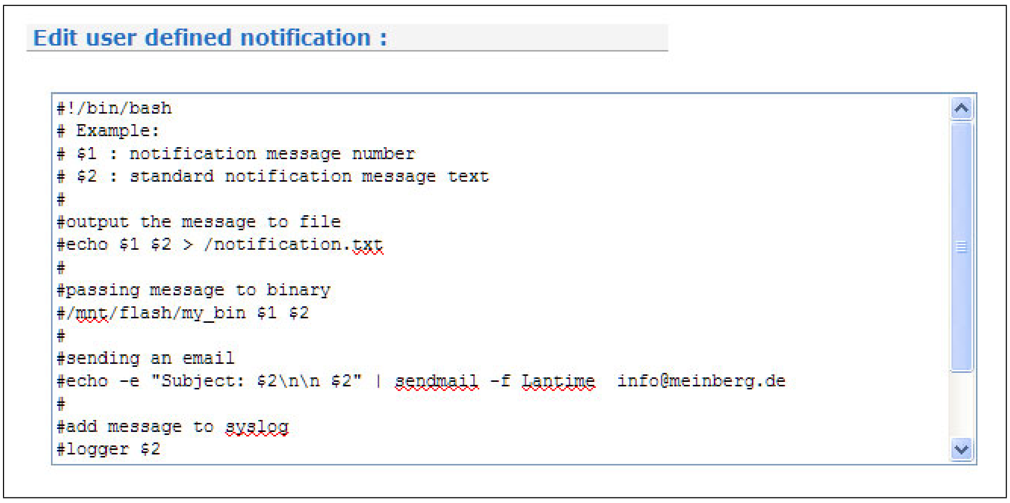
VP100/NET Display Information

Display 1		Serial Number	
Display 2		Serial Number	

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.

8.3.6 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.



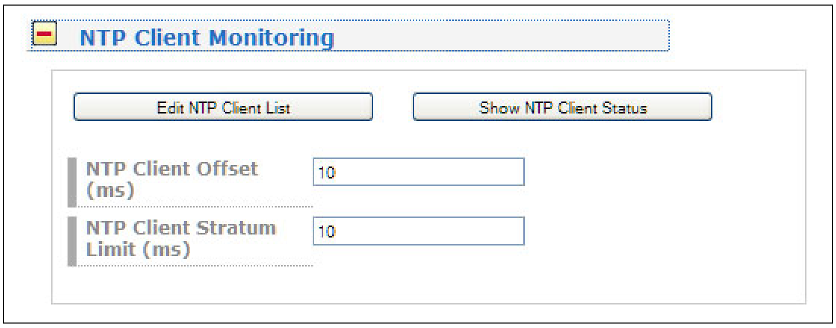
Edit user defined notification :

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

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.

8.3.7 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:



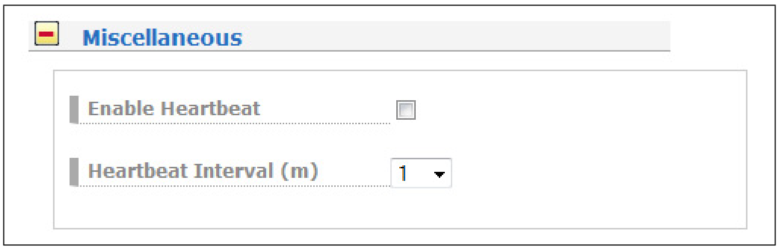
NTP Client Monitoring

NTP Client Offset (ms): 10

NTP Client Stratum Limit (ms): 10

You can monitor the current states of the configured clients:

8.3.8 Miscellaneous



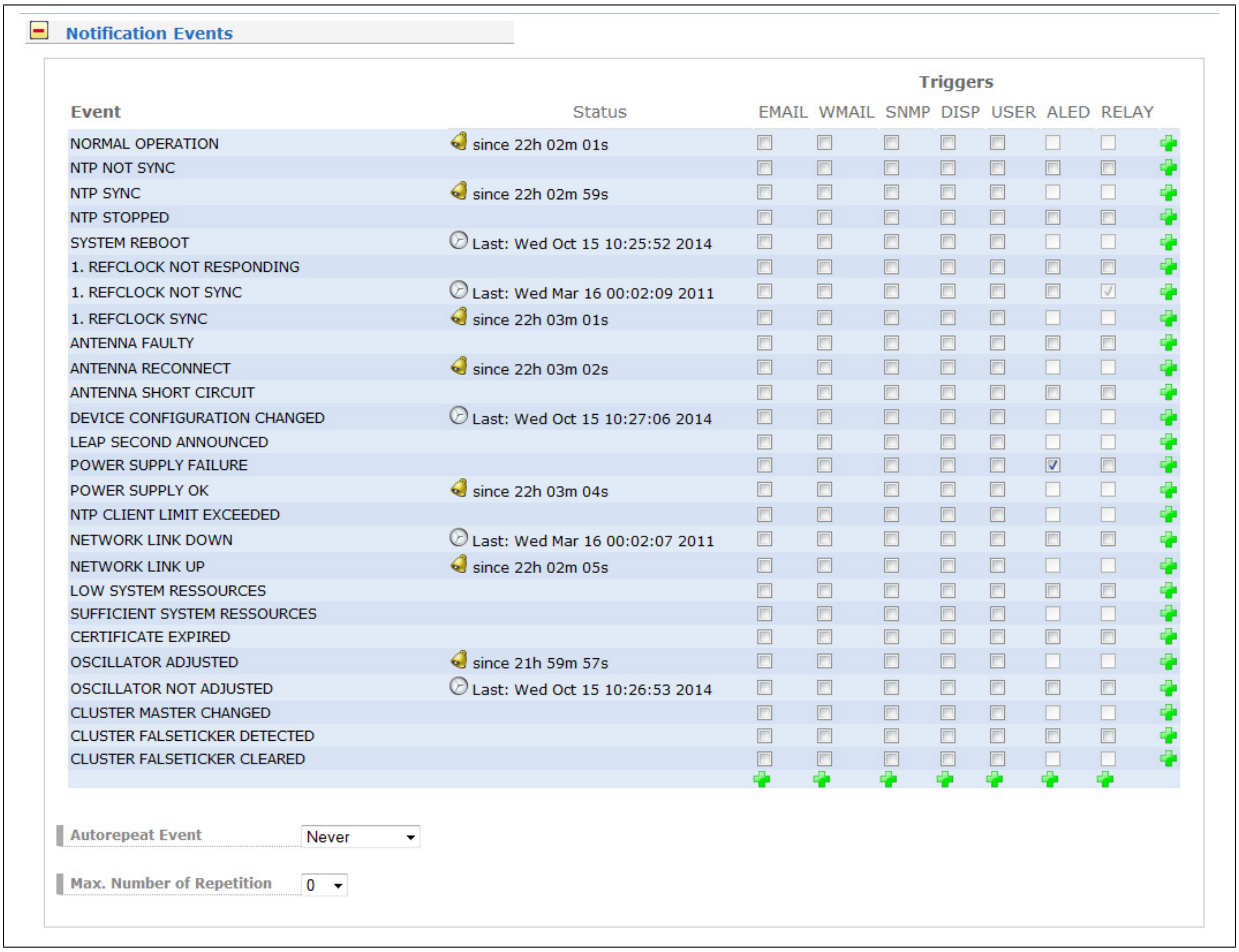
Miscellaneous

Enable Heartbeat □

Heartbeat Interval (m) 1

A heartbeat is a periodic signal generated by hardware or software to indicate normal operation or to synchronize other parts of a system. Usually a heartbeat is sent between machines at a regular interval on the order of seconds. If a heartbeat isn't received for a time - usually a few heartbeat intervals - the machine that should have sent the heartbeat is assumed to have failed.

8.3.9 Alarm events



Notification Events

Event	Status	EMAIL	WMAIL	SNMP	DISP	USER	ALED	RELAY	
NORMAL OPERATION	since 22h 02m 01s	□	□	□	□	□	□	□	+
NTP NOT SYNC		□	□	□	□	□	□	□	+
NTP SYNC	since 22h 02m 59s	□	□	□	□	□	□	□	+
NTP STOPPED		□	□	□	□	□	□	□	+
SYSTEM REBOOT	Last: Wed Oct 15 10:25:52 2014	□	□	□	□	□	□	□	+
1. REFCLOCK NOT RESPONDING		□	□	□	□	□	□	□	+
1. REFCLOCK NOT SYNC	Last: Wed Mar 16 00:02:09 2011	□	□	□	□	□	□	☑	+
1. REFCLOCK SYNC	since 22h 03m 01s	□	□	□	□	□	□	□	+
ANTENNA FAULTY		□	□	□	□	□	□	□	+
ANTENNA RECONNECT	since 22h 03m 02s	□	□	□	□	□	□	□	+
ANTENNA SHORT CIRCUIT		□	□	□	□	□	□	□	+
DEVICE CONFIGURATION CHANGED	Last: Wed Oct 15 10:27:06 2014	□	□	□	□	□	□	□	+
LEAP SECOND ANNOUNCED		□	□	□	□	□	□	□	+
POWER SUPPLY FAILURE		□	□	□	□	□	☑	□	+
POWER SUPPLY OK	since 22h 03m 04s	□	□	□	□	□	□	□	+
NTP CLIENT LIMIT EXCEEDED		□	□	□	□	□	□	□	+
NETWORK LINK DOWN	Last: Wed Mar 16 00:02:07 2011	□	□	□	□	□	□	□	+
NETWORK LINK UP	since 22h 02m 05s	□	□	□	□	□	□	□	+
LOW SYSTEM RESSOURCES		□	□	□	□	□	□	□	+
SUFFICIENT SYSTEM RESSOURCES		□	□	□	□	□	□	□	+
CERTIFICATE EXPIRED		□	□	□	□	□	□	□	+
OSCILLATOR ADJUSTED	since 21h 59m 57s	□	□	□	□	□	□	□	+
OSCILLATOR NOT ADJUSTED	Last: Wed Oct 15 10:26:53 2014	□	□	□	□	□	□	□	+
CLUSTER MASTER CHANGED		□	□	□	□	□	□	□	+
CLUSTER FALSETICKER DETECTED		□	□	□	□	□	□	□	+
CLUSTER FALSETICKER CLEARED		□	□	□	□	□	□	□	+
		+	+	+	+	+	+	+	

Autorepeat Event: Never

Max. Number of Repetition: 0

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 (read section "User defined Alarm scripts") and the error relay out.

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

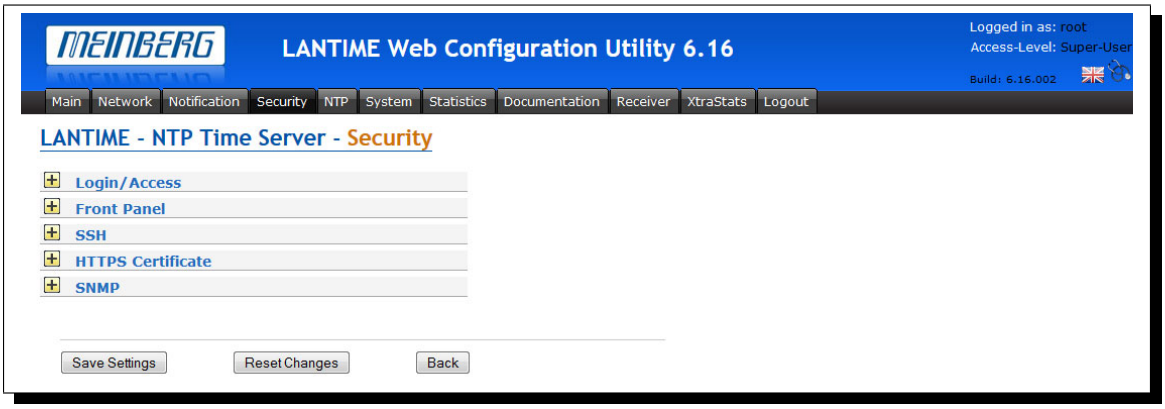
Trapname	**Cleared By**
NTPStopped	NTPNotSync or NTP Sync
NTPNotSync	NTPSync
ReceiverNotResponding	ReceiverNotSync or ReceiverSync
ReceiverNotSync	ReceiverSync
AntennaFaulty	AntennaReconnect
SecondaryRecNotSync	SecondaryRecSync
PowerSupplyFailure	PowerSupplyUp
NetworkDown	NetworkUp
SecondaryRecNotResp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

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

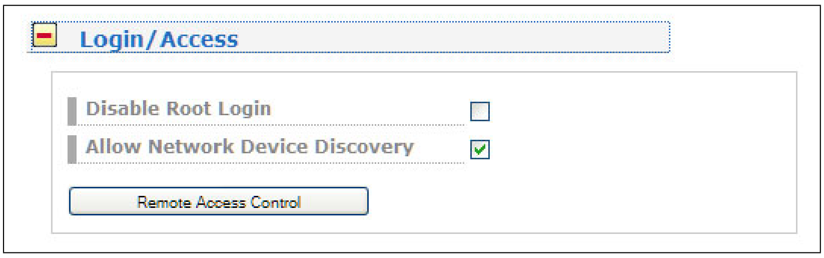
- mbgLtTrapConfigChanged
- mbgLtTrapLeapSecondAnnounced
- mbgLtTrapServerBoot

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.

8.4 Configuration: Security

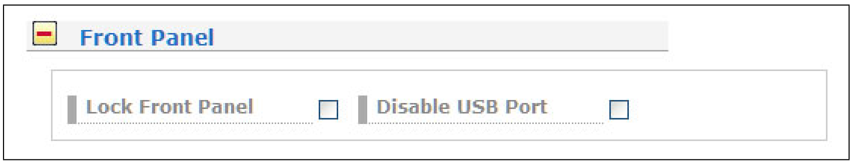


8.4.1 HTTP Access Control



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

8.4.2 Front Panel



With the checkboxes the frontpanel and USB port of the LANTIME can be locked.

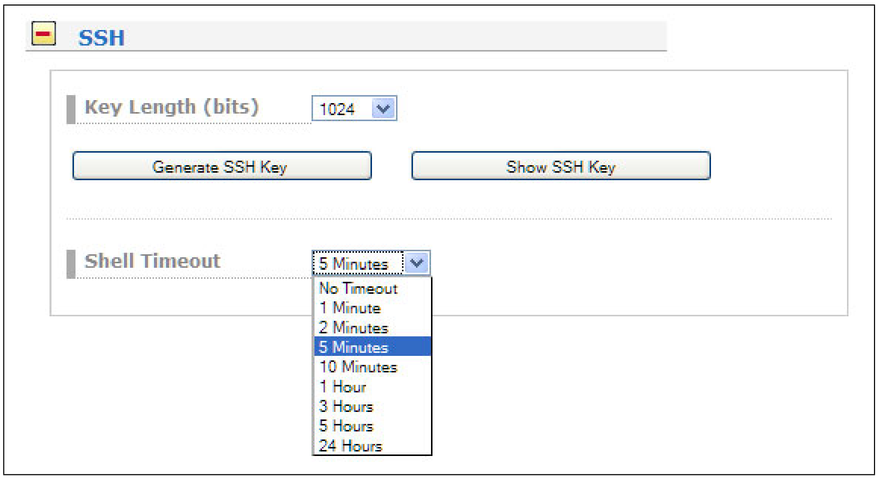
8.4.3 SSH Secure Shell Login

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).



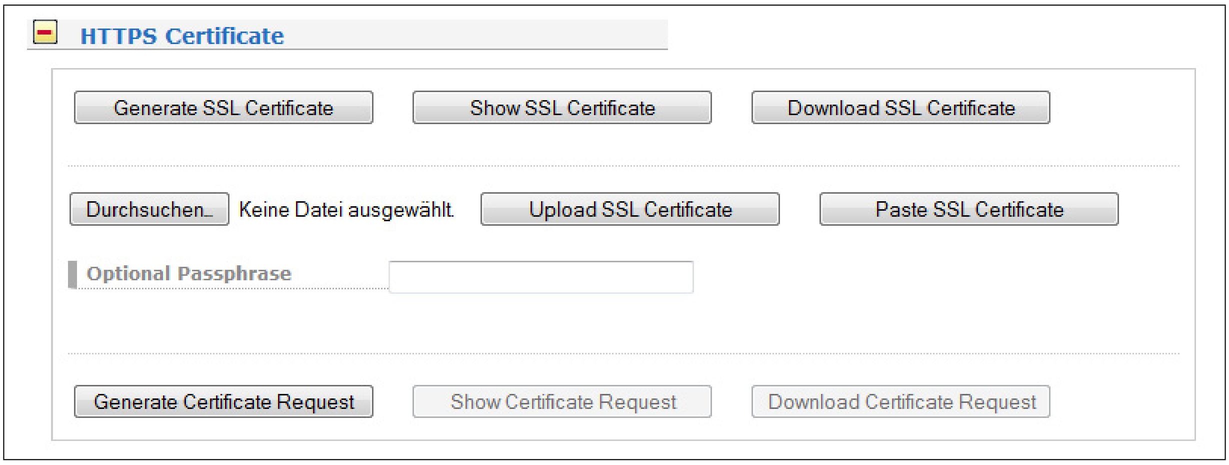
Key Length (bits) 1024

Shell Timeout 5 Minutes

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.

8.4.4 Generate SSL Certificate for HTTPS

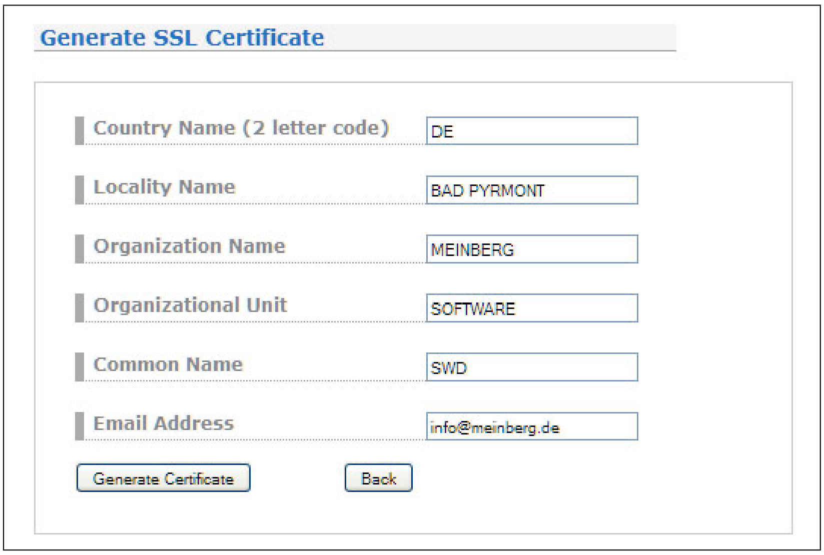
HTTPS is the standard for encrypted transmission of data between web browser and web server. It relies on X.509 certificates and asymmetric crypto procedures. The timeserver uses these certificates to authenticate itself to the client (web browser). The first time a web browser connects to the HTTPS 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.



Keine Datei ausgewählt.

Optional Passphrase

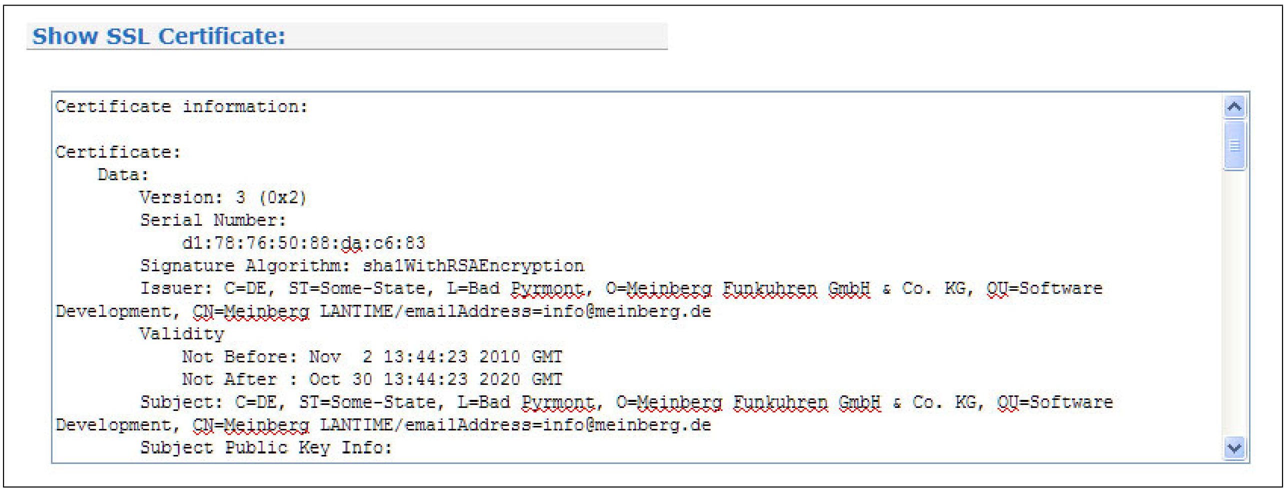
By using the button "Generate SSL certificate for HTTP" you can create a new certificate. Please enter your organisation, name, mail address and the location in the upcoming form and press "Generate SSL certificate" to finally generate it.



Generate SSL Certificate

Country Name (2 letter code)	DE
Locality Name	BAD PYRMONT
Organization Name	MEINBERG
Organizational Unit	SOFTWARE
Common Name	SWD
Email Address	info@meinberg.de

After the successful generation of the certificate and with the button "SSL..." the certificate is shown to you in the tetxtarea:



Show SSL Certificate:

```
Certificate information:

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d1:78:76:50:88:da:c6:83
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, ST=Some-State, L=Bad Pyrmont, O=Meinberg Funkuhren GmbH & Co. KG, OU=Software
Development, CN=Meinberg LANTIME/emailAddress=info@meinberg.de
        Validity
            Not Before: Nov  2 13:44:23 2010 GMT
            Not After : Oct 30 13:44:23 2020 GMT
        Subject: C=DE, ST=Some-State, L=Bad Pyrmont, O=Meinberg Funkuhren GmbH & Co. KG, OU=Software
Development, CN=Meinberg LANTIME/emailAddress=info@meinberg.de
        Subject Public Key Info:
```

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

Uploading certified SSL Certificates

A certificate which is certified by a certification authority (CA) can be installed using the "Upload SSL Certificate" button. This certificate must be in PEM file format, it must contain a private key and the certificate itself.

The content of the private key starts with
"—–BEGIN RSA PRIVATE KEY—–"
and ends with
"—–END RSA PRIVATE KEY—–"

the certificate itself starts with
"—–BEGIN CERTIFICATE—–"
and ends with
"—–END CERTIFICATE—–".

This example is an excerpt from a PEM file:

```
---BEGIN RSA PRIVATE KEY---
MIICXQIBAAKBgQC6FkGxyJ6+Bqxzfp3bNtEYyiRIAbQAIsHblYPG7aQk+8XbIXWB
...
aiLbmu7N3TEdWVDgro8kMuQC/Ugkttx7TdJJbqJoVsF5
---END RSA PRIVATE KEY---
---BEGIN CERTIFICATE---
MIIEJTCCA46gAwIBAgIJANF4dlCI2saDMA0GCSqGSIb3DQEBBQUAMIG+MQswCQYD
...
ekZ970dAaPca
---END CERTIFICATE---
```

IMPORTANT: The certificate should not be protected with a password, otherwise the web server cannot start automatically.

Uploading certified Multi-Level / chained Certificates

Steps below require an SSH access to your timeserver.

In addition to SSL certificates, also multi-level / chained certificates are supported. In this case, a private key and a certificate chain are divided into two files, which are both in a PEM format. The actual PEM file contains the private key which is enclosed between BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY line as shown above. The CA-file on the other hand contains the certificate chain, where each single certificate is enclosed between BEGIN and END CERTIFICATE line as shown above.

The PEM file that contains the private key should be copied manually to *"/etc/https.pem"* and the CA to *"/etc/https_cert.pem"*.

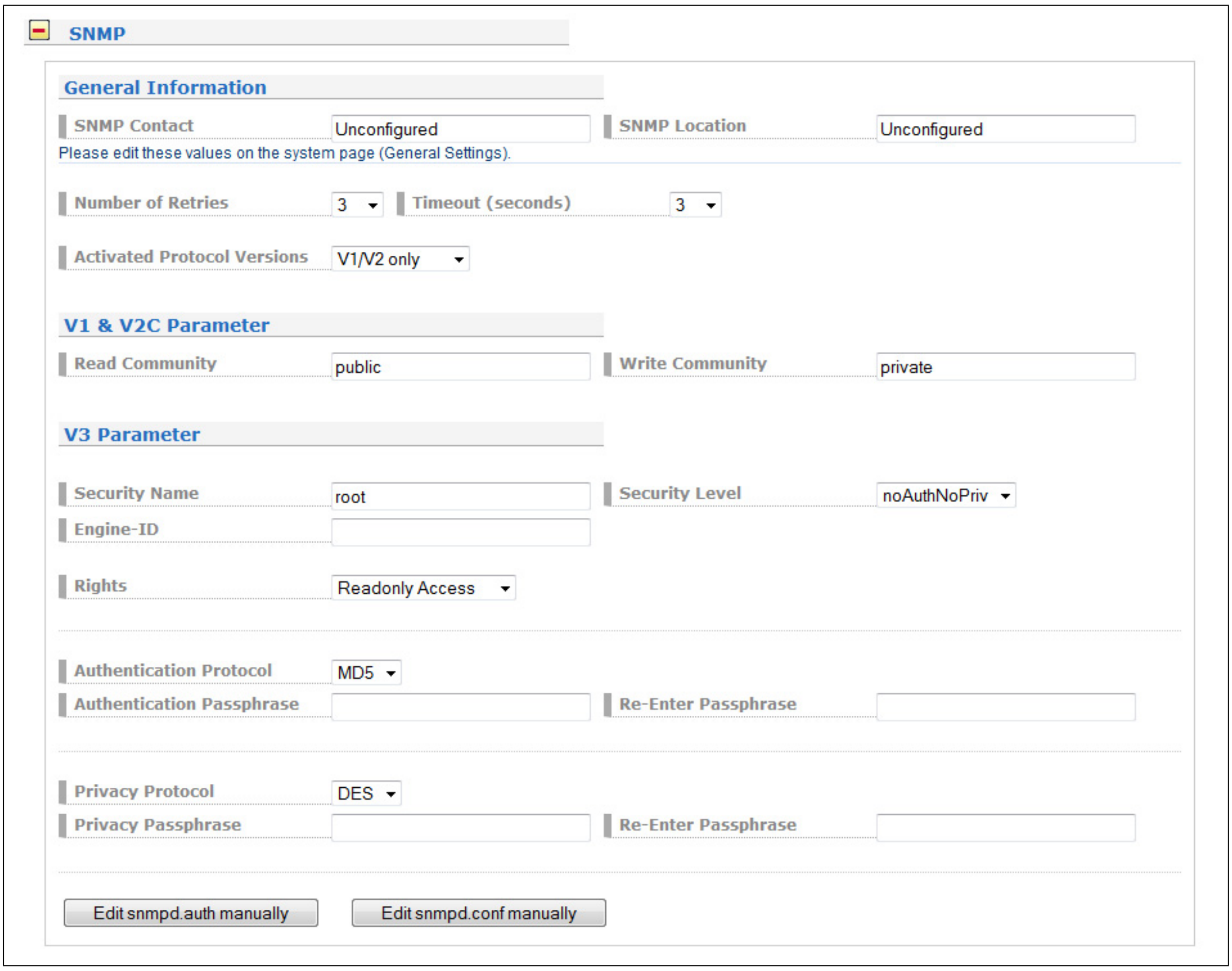
Subsequently, the line 'ssl.ca-file = "/etc/https_cert.pem"' should be added in a server configuration file *"/etc/httpsd.conf"*.

Running the command "saveconfig" saves the settings persistently, the command "restart https" applies the settings.

Please Note: the certificates should not be protected with a password for the reasons stated above.

8.4.5 SNMP Parameter

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



SNMP

General Information

SNMP Contact: Unconfigured
SNMP Location: Unconfigured

Please edit these values on the system page (General Settings).

Number of Retries: 3
Timeout (seconds): 3

Activated Protocol Versions: V1/V2 only

V1 & V2C Parameter

Read Community: public
Write Community: private

V3 Parameter

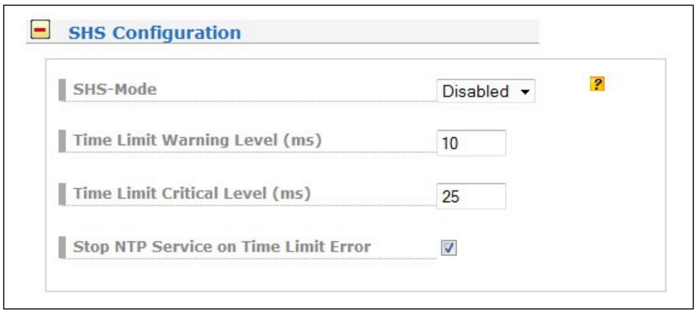
Security Name: root
Security Level: noAuthNoPriv
Engine-ID:

Rights: Readonly Access

Authentication Protocol: MD5
Authentication Passphrase:
Re-Enter Passphrase:

Privacy Protocol: DES
Privacy Passphrase:
Re-Enter Passphrase:

8.4.6 SHS Configuration



SHS Configuration

SHS-Mode: Disabled

Time Limit Warning Level (ms): 10

Time Limit Critical Level (ms): 25

Stop NTP Service on Time Limit Error: ☑

SHS Parameter
SHS is the abbrevation of Secure Hybrid Systems and is available on systems with two reference clocks. It provide a plausibility mode where the incoming times of both time signals are continuously compared against each other. Only if the time difference between those reference times does not exceed a certain limit (configurable) it will give over the time to the NTP service. Otherwise the time output is stopped immediately.

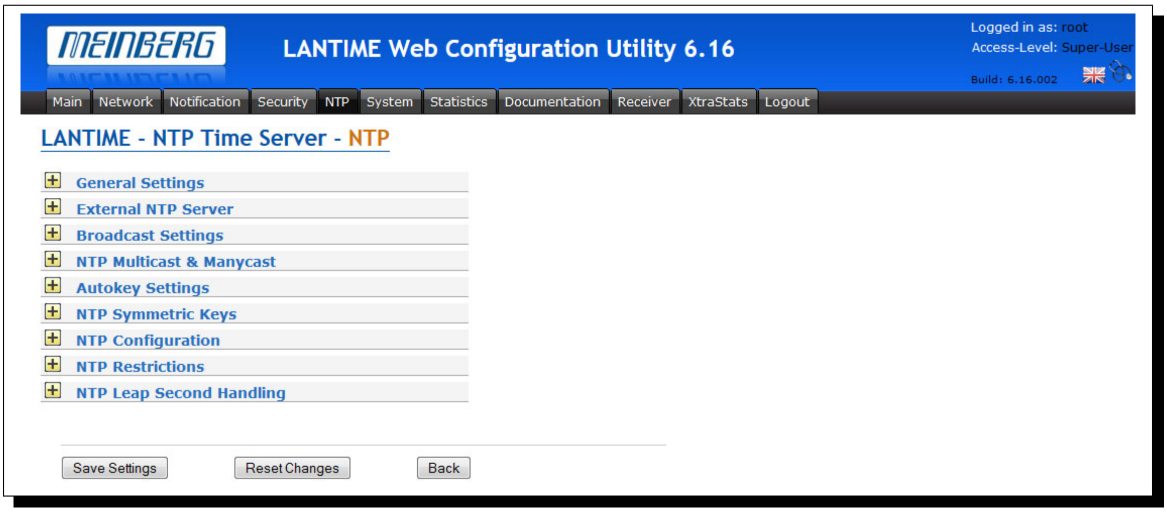
SHS-Mode
This parameter is used to activate the SHS feature and with it the comparison of time. If the SHS mode is disabled the times of both receivers are passed directly to the NTP service. The NTP service decide autonomous which reference time will be used. In case of the master reference time got unavailable the NTP service just switch over to the other time source.

Time Limit Warning Level(ms)
This value indicate at which calculated time difference between the two reference times an alarm is generated over the built-in notifcation system. The warning level indicate that the reference times are no longer equal and that a time error may be imminent. The NTP service is still receiving the time from the SHS system.

Time Limit Error Level(ms)
This value indicate at which difference the time output to NTP is stopped and an appropriate alarm is generated over the built-in notification system. If the SHS error was triggered an administrator action is needed to bring the NTP service back to normal operation. The administrator must check the times of both receiver and confirm that everything is ok. An appropriate dialog is shown on the web interface. After affirmation the handover of time to the NTP service is resumed and NTP will resynchronize.

Stop NTP Service on Time Limit Error
This parameter is used to decide whether the NTP service is stopped directly in case of a time limit error. In this case no NTP client got an answer anymore from the time server.

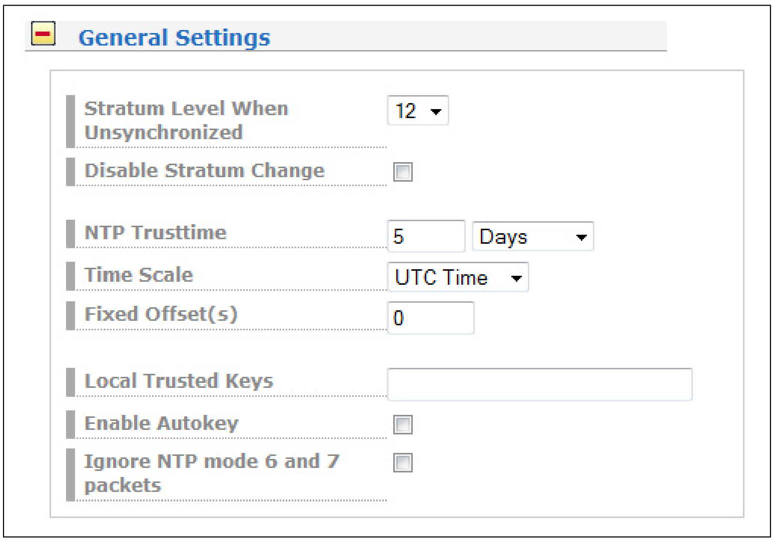
8.5 Configuration: NTP



Logged in as: root
Access-Level: Super-User
Build: 6.16.002

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

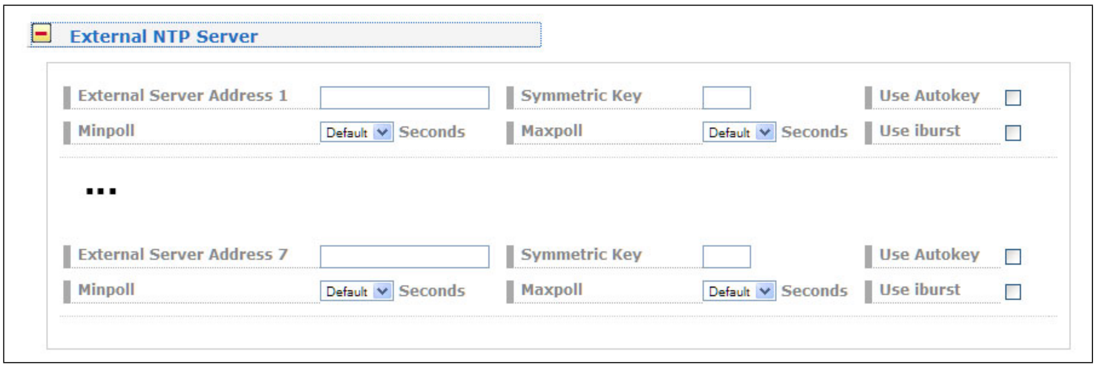
8.5.1 General Settings



Stratum Level When Unsynchronized: 12
Disable Stratum Change: □
NTP Trusttime: 5 Days
Time Scale: UTC Time
Fixed Offset(s): 0
Local Trusted Keys:
Enable Autokey: □
Ignore NTP mode 6 and 7 packets: □

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.

8.5.2 External NTP Server



External NTP Server

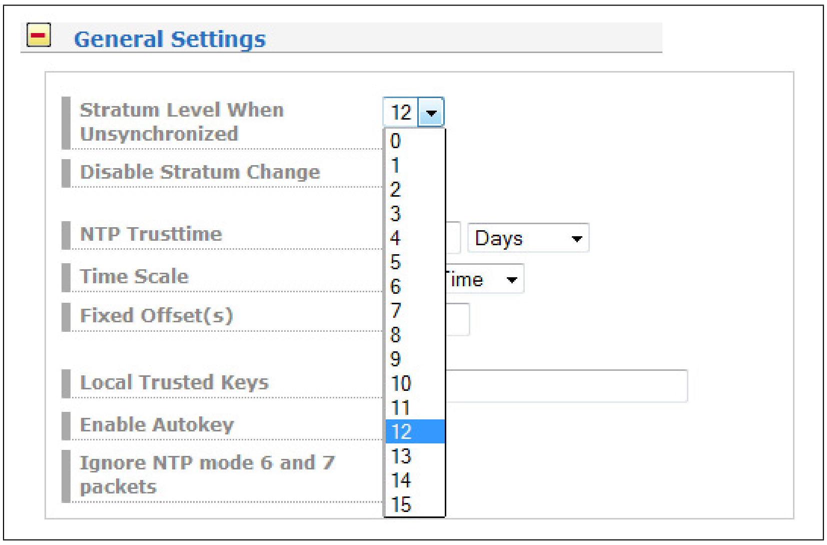
External Server Address 1		Symmetric Key			Use Autokey	□
Minpoll	Default	Seconds	Maxpoll	Default	Seconds	Use iburst	□

...

External Server Address 7		Symmetric Key			Use Autokey	□
Minpoll	Default	Seconds	Maxpoll	Default	Seconds	Use iburst	□

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 seven 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.

8.5.3 NTP Local Clock



General Settings

Stratum Level When Unsynchronized: 12

Disable Stratum Change

NTP Trusttime: Days

Time Scale

Fixed Offset(s)

Local Trusted Keys

Enable Autokey

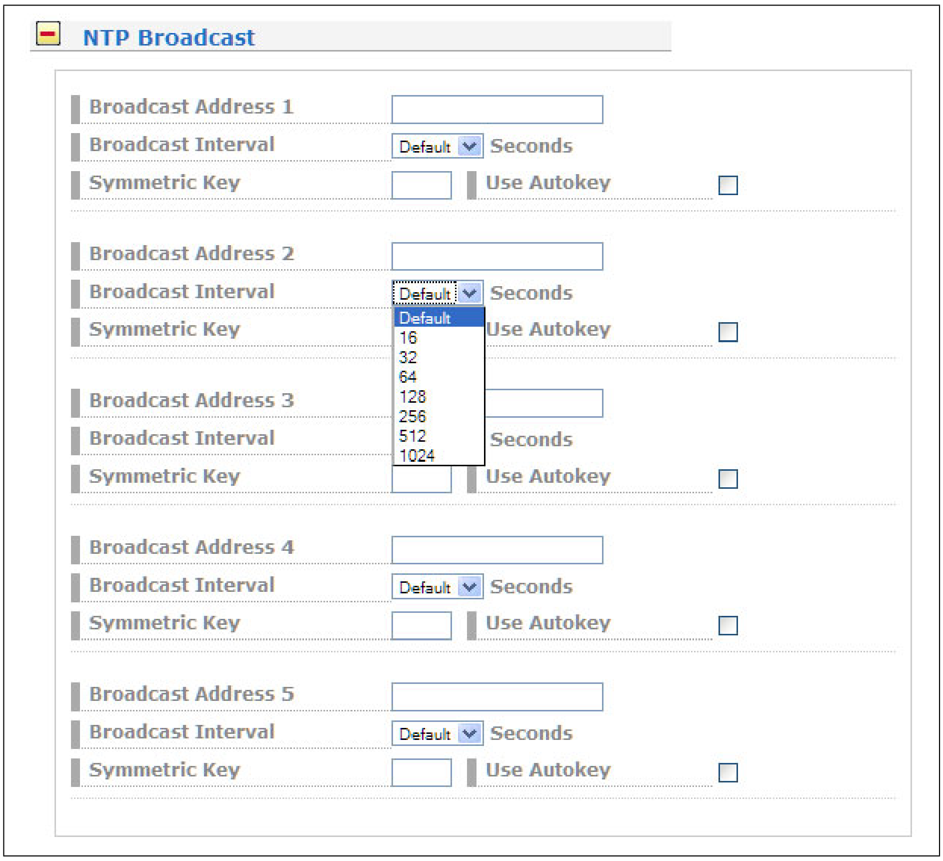
Ignore NTP mode 6 and 7 packets

The default configuration of the timeserver consists of a local clock, which represents the hardware clock of your LANTIME system and the reference clock. The local clock is only chosen as the NTP time reference after the receiver's 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 PPS (PulsePerSecond) of the reference clock (GPS), which is evaluated by the operating system. 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
```

8.5.4 NTP Broadcast



NTP Broadcast

Broadcast Address 1

Broadcast Interval Default Seconds

Symmetric Key ▌Use Autokey □

Broadcast Address 2

Broadcast Interval Default Seconds

Symmetric Key ▌Use Autokey □

Broadcast Address 3

Broadcast Interval Seconds

Symmetric Key ▌Use Autokey □

Broadcast Address 4

Broadcast Interval Default Seconds

Symmetric Key ▌Use Autokey □

Broadcast Address 5

Broadcast Interval Default Seconds

Symmetric Key ▌Use Autokey □

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
```

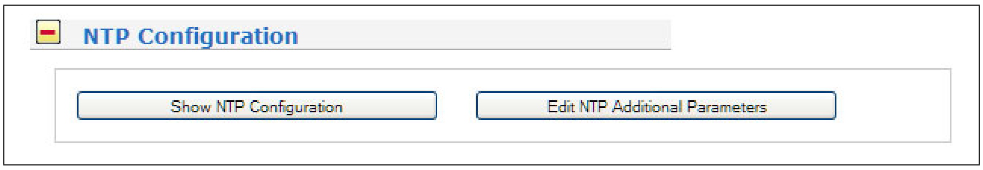
In the next section you can enable the AUTOKEY feature for your LANTIME timeserver and the PPS mode (which is enabled in default settings), see above for a description.

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:

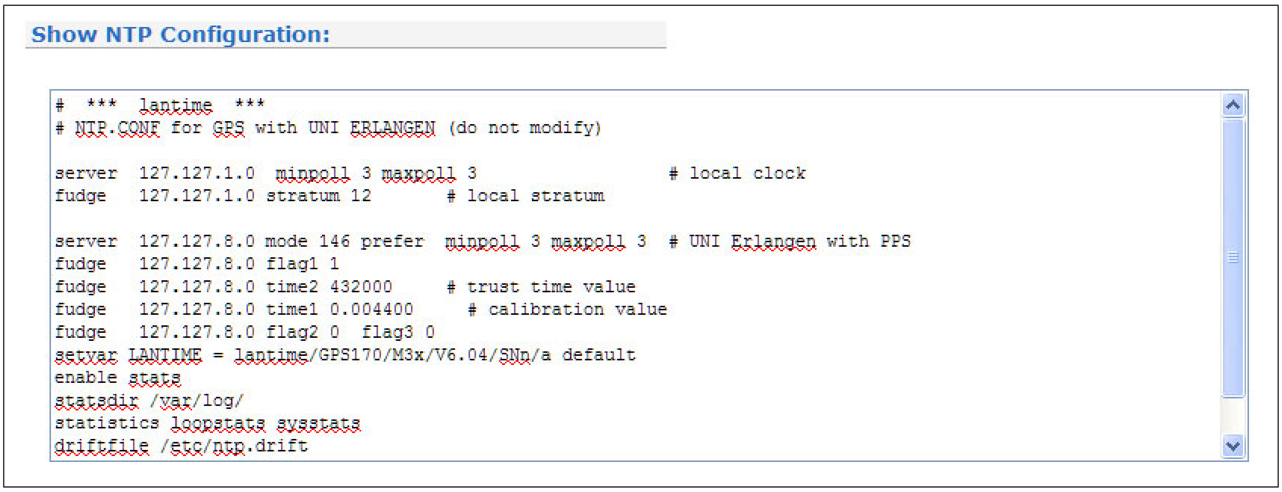
LANTIME/GPS:	96 h
LANTIME/PZF:	0,5 h
LANTIME/RDT:	0,5 h
LANTIME/MRS:	96 h

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".

8.5.5 Show NTP Configuration



By choosing "Show 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.



```
#  ***  lantime  ***
# NTP.CONF for GPS with UNI ERLANGEN (do not modify)

server  127.127.1.0  minpoll 3 maxpoll 3                  # local clock
fudge   127.127.1.0 stratum 12       # local stratum

server  127.127.8.0 mode 146 prefer  minpoll 3 maxpoll 3  # UNI Erlangen with PPS
fudge   127.127.8.0 flag1 1
fudge   127.127.8.0 time2 432000     # trust time value
fudge   127.127.8.0 time1 0.004400     # calibration value
fudge   127.127.8.0 flag2 0  flag3 0
setvar LANTIME = lantime/GPS170/M3x/V6.04/SNn/a default
enable stats
statsdir /var/log/
statistics loopstats sysstats
driftfile /etc/ntp.drift
```

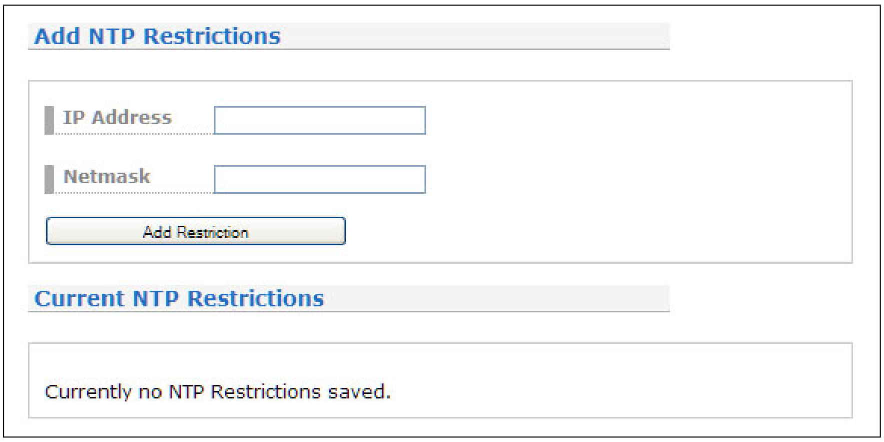
8.5.6 NTP Restrictions

With "Edit NTP Restrictions" you can allow access to specified NTP clients. Enter the IP address and the netmask as shown in the section below. All other IP address are invalid if an entry in the restriction list is made. Only the users from the list have NTP access on this time server.

The following lines are written automatically in the NTP configuration file:

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

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

The address 172.16.3.13 and all IPs from the subnet 172.16.5.xx
have access to all NTP services.



Currently no NTP Restrictions saved.

8.5.7 NTP Authentication

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

Please note that the distribution of DES in the United States of America and Canada is subject to restrictions, while MD5 is not affected by that. With any of these algorithms the receiving NTP clients validate the checksum. Both parties (server and client) need to have the same crypto key with the same key ID.
In the authentication mode a party is marked “untrusted” and not suitable for synchronisation, whenever unauthorised packets or authorised packets with a wrong key are used. Please note that a server may recognise a lot of keys but uses only a few of them. This allows a timeserver to serve a client, who is demanding an authenticated time information, without “trusting” the client.

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

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

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

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

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

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

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

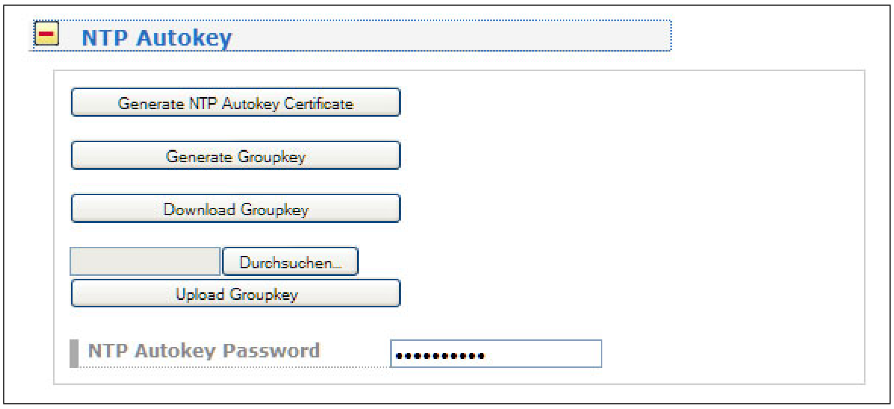
```
# ntp keys file (ntp.keys)

1     N 29233E0461ECD6AE     # des key in NTP format
2     M RIrop8KPPvQvYotM     # md5 key as an ASCII random string
14    M sundial              # md5 key as an ASCII string
15    A sundial              # des key as an ASCII string
                             # the following 3 keys are identical
10    A SeCReT
10    N d3e54352e5548080
10    S a7cb86a4cba80101
```

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

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

8.5.8 NTP Autokey Settings

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.



NTP Autokey Password ••••••••••

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 NTP Autokey Certificate" in section "NTP Autokey Settings" 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).

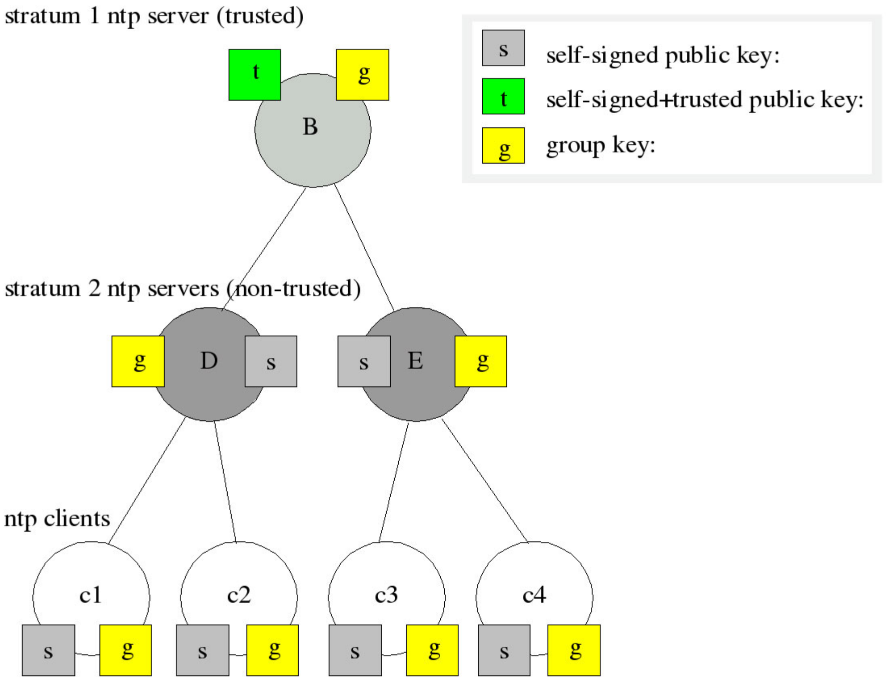
```
LantimeGpsV4:/etc/ntp # ntp-keygen -q cryptosecret
```

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).

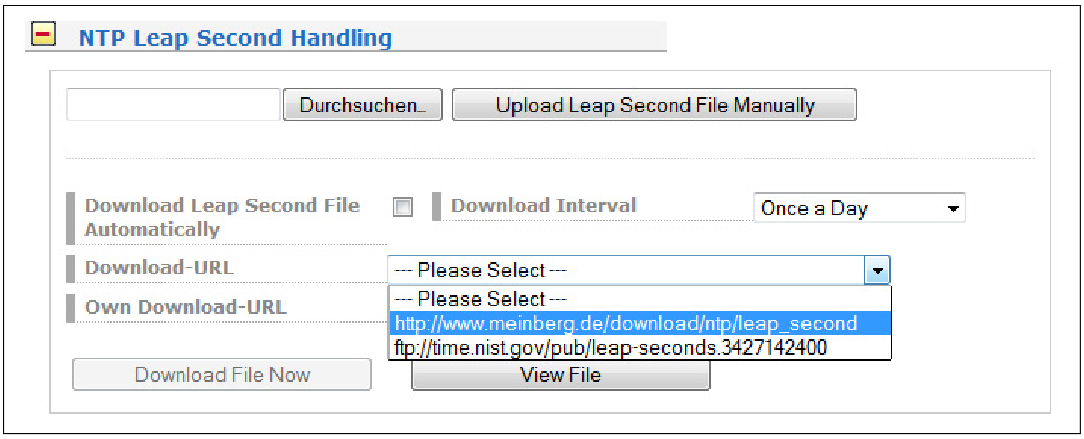
Example:
This autokey group is formed by one Stratum-1-server (B), two Stratum-2-servers (D and E) and a number of clients (in the diagram there are 4 clients shown, c1 – c4). B is the trusted host, he holds the group key and a self-signed certificate marked as "trusted".


stratum 1 ntp server (trusted)
t
g
B
s
self-signed public key:
t
self-signed+trusted public key:
g
group key:
stratum 2 ntp servers (non-trusted)
g
D
s
s
E
g
ntp clients
c1
c2
c3
c4
s
g
s
g
s
g
s
g

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).

8.5.9 NTP Leap Second Handling



NTP Leap Second Handling

Download Leap Second File Automatically ☐

Download Interval: Once a Day

Download-URL: --- Please Select ---

Own Download-URL

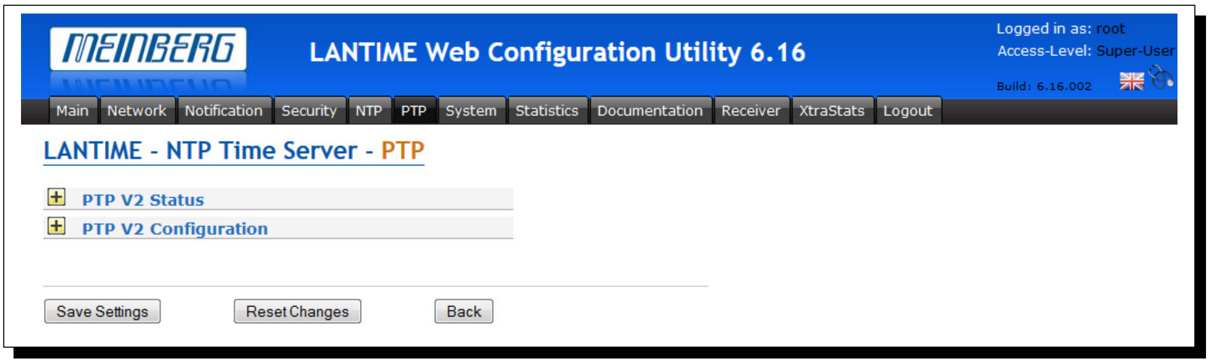
Durchsuchen...
Upload Leap Second File Manually
--- Please Select ---
http://www.meinberg.de/download/ntp/leap_second
ftp://time.nist.gov/pub/leap-seconds.3427142400
Download File Now
View File

GPS system time differs from the universal time scale (UTC) by the number of leap seconds which have been inserted into the UTC time scale since GPS was initiated in 1980. The current number of leap seconds is part of the navigation message supplied by the satellites or radio transmitters, so the internal real time of the clock is based on UTC.

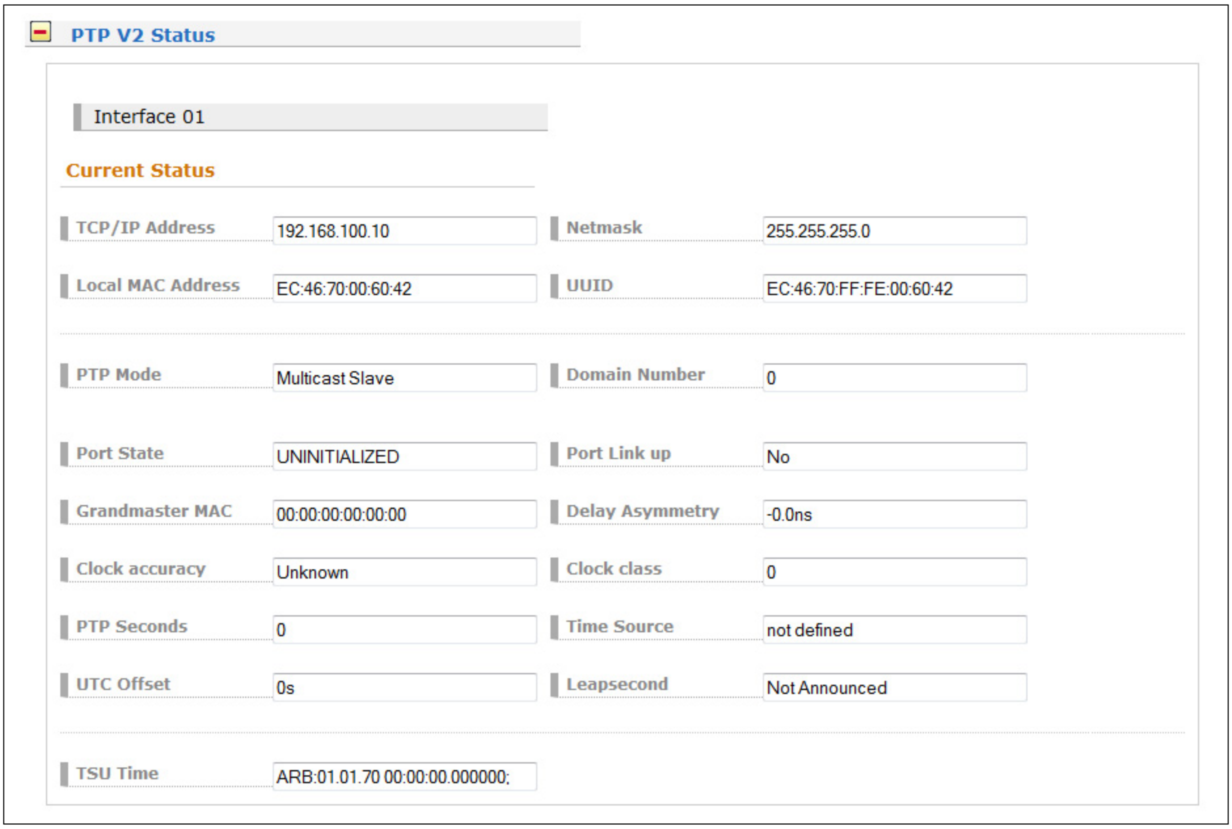
In this menu you can select an available "Leap Second File" from the Meinberg or NTP web server. Of course you can enter your an other download link or you can upload your own file for leap second handling.

Available Download Sources
Meinberg: http://www.meinberg.de/download/ntp/leap_second
NTP.ORG: ftp://time.nist.gov/pub/ (leap-seconds.xxxxxxxxxx)

8.6 Configuration: PTP


MEINBERG
LANTIME Web Configuration Utility 6.16
Logged in as: root
Access-Level: Super-User
Build: 6.16.002
Main Network Notification Security NTP PTP System Statistics Documentation Receiver XtraStats Logout
LANTIME - NTP Time Server - PTP
PTP V2 Status
PTP V2 Configuration
Save Settings
Reset Changes
Back

In the PTP section, all parameters of the PTP subsystem can be configured. The current state can be monitored as well. When operating in SLAVE mode (as with MRS devices), a graphical representation of the offset and the path delay to the grandmaster will be shown on page **Statistics** -> **PTPv2 Statistics**.



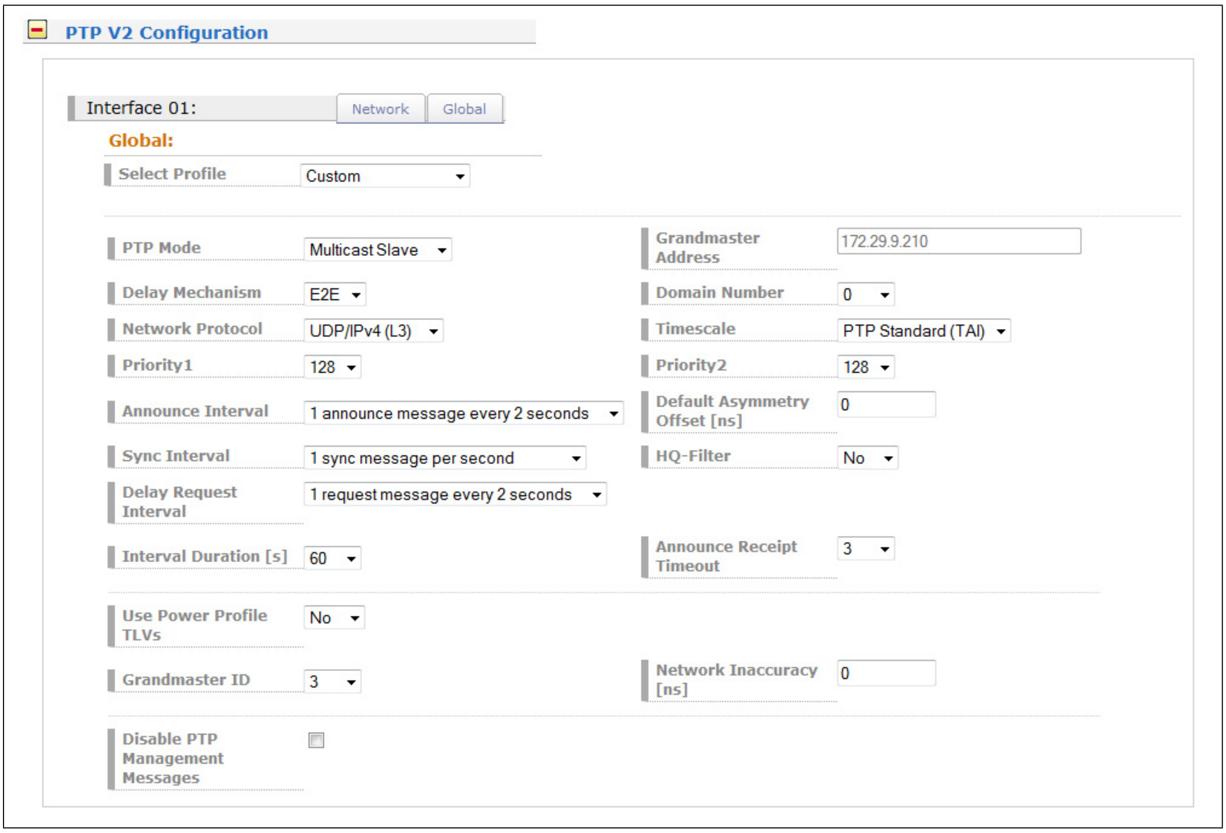
TCP/IP Address	192.168.100.10	Netmask	255.255.255.0
Local MAC Address	EC:46:70:00:60:42	UUID	EC:46:70:FF:FE:00:60:42
PTP Mode	Multicast Slave	Domain Number	0
Port State	UNINITIALIZED	Port Link up	No
Grandmaster MAC	00:00:00:00:00:00	Delay Asymmetry	-0.0ns
Clock accuracy	Unknown	Clock class	0
PTP Seconds	0	Time Source	not defined
UTC Offset	0s	Leapsecond	Not Announced
TSU Time	ARB:01.01.70 00:00:00.000000;		

All configuration parameters of the PTP unit can be viewed and changed by accessing the "ptp2_global_conf_0" file. This can be done with the "PTP v2 Configuration" submenu. If more than one PTP unit (PTP ports) is built into the system, then the configuration for each port can be edited separately and will be listed on this page.

The IP address and VLAN configuration can be edited by selecting the "Network" chapter of the configuration submenu. You can change the global PTP parameters and the PTP profile here too.

A detailed description of the parameters can be found in chapter 8.6.1 (Global PTP Parameters).

8.6.1 PTPv2 - Global Configuration



PTP V2 Configuration

Interface 01: Network Global

Global:

Select Profile: Custom

PTP Mode: Multicast Slave

Delay Mechanism: E2E

Network Protocol: UDP/IPv4 (L3)

Priority1: 128

Announce Interval: 1 announce message every 2 seconds

Sync Interval: 1 sync message per second

Delay Request Interval: 1 request message every 2 seconds

Interval Duration [s]: 60

Grandmaster Address: 172.29.9.210

Domain Number: 0

Timescale: PTP Standard (TAI)

Priority2: 128

Default Asymmetry Offset [ns]: 0

HQ-Filter: No

Announce Receipt Timeout: 3

Use Power Profile TLVs: No

Grandmaster ID: 3

Network Inaccuracy [ns]: 0

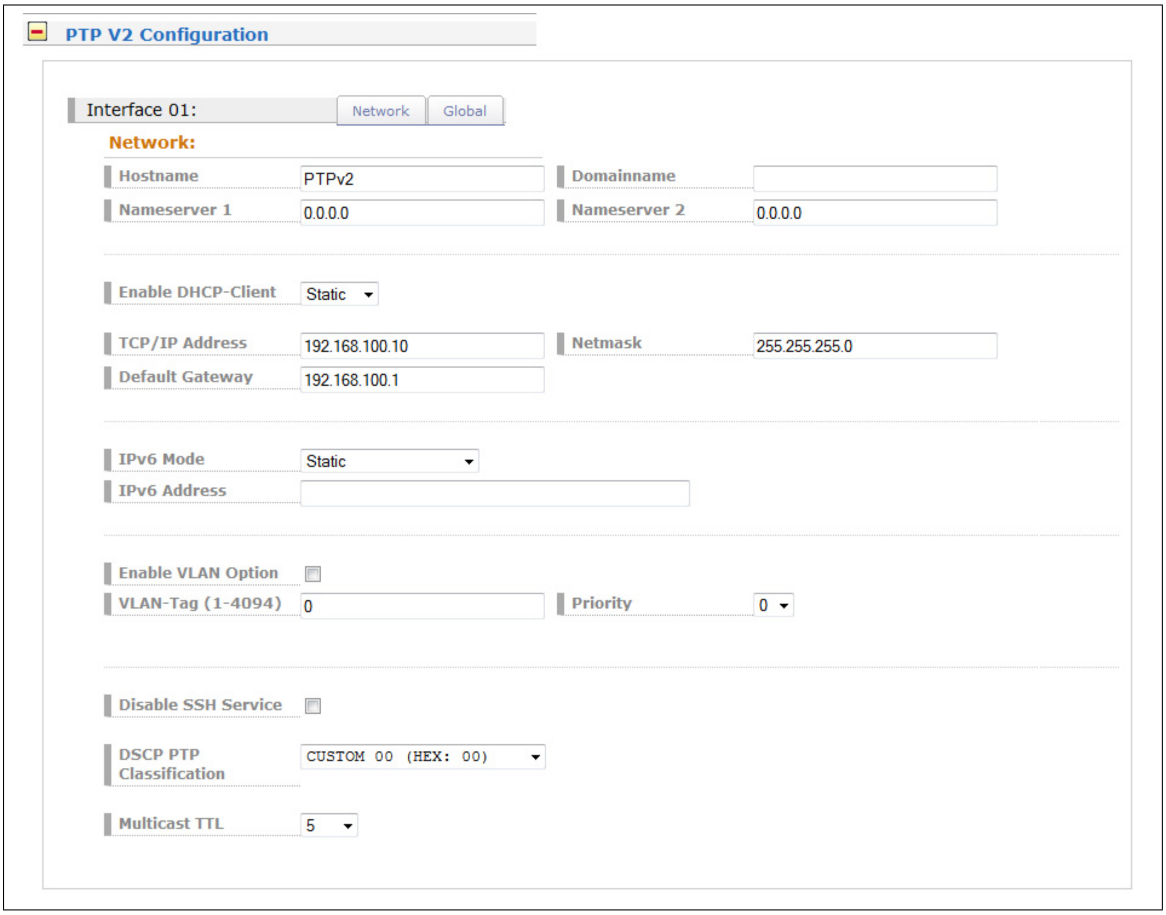
Disable PTP Management Messages: □

Parameter	Value	Description
PTP Mode	[NUM]	0=Multicast (MC), 1=Unicast (UC)
PTP is slave	[BOOL]	1=Slave only, 0=Grandmaster only
PTP Delay Mechanism	[0,1]	0=End-to-End, 1=Peer-to-Peer
PTP V1 Hardware Compatibility	[0,1]	PTP packet length as with PTPv1 standard (0= default)
PTP Domain Number	[NUM,0:3]	A domain is logical group of PTP devices
PTP Network Protocol	[NUM,1,3]	1=UDP/IPv4 (L3), 3=IEEE 802.3 (L2)
PTP Timescale	[NUM,0:1]	0=ARB, 1=PTP (default)
PTP priority1	[NUM:0:255]	Priority 1 as used in Best Master Clock Algorithm
PTP priority2	[NUM:0:255]	Priority 2 as used in Best Master Clock Algorithm
PTP Sync Interval	[2^x]:0	used in MC Master or UC Slave mode
PTP Announce Interval	[2^x]:1	used in MC Master or UC Slave mode
PTP DelayRequest Interval	[2^x]:3	used in MC Master or UC Slave mode
PTP Unicast interval duration [s]	[NUM]:60	Requested duration until timeout/renewal
PTP Unicast clockid of master	[ASCII,50]	Unicast: Master Clock ID (eg. FF:FF:FF:FF:FF:FF:FF:FF)
PTP Unicast IP address of master	[IP]	Unicast: IP address of Grandmaster (eg. 172.29.9.236)
Feature Presets	[NUM]	1 = Power Profile Preset
User defined Fix Offset positive	[BOOL]	1 = Positive PTP Phase shift to RefTime
User defined Fix Offset [ns]	[NUM]	0 - 1000000ns = Phase shift to RefTime

HQ Filter active	[BOOL]:0	Slave: Optimized filter for high load/jitter
HQ Filter estimated accuracy [ns]	[NUM]:5000	estimated accuracy of HQ Filter,maximum jitter in network
PDSC active	[BOOL]:0	Path Delay Step Compensation (Filter on) (see also chapter **??**)

8.6.2 PTP Network Configuration

All network configurations of the selected PTP interface can be done with this menu:



Interface 01:

Network:

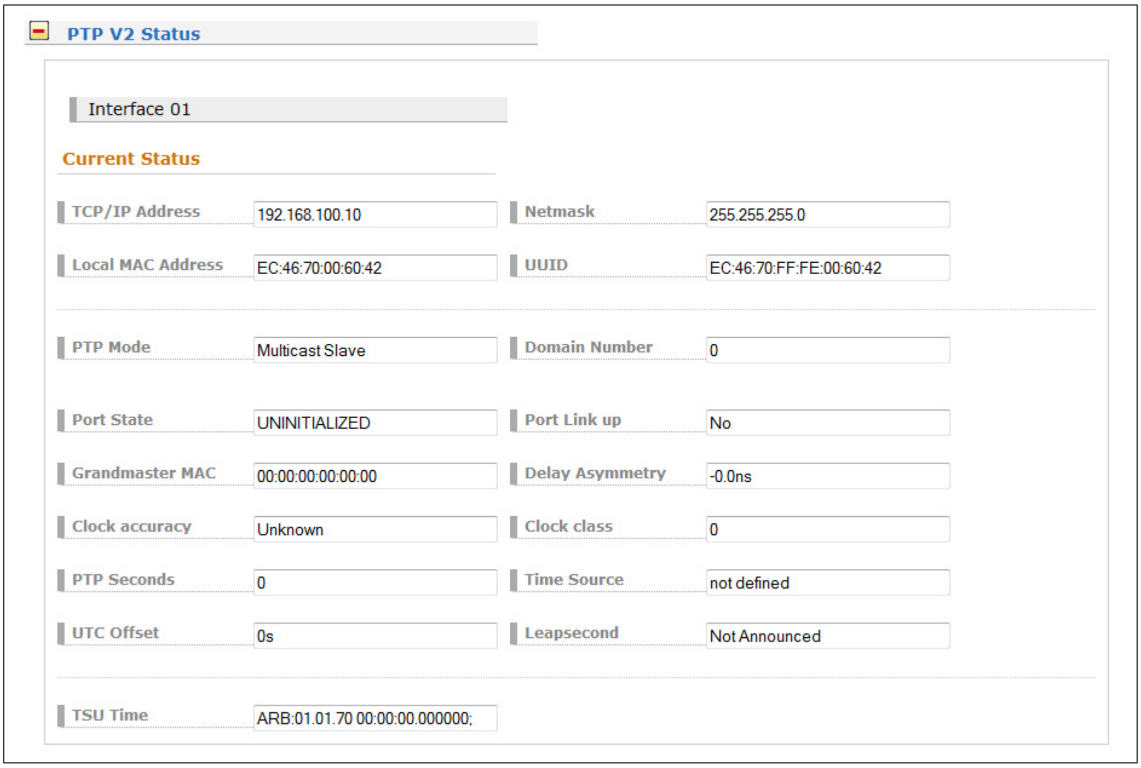
Hostname	PTPv2	Domainname	
Nameserver 1	0.0.0.0	Nameserver 2	0.0.0.0
Enable DHCP-Client	Static		
TCP/IP Address	192.168.100.10	Netmask	255.255.255.0
Default Gateway	192.168.100.1		
IPv6 Mode	Static		
IPv6 Address			
Enable VLAN Option	□		
VLAN-Tag (1-4094)	0	Priority	0
Disable SSH Service	□		
DSCP PTP Classification	CUSTOM 00 (HEX: 00)		
Multicast TTL	5		

Content of the PTP Network Configuration File:

Parameter	Value	Description
Hostname	[ASCII,50]:PTPv2	Hostname for PTP port
Domainname	[ASCII,50]:	Domainname for PTP port
Nameserver 1	[ASCII,50]:	
Nameserver 2	[ASCII,50]:	
TCPIP address	[IP]:192.168.100.10	IP address of PTP port
NETMASK	[IP]:255.255.255.0	Netmask of PTP port
Default Gateway	[IP]:192.168.100.1	Gateway
DHCP CLIENT	[BOOL]:0	1=Activate DHCP client
VLan enabled	[BOOL]:0	Enable Virtual LAN interface (IEEE 802.1Q)
VLan ID	[NUM]:	VLAN ID for virtual interface
VLan Priority	[NUM]:	VLAN priority for virtual interface
PTP IP TTL	[NUM]:	Multicast IP Packet Time To Live (TTL default:5)

8.6.3 PTP State Files

In this submenu all status information of the selected Time Stamp Unit (TSU) is displayed:

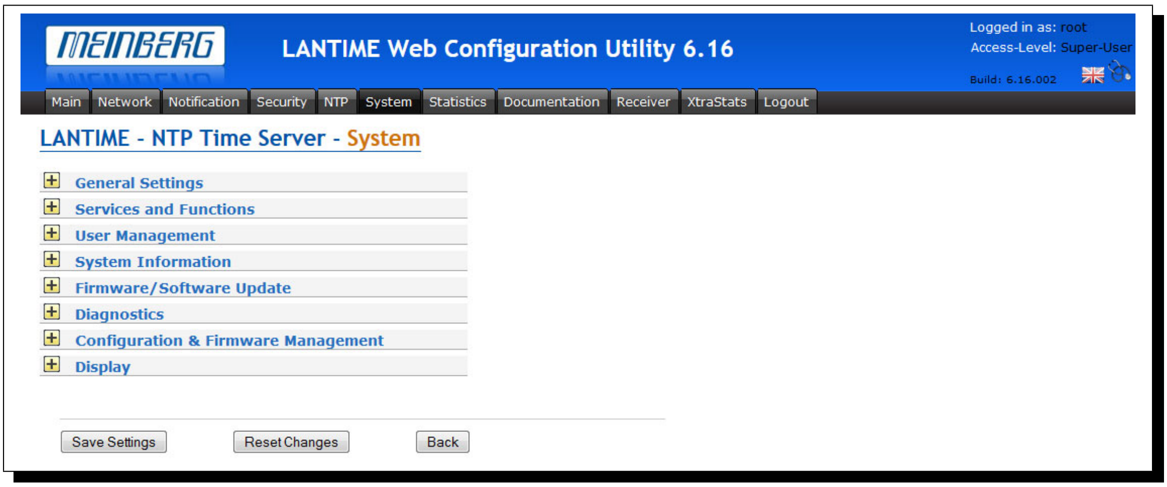


Current Status

TCP/IP Address	192.168.100.10	Netmask	255.255.255.0
Local MAC Address	EC:46:70:00:60:42	UUID	EC:46:70:FF:FE:00:60:42
PTP Mode	Multicast Slave	Domain Number	0
Port State	UNINITIALIZED	Port Link up	No
Grandmaster MAC	00:00:00:00:00:00	Delay Asymmetry	-0.0ns
Clock accuracy	Unknown	Clock class	0
PTP Seconds	0	Time Source	not defined
UTC Offset	0s	Leapsecond	Not Announced
TSU Time	ARB:01.01.70 00:00:00.000000;		

PTP Mode : [MASTER,SLAVE]
Domain number : [0...3]
Network Protocol : [UDP IPv4 Layer3,IEEE 802.3 Layer 2]
PTP DelayMech : [E2E,P2P]
Current Port State: [INITIALIZING,LISTENING,UNCALIBRATED,MASTER,UnicastMASTER,SLAVE,UnicastSLAVE]
Clock class : [6=RefClock Sync, 7= RefClock Holdover, 52=RefClock unsynchronized, 255=Slave only]
Clock accuracy : 33
Clock variance : 13565
Grandmaster MAC : 00:60:6E:7C:27:2C
Number of clients : 0
Number of masters : 0
PTP Port Link up : 1
IPv4 address : 172.29.4.10
Netmask : 255.255.255.0
Gateway : 172.29.4.1
Local Mac Address : 00:60:6E:7C:27:2C
PTP seconds : 1299849447
PTP timescale : PTP (TAI)
PTP time source : GPS
PTP UTC Offset : 34
PTP Leapsecond : 0
TSU Time: TAI:11.03.11 13:17:27.652680;
SYS Time: UTC:11.03.11 13:16:53.655558;

8.7 Configuration: System

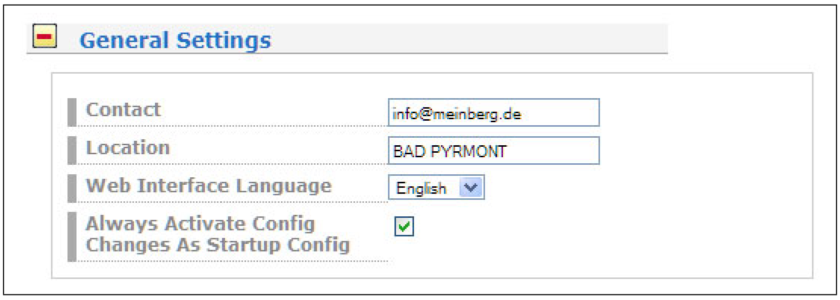


LANTIME Web Configuration Utility 6.16

Logged in as: root
Access-Level: Super-User
Build: 6.16.002

LANTIME - NTP Time Server - System

8.7.1 Common Configuration

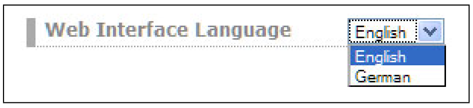


General Settings

Contact	info@meinberg.de
Location	BAD PYRMONT
Web Interface Language	English
Always Activate Config Changes As Startup Config	☑

You can enter a contact address, the location of the LANTIME and the language of the web interface. If the checkbox is activated then all changes during the last session will be stored as new startup configuration.

8.7.2 Web interface language

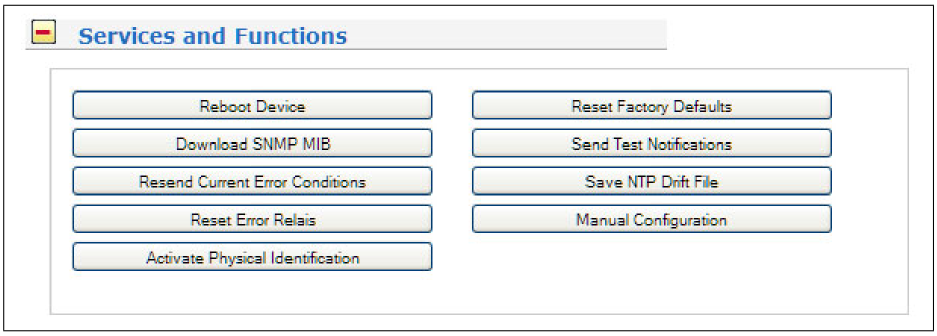


Web Interface Language: English

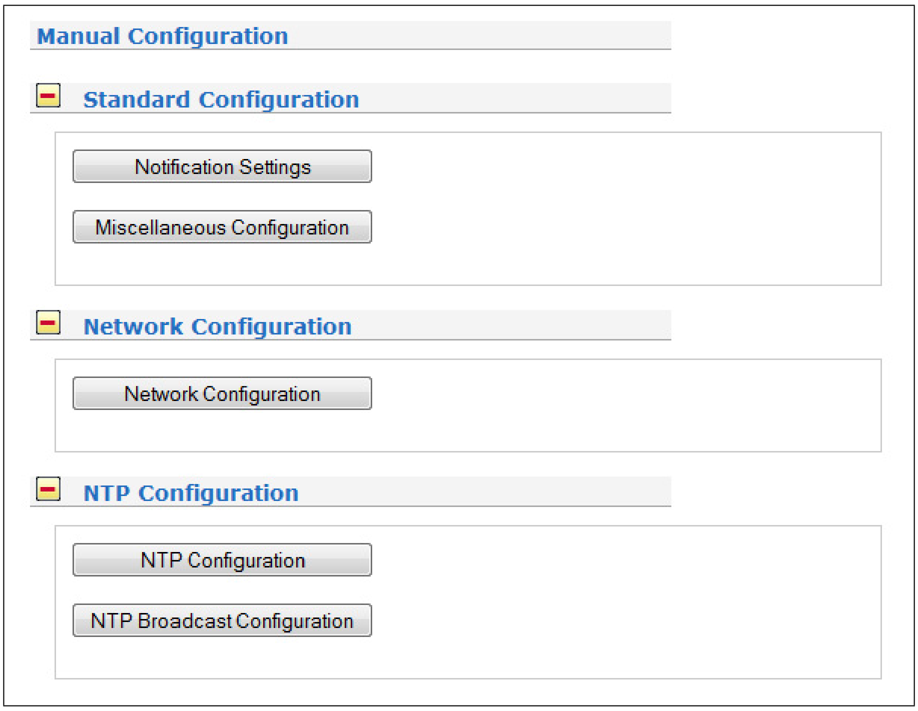
With the selector box “Web interface language” you can change the displayed language of the WEB interface.

8.7.3 Services and Functions

In the first section there are several functions which may be used by the administrator. The button "Reboot Device" 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).

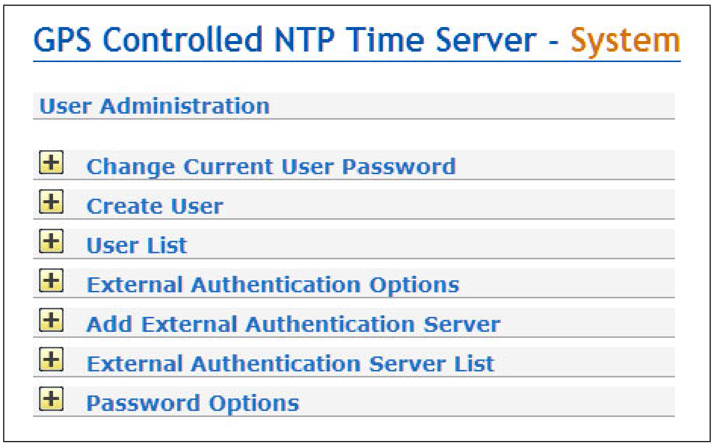
You can use the function "Save NTP drift file" to copy the file /etc/ntp.drift to the internal flash disc of your LANTIME. NTP is using this file to have the parameters for compensation of the incorrectness of the system clock available directly after a restart. This results in a faster synchronisation 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.

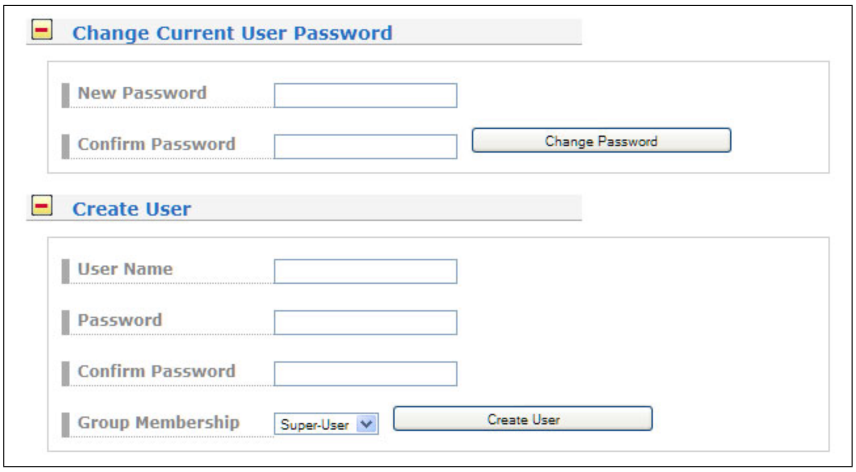
The point “Download SNMP MIB files“ can be used to download all Meinberg specific SNMP MIB files to your workstation. They can be distributed to all SNMP management clients afterwards.

8.7.4 User Management

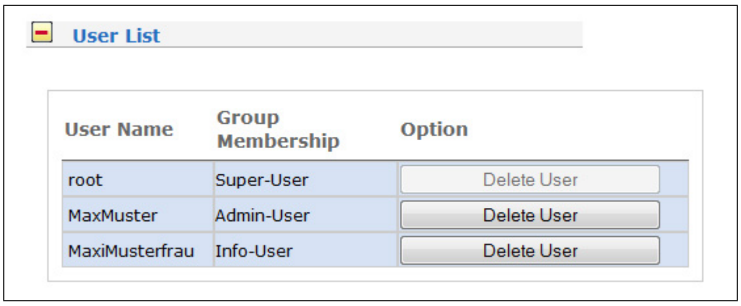

GPS Controlled NTP Time Server - System
User Administration
⊞ Change Current User Password
⊞ Create User
⊞ User List
⊞ External Authentication Options
⊞ Add External Authentication Server
⊞ External Authentication Server List
⊞ Password Options

It is possible to create multiple user accounts on a LANTIME system, each account can be assigned one of three access levels: the Super-User level has full read-write access to the configuration of the LANTIME system, it can modify all parameters and has full shell access to the system when logging in via Telnet, SSH or serial console port.

Administrator level accounts can only modify parameters via the WEB interface but does not have shell access. The access level "Info" can only review status and configuration options but is not allowed to modify any parameters or configuration files.

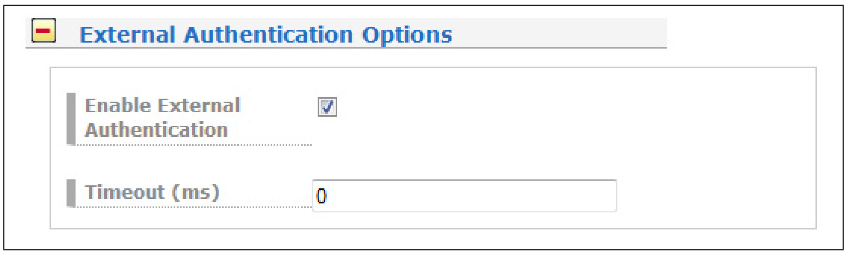


The "User Management" menu allows you to set up different users with password and the access level. To change the properties of an user you have to delete the old user and set up a new one. The user “root“ cannot be deleted and has always the membership of Super-User. The password of the user "root"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



User Name	Group Membership	Option
root	Super-User	Delete User
MaxMuster	Admin-User	Delete User
MaxiMusterfrau	Info-User	Delete User

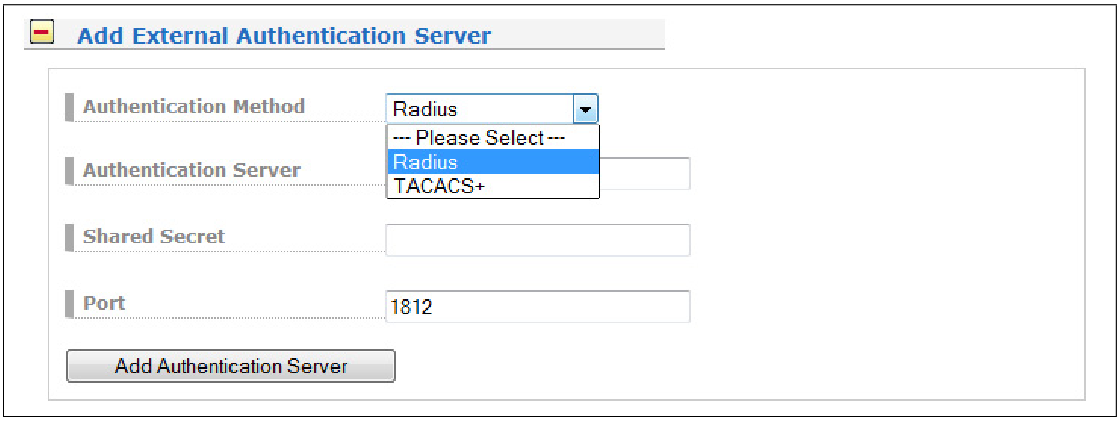
Authentification Options



External Authentication Options

Enable External Authentication ☑

Timeout (ms) 0



Add External Authentication Server

Authentication Method Radius

Authentication Server

Shared Secret

Port 1812

You can choose between several Authentification Methods:

TACACS: Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks.

The LANTIME TACACS authentication feature requires that each account that should be able to login to the LANTIME needs a special attribute called „priv-lvl". This attribute has to be configured on the TACACS Server. In addition to that, you need to assign a value of 100 (=Super User), 200 (=Admin User) or 300 (=Info User) for this attribute to each TACACS user account that should be able to login to a LANTIME.

Please note that you have to define the attribute for the service "lantime_mgmt", for example:

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

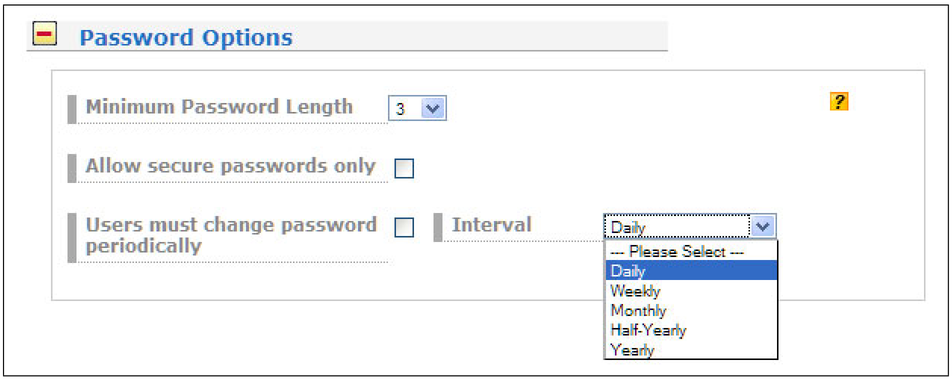
RADIUS: Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication for MEINBERG Time Servers to connect and use the network services. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport.

The LANTIME RADIUS authentication feature requires that each account that should be able to login to the LANTIME needs a Vendor Specific Attribute (VSA) called MBG-Management-Privilege-Level. This VSA has to be defined in the so-called dictionary of the RADIUS Server.

In addition to that file, you need to assign a value of 100 (=Super User), 200 (=Admin User) or 300 (=Info User) for this attribute to each RADIUS user account that should be able to login to a LANTIME.

Passwort-Options

In this section you can activate special options to enhance security features of the user passwords.



Password Options

Minimum Password Length 3

Allow secure passwords only □

Users must change password periodically □

Interval Daily

Minimum Password Length

This parameter set the minimum number of characters of a password before it is accepted by the system as a valid password. This value is used when creating a new user as well as when you change a current user password.

Allow Secure Passwords Only

The password must contain at least one lower character [a-z], one upper character [A-Z], one number [0-9] and one special character.

List of valid special characters:

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

User must change password periodically

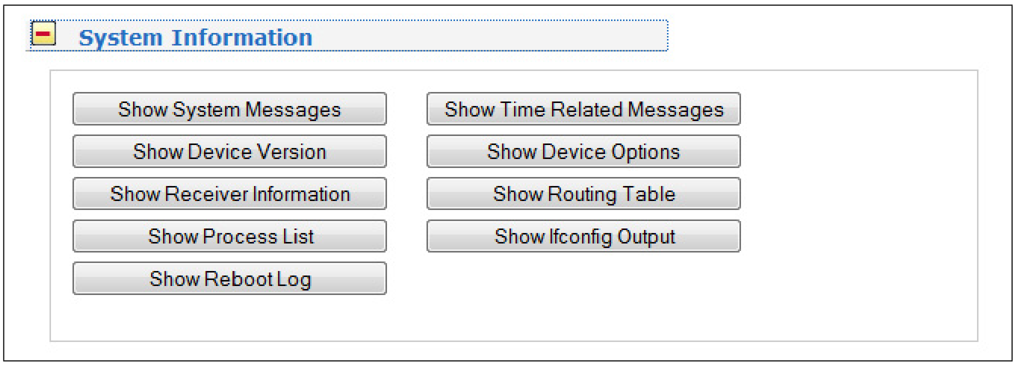
Users will be forced to change there passwords at regular intervals. If a password is expired the user can't log in to the unit before changing his current password.

Available intervals:

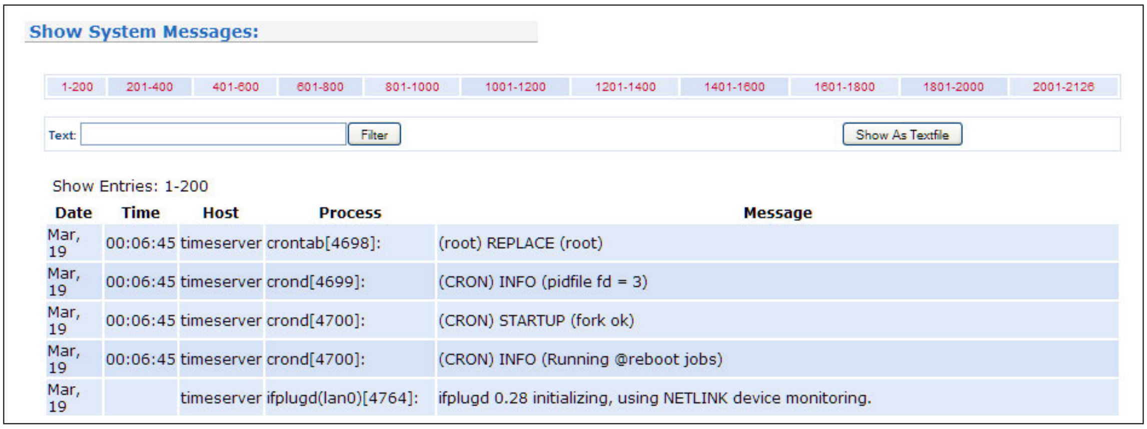
Monthly	= Every 30 Days
Half-Yearly	= Every 180 Days
Yearly	= Every 360 Days

8.7.5 System Information

The button "System Information" 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.



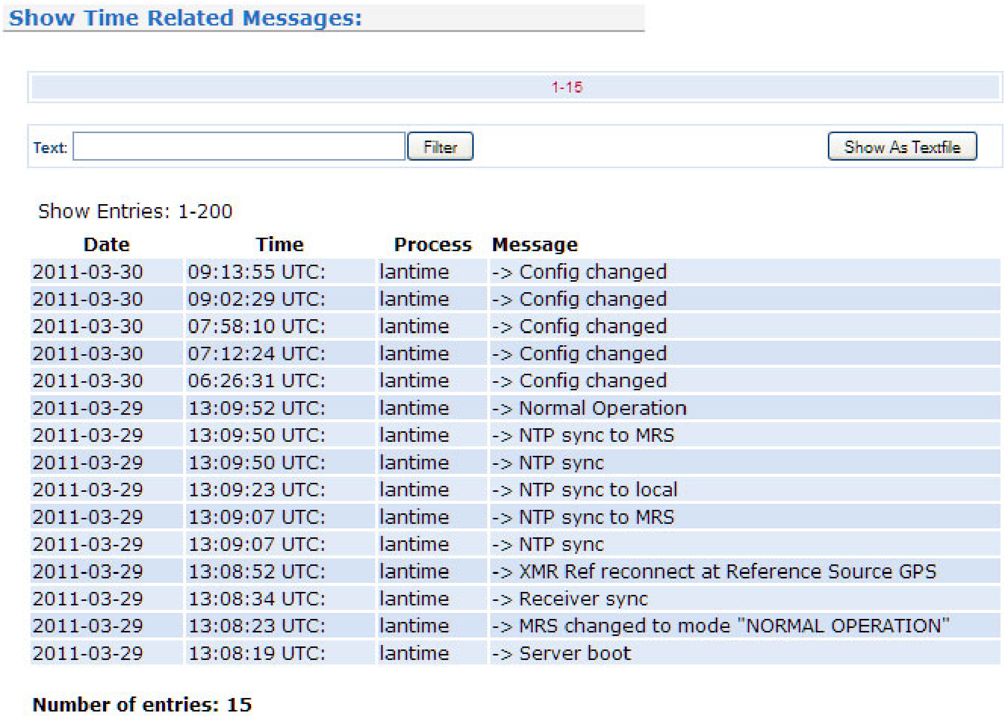
8.7.6 Show System Messages



Show Entries: 1-200

Date	Time	Host	Process	Message
Mar, 19	00:06:45	timeserver	crontab[4698]:	(root) REPLACE (root)
Mar, 19	00:06:45	timeserver	crond[4699]:	(CRON) INFO (pidfile fd = 3)
Mar, 19	00:06:45	timeserver	crond[4700]:	(CRON) STARTUP (fork ok)
Mar, 19	00:06:45	timeserver	crond[4700]:	(CRON) INFO (Running @reboot jobs)
Mar, 19		timeserver	ifplugd(lan0)[4764]:	ifplugd 0.28 initializing, using NETLINK device monitoring.

Show Time Related Messages:



Show Entries: 1-200

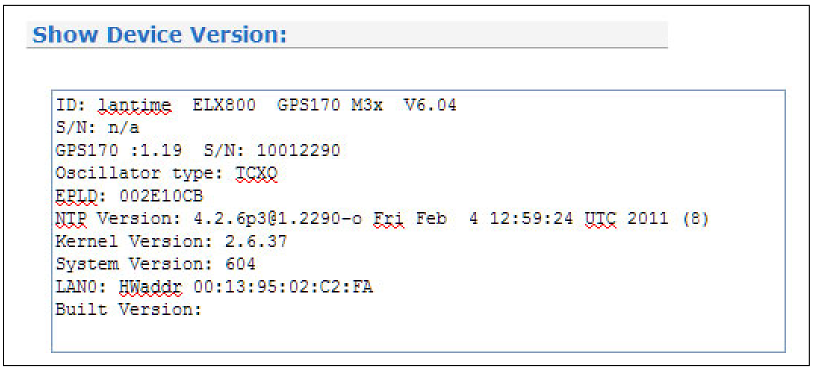
Date	Time	Process	Message
2011-03-30	09:13:55 UTC:	lantime	-> Config changed
2011-03-30	09:02:29 UTC:	lantime	-> Config changed
2011-03-30	07:58:10 UTC:	lantime	-> Config changed
2011-03-30	07:12:24 UTC:	lantime	-> Config changed
2011-03-30	06:26:31 UTC:	lantime	-> Config changed
2011-03-29	13:09:52 UTC:	lantime	-> Normal Operation
2011-03-29	13:09:50 UTC:	lantime	-> NTP sync to MRS
2011-03-29	13:09:50 UTC:	lantime	-> NTP sync
2011-03-29	13:09:23 UTC:	lantime	-> NTP sync to local
2011-03-29	13:09:07 UTC:	lantime	-> NTP sync to MRS
2011-03-29	13:09:07 UTC:	lantime	-> NTP sync
2011-03-29	13:08:52 UTC:	lantime	-> XMR Ref reconnect at Reference Source GPS
2011-03-29	13:08:34 UTC:	lantime	-> Receiver sync
2011-03-29	13:08:23 UTC:	lantime	-> MRS changed to mode "NORMAL OPERATION"
2011-03-29	13:08:19 UTC:	lantime	-> Server boot

Number of entries: 15

A list of time related messages appears which are registered by certain events like reboot of the system, change of configuration settings and so on. After a restart this list is overwritten!

Show Device Version

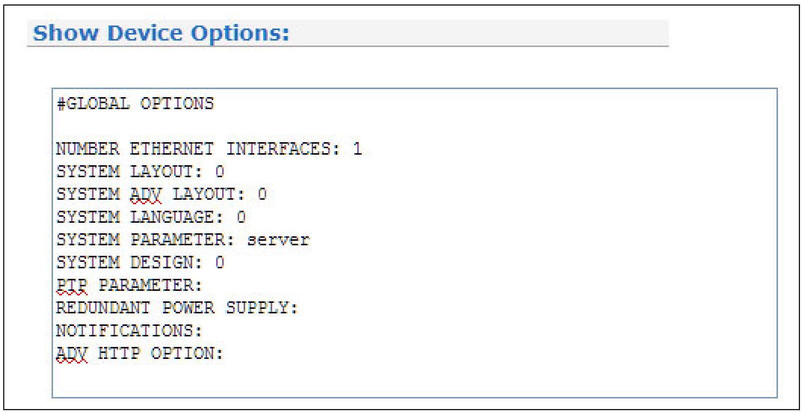
With "Show Device Version" a number of version numbers (including LANTIME software, operating system and NTPD) are shown in a textbox.



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

Show Device Options

The function “Show Device Options“ shows the hardware options installed in your LANTIME.

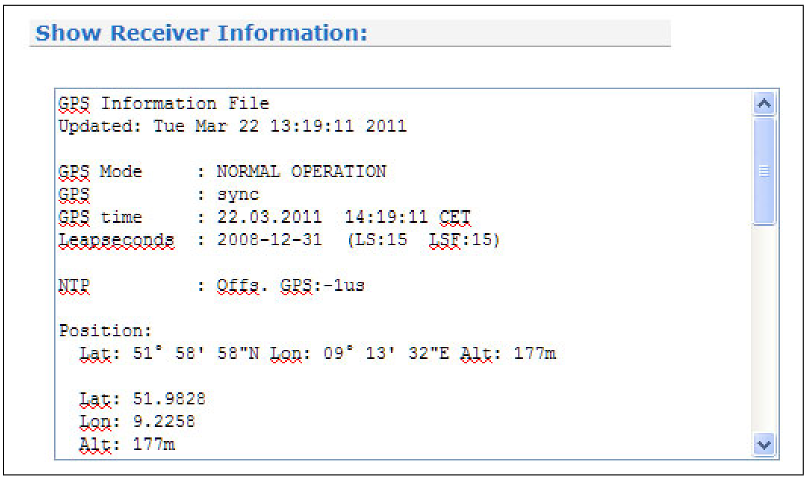


Show Device Options:

```
#GLOBAL OPTIONS

NUMBER ETHERNET INTERFACES: 1
SYSTEM LAYOUT: 0
SYSTEM ADV LAYOUT: 0
SYSTEM LANGUAGE: 0
SYSTEM PARAMETER: server
SYSTEM DESIGN: 0
PTP PARAMETER:
REDUNDANT POWER SUPPLY:
NOTIFICATIONS:
ADV HTTP OPTION:
```

Show Receiver Information

Using the button "Show Receiver Information" gives you the possibility to check detailed receiver status information. The first parameter indicates the time and date of the last update of the shown parameters. Next you find the receiver status and the NTP status.



```
GPS Information File
Updated: Tue Mar 22 13:19:11 2011

GPS Mode     : NORMAL OPERATION
GPS          : sync
GPS time     : 22.03.2011  14:19:11 CET
Leapseconds  : 2008-12-31  (LS:15  LSF:15)

NTP          : Offs. GPS:-1us

Position:
  Lat: 51° 58' 58"N Lon: 09° 13' 32"E Alt: 177m

  Lat: 51.9828
  Lon: 9.2258
  Alt: 177m
```

In case of a GPS receiver you can find GPS position data in this file. 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).

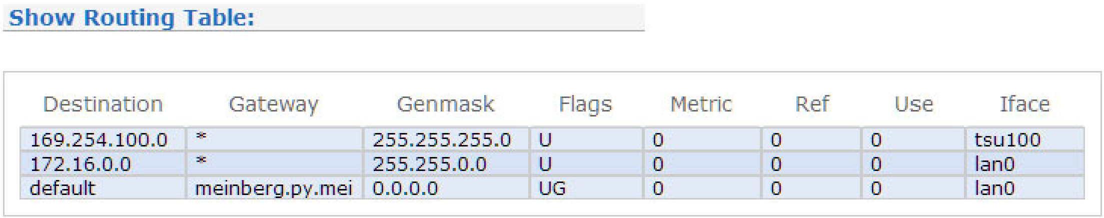
MRS Systems: The configured external NTP servers can be found under:

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

---

The list shows also the currently used external NTP server (adjust).

Show Routing Table:

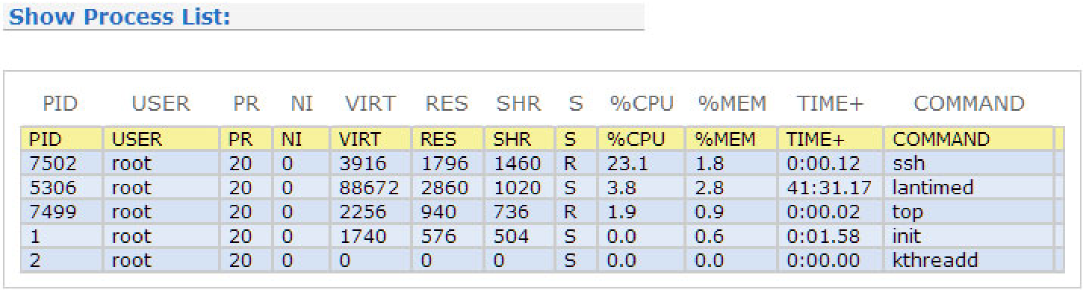


Show Routing Table:

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

The table shows all available and configured network routes.

Show Process List

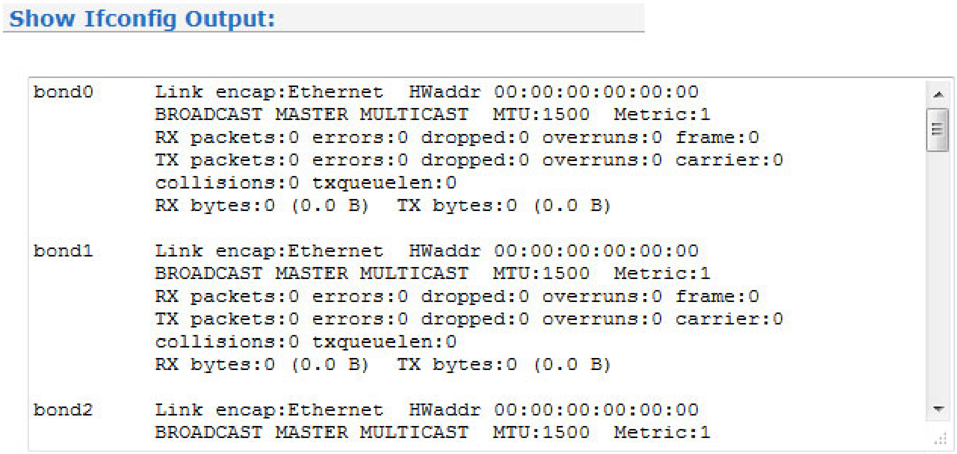


Show Process List:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
7502	root	20	0	3916	1796	1460	R	23.1	1.8	0:00.12	ssh
5306	root	20	0	88672	2860	1020	S	3.8	2.8	41:31.17	lantimed
7499	root	20	0	2256	940	736	R	1.9	0.9	0:00.02	top
1	root	20	0	1740	576	504	S	0.0	0.6	0:01.58	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd

A list of all active processes (CPU performance, used memory, runtime...) of the LAN-CPU is indicated with this table.

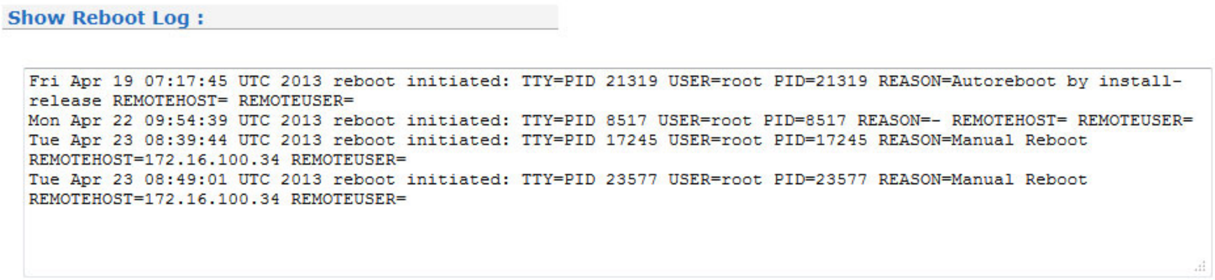
Show Ifconfig Output



Show Ifconfig Output:

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

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

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

Show Reboot Log

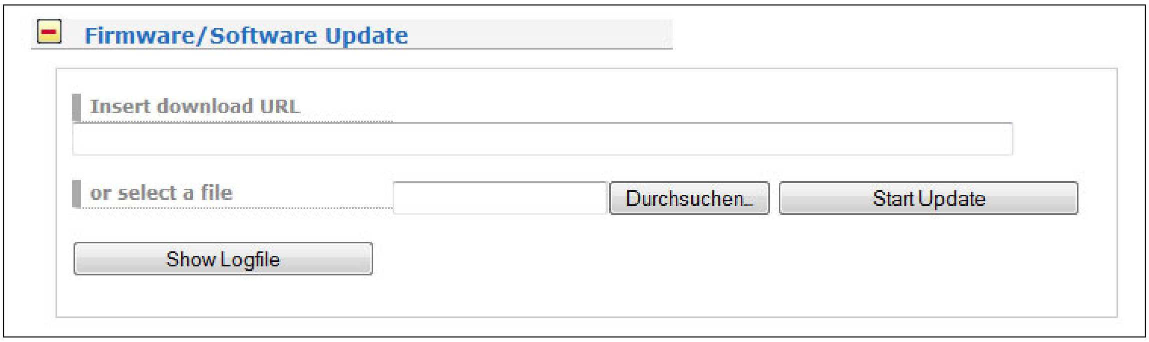


Show Reboot Log :

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

8.7.7 Firmware/Software Update

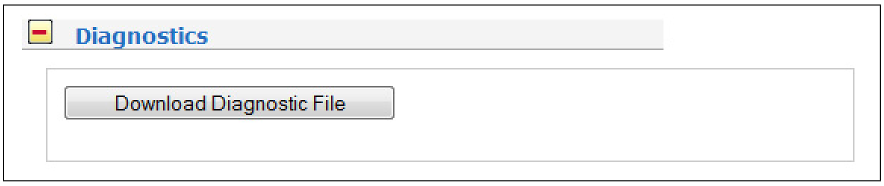
If you need to update the software of your LANTIME, you need a special file from Meinberg, which can be uploaded to the LANTIME by first choosing the file on your local computer with the “Browse” button and then press “Start Update”.



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.

8.7.8 Download Diagnostic File

A diagnostic file which includes all status data of a LANTIME system logged since the last reboot can be downloaded from all LANTIME Time servers. The file format of the diagnostic file is a tgz-archive. The archive contains all the important configuration and logfiles. In most support cases it is the first action to ask the customer to download the diagnostic file, because it is very helpful to identify the current state of the LANTIME and to find possible errors.



Download via Web Interface

1. Open the "System" page and the submenu "Diagnostics".
2. Press the "Download Diagnostic File" button.
3. Send the tgz-archive with a short description of your problem
   to our technical support: techsupport@meinberg.de

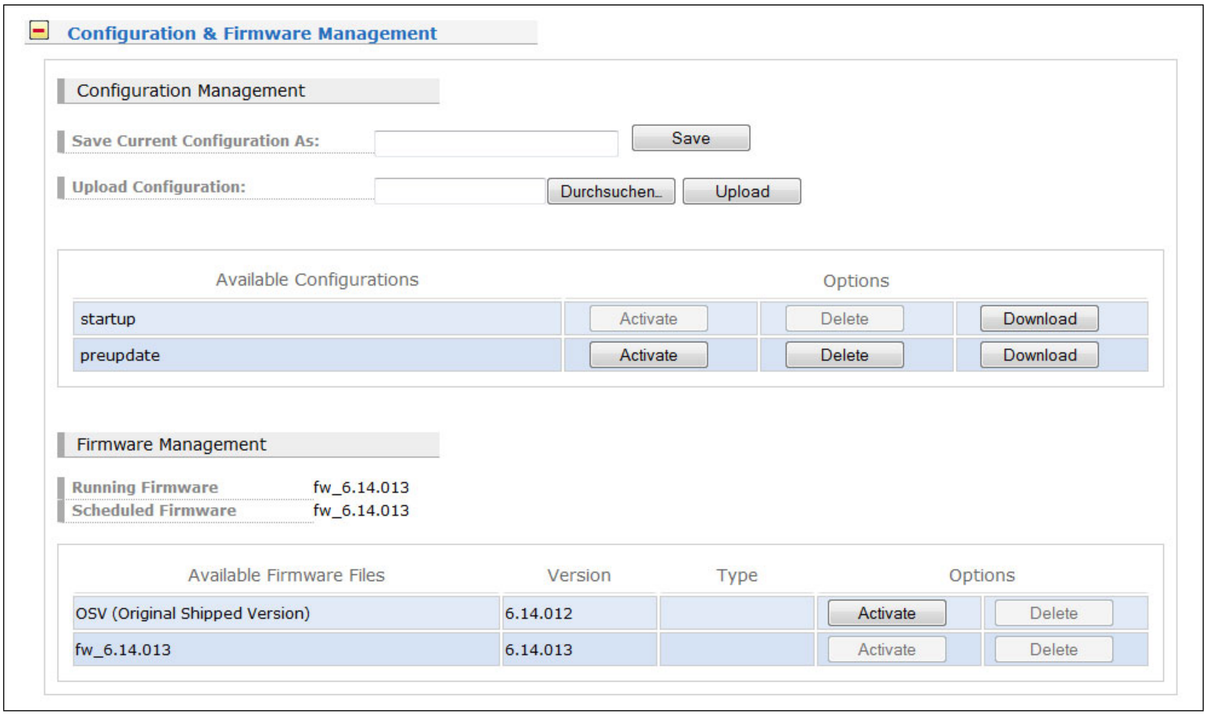
8.7.9 Download Diagnostic File

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 “lt_diag_**.tgz“ to your local computer. If you have any questions or problems with your LANTIME please send this diagnostic file as an attachment of an e-mail to Meinberg support and describe your problem.

8.7.10 Configuration and Firmware Management

With this menu you can save the current configuration on the flash memory of the LANTIME. On this way it is possible to save different configuration files on the system. Later you can activate a stored configuration as startup file.

Additionally more than one Firmware version can be archived on the LANTIME. If a updated version is not correspond correctly in the environment, then it is possible to reload an established version on the LANTIME.



Configuration & Firmware Management

Configuration Management

Save Current Configuration As: [Save]

Upload Configuration: [Durchsuchen...] [Upload]

Available Configurations	Options		
startup	Activate	Delete	Download
preupdate	Activate	Delete	Download

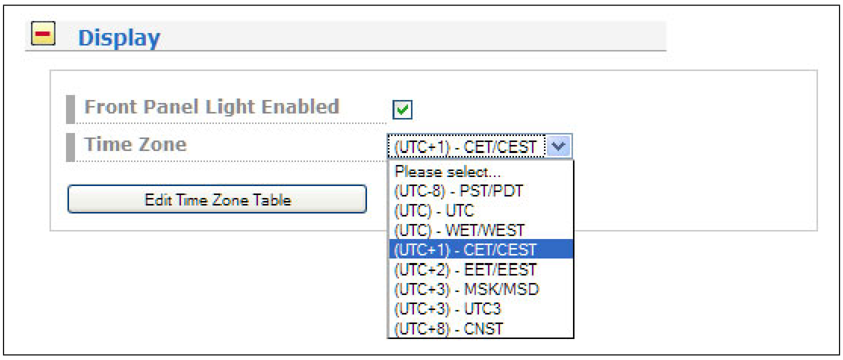
Firmware Management

Running Firmware fw_6.14.013

Scheduled Firmware fw_6.14.013

Available Firmware Files	Version	Type	Options	
OSV (Original Shipped Version)	6.14.012		Activate	Delete
fw_6.14.013	6.14.013		Activate	Delete

8.7.11 Display



Display

Front Panel Light Enabled ☑

Time Zone (UTC+1) - CET/CEST

Time Table:
Here you can edit the Time Table directly. You can add a new timezone with daylight savings and the app. parameters. So you can show the local time on the LC Display of the LANTIME.

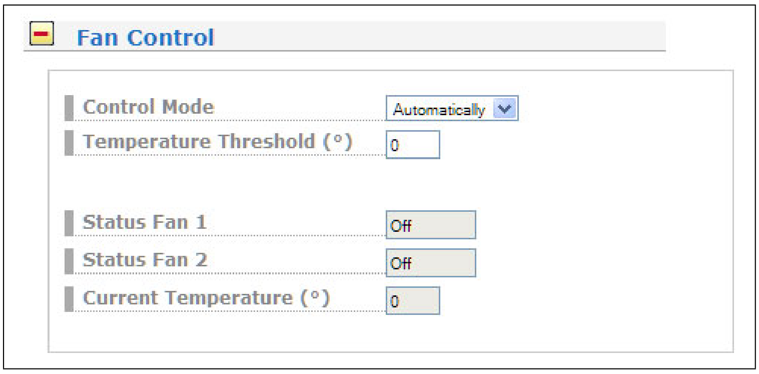
Example:

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

The string above is the local time zone of middle europe. The offset from UTC is +1 hour. Daylight saving ON with an offset of +2 hours on 25th of march at 2:00 am and OFF at 3:00 am at 25th of october.

The first part of the character string (the Komma is delimiter), you can see as option in the dropdown selection list.

8.7.12 Option: Fan Control



Fan Control

Control Mode: Automatically

Temperature Threshold (°): 0

Status Fan 1: Off

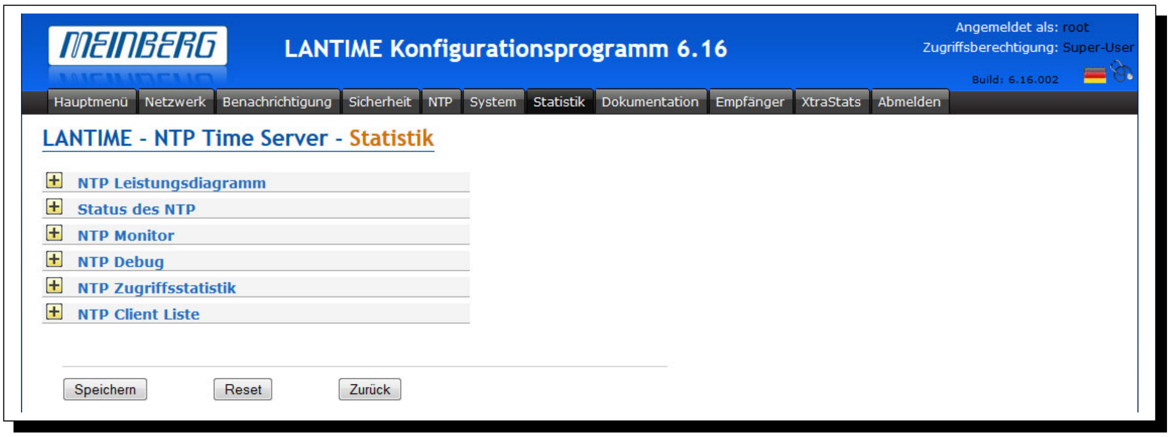
Status Fan 2: Off

Current Temperature (°): 0

With the optional fan control menu the current status of the operational temperature and the fans can be displayed on the systems interface. The mode of the fans can be selected here:

On the ventilators are always running
Off the ventilators are off
Automatically the ventilation runs from the temperature, which is specified by the "Temperature Threshold" parameter. This value is only editable, if the operation mode "Automatically" is selected. If the temperature of the device is less than 7 degrees (Celsius) as the specified value, the fan control turns off automatically.

8.8 Configuration: Statistics



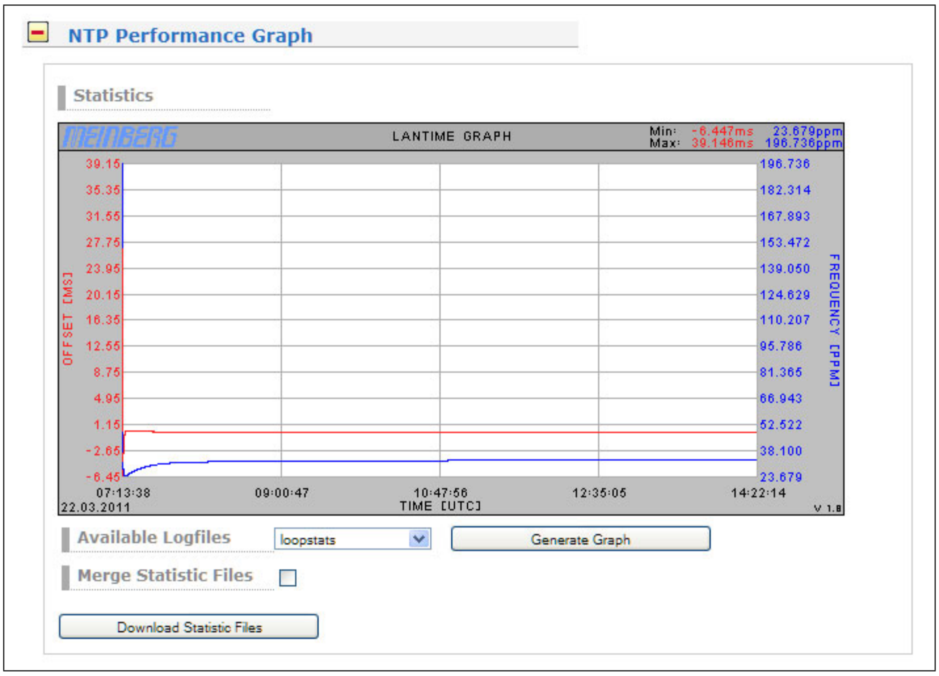
LANTIME Konfigurationsprogramm 6.16

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

LANTIME - NTP Time Server - Statistik

- ⊞ NTP Leistungsdiagramm
- ⊞ Status des NTP
- ⊞ NTP Monitor
- ⊞ NTP Debug
- ⊞ NTP Zugriffsstatistik
- ⊞ NTP Client Liste

NTP Performance Graph



⊟ NTP Performance Graph

Statistics

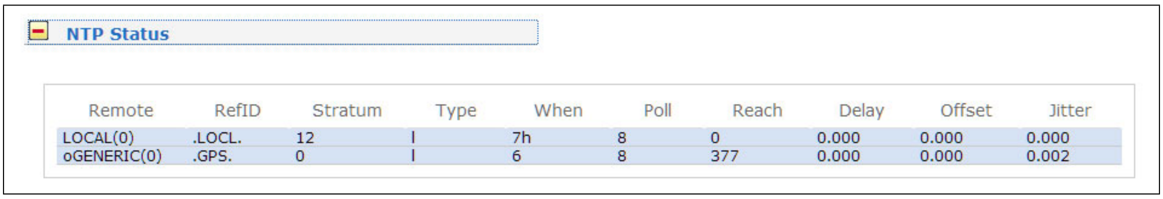
Available Logfiles: loopstats

Merge Statistic Files □

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.

NTP Status

After that a list of all actually refclocks of the internal NTP server will be shown. The last section will show some NTP specific informations about the refclock.

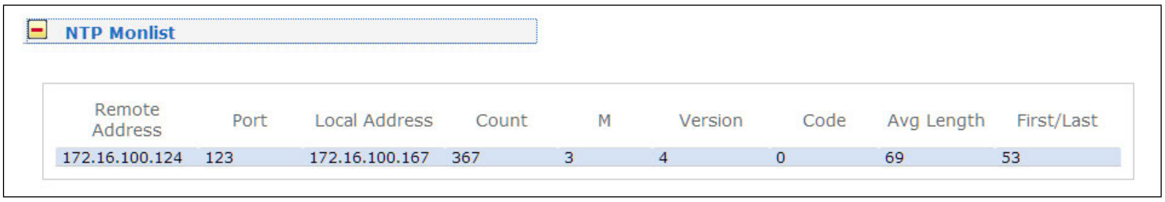


Remote	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
LOCAL(0)	.LOCL.	12	l	7h	8	0	0.000	0.000	0.000
oGENERIC(0)	.GPS.	0	l	6	8	377	0.000	0.000	0.002

with the following meaning:

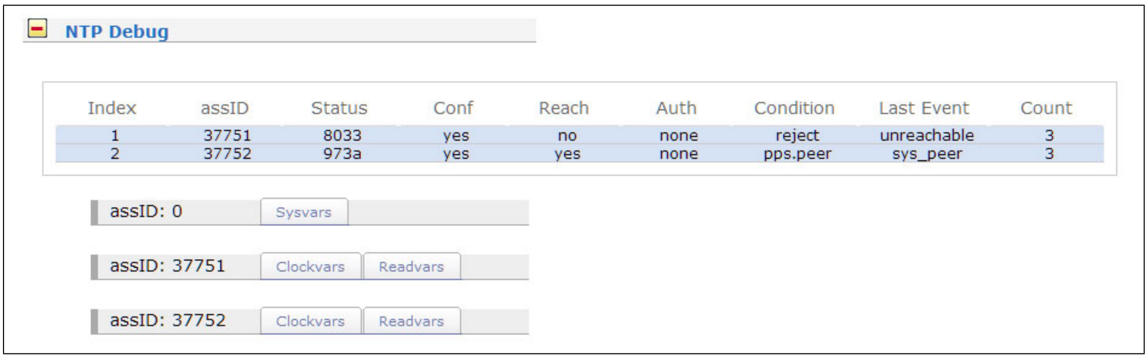
- remote:	list of all valid time servers (ntp.conf)
- refid:	reference number
- st:	actual stratum value (hierarchy level)
- when:	last request (seconds)
- poll:	period of requesting the time server (seconds)
- reach:	octal notation of the successful requests, shifted left
- delay:	delay of the network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

NTP Monitor



Remote Address	Port	Local Address	Count	M	Version	Code	Avg Length	First/Last
172.16.100.124	123	172.16.100.167	367	3	4	0	69	53

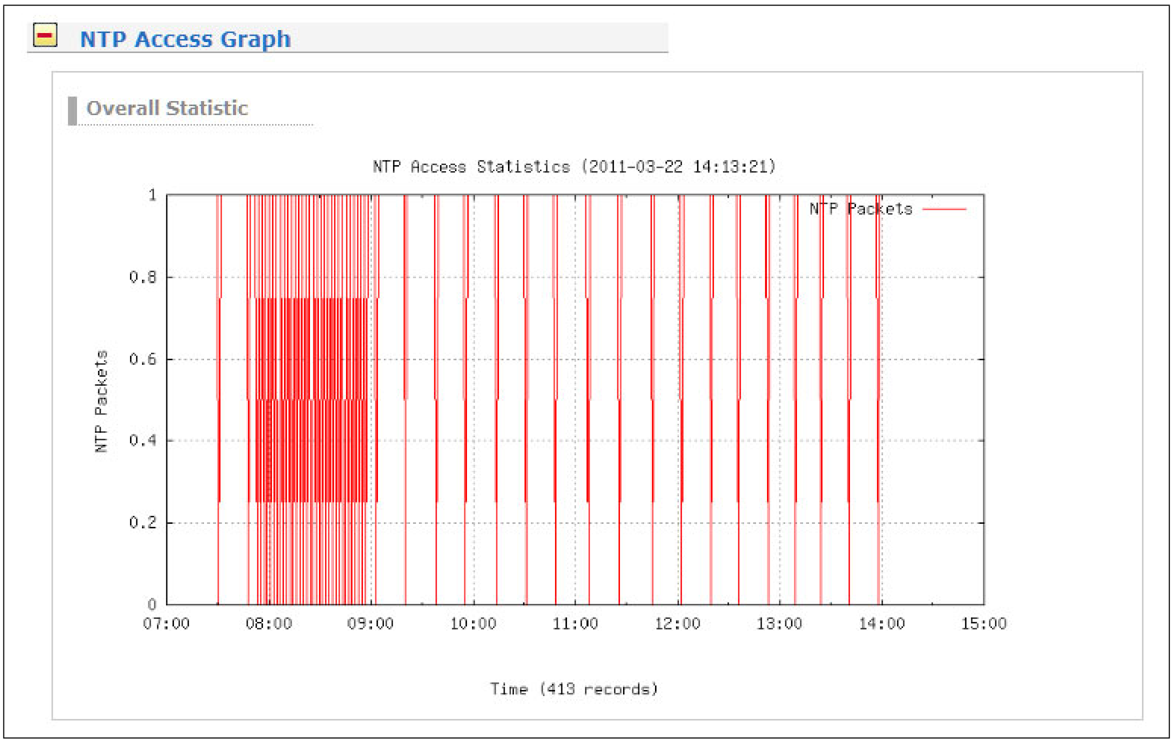
NTP Debug



Index	assID	Status	Conf	Reach	Auth	Condition	Last Event	Count
1	37751	8033	yes	no	none	reject	unreachable	3
2	37752	973a	yes	yes	none	pps.peer	sys_peer	3

NTP Access Graph

In the next section all NTP clients accessing the NTP server are listed. This list is maintained internally by NTPD, clients who did not access the NTPD for a longer period are automatically removed. This section can grow very long in large networks. There are no further information found about the parameters “code, avglen and



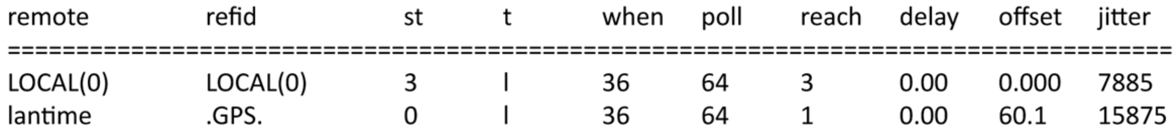
first. The name resolution of the IP address in the first colume will take too much time; so its disabled.

8.8.1 Statistical Information

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

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

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



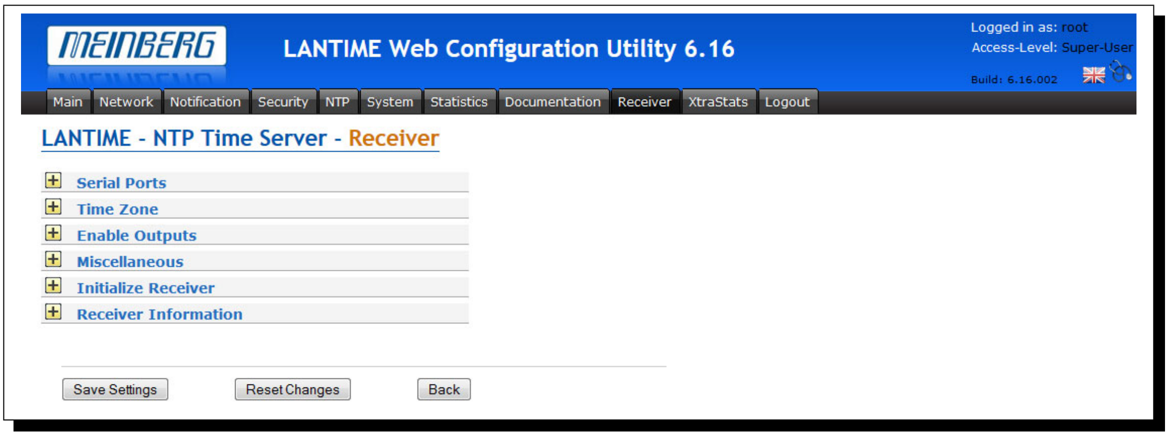
```
remote       refid        st    t     when   poll   reach   delay   offset   jitter
==================================================================================
LOCAL(0)     LOCAL(0)     3     l     36     64     3       0.00    0.000    7885
lantime      .GPS.        0     l     36     64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

with the following meaning:

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

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

8.9 Configuration: Receiver



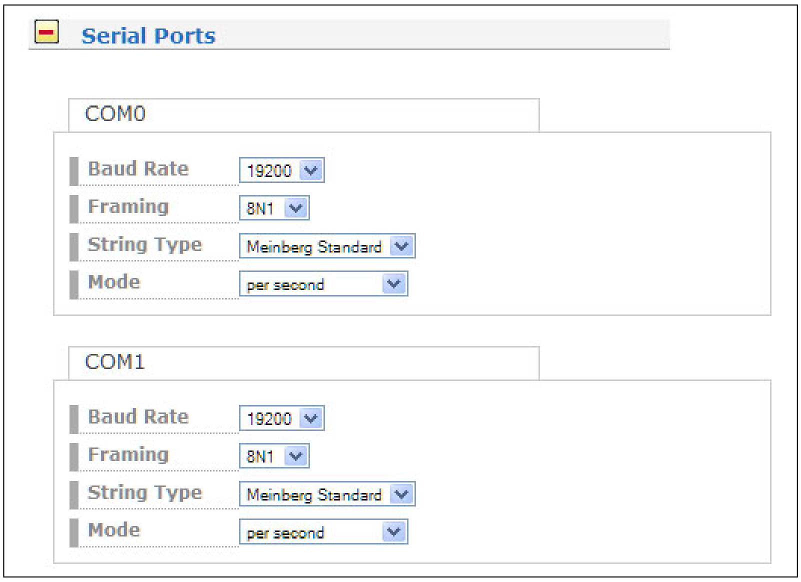
LANTIME - NTP Time Server - Receiver

⊞ Serial Ports
⊞ Time Zone
⊞ Enable Outputs
⊞ Miscellaneous
⊞ Initialize Receiver
⊞ Receiver Information

On this page you can edit the important receiver settings like "Serial Ports" or "Time Zone" and you can get an overview about the information of ypur LANTIME's internal receiver.

8.9.1 Serial Ports

This menu lets the user configure the baud rate, the framing and the string type of the serial RS232 port to one of the following values:



⊟ Serial Ports

COM0

Baud Rate: 19200
Framing: 8N1
String Type: Meinberg Standard
Mode: per second

COM1

Baud Rate: 19200
Framing: 8N1
String Type: Meinberg Standard
Mode: per second

Baud Rate: 300 to 19200
Framing: 7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8N1, 8N2, 8O1

Selectable Telegrams

- Meinberg Standard
- SAT
- NMEA RMC
- Uni Erlangen

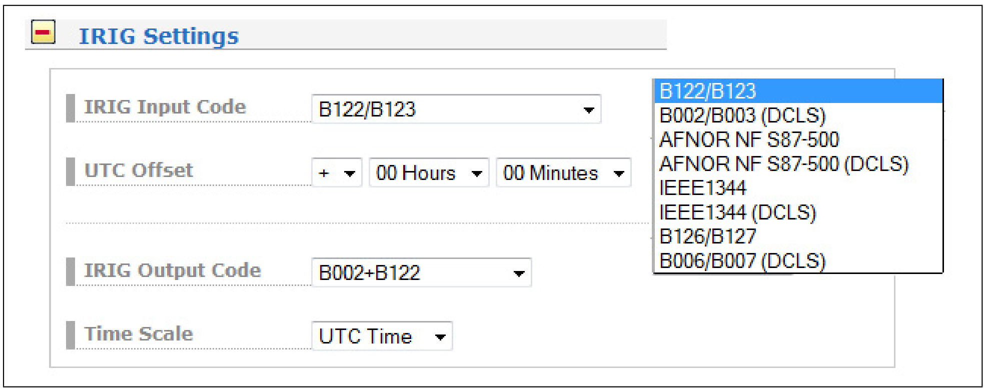
- Computime
- Sysplex 1
- Meinberg Capture
- SPA
- RACAL
- Meinberg GPS
- NMEA GGA
- NMEA RMC GGA
- NMEA ZDA
- ION

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

Default settings: COM:19200 baud, 8N1, per second, Meinberg Standard Time String

8.9.2 IRIG Settings

With IRIG Settings you can adjust the IRIG/AFNOR outputs of the device:



IRIG Settings

IRIG Input Code: B122/B123

UTC Offset: + 00 Hours 00 Minutes

IRIG Output Code: B002+B122

Time Scale: UTC Time

B002+B122	IRIG-B 100PPS:
DC Level Shift (DCLS), No carrier(DCLS),
coding of time (HH,MM,SS,DDD)
+
modulated, 1 kHz / 1 millisecond resolution,
coding of time (HH,MM,SS,DDD), Control Functions

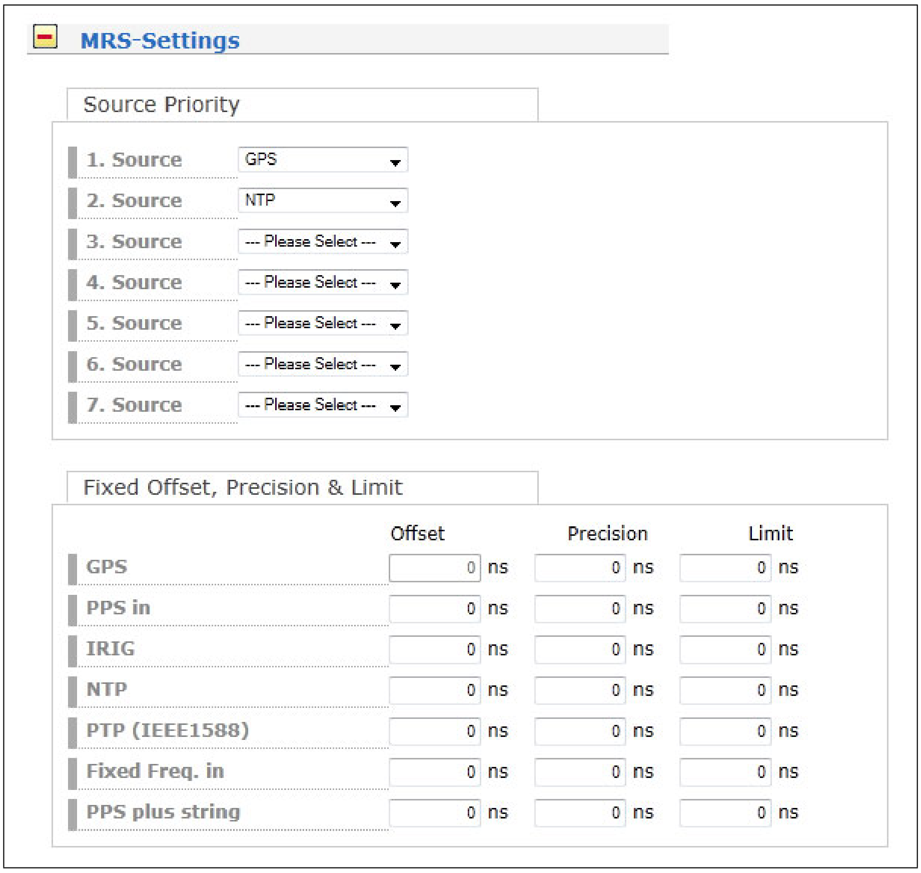
B003+B123	like B002+B122, with second of day (0....86400)

AFNOR NF S87-500	AFNOR NFS 87-500 is a standarized french time code
similar to IRIG-B but contains additional day,
day-of-month and year information.

IEEE1344	Additional extensions to the IRIG-B time code:
year, time quality, daylight savings time, local time offset
and leap second information

8.9.3 MRS Settings

With this submenu you can setup some important parameters of the selected systems reference time:



MRS-Settings

Source Priority

1. Source	GPS
2. Source	NTP
3. Source	--- Please Select ---
4. Source	--- Please Select ---
5. Source	--- Please Select ---
6. Source	--- Please Select ---
7. Source	--- Please Select ---

Fixed Offset, Precision & Limit

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

In the next menu the user can define in which order the references will be used to control the internal oscillator. The reference clock with the highest priority will be used always if this is available. You can set an fixed offset for the available references in the next sub menu. By default this value is 0 ns. The bias of the internal GPS receiver can not be set up – indirectly this can be done via the antenna cable length.

Possible values for reference input signals:

GPS	GPS signal of internal receiver
PPS in	PulsePerSecond input reference
IRIG	IRIG Time Code (DCLS/AM)
NTP	external NTP time server
PTP (IEEE1588)	IEEE 1588 Grandmaster
Fixed Freq. in	Frequency input

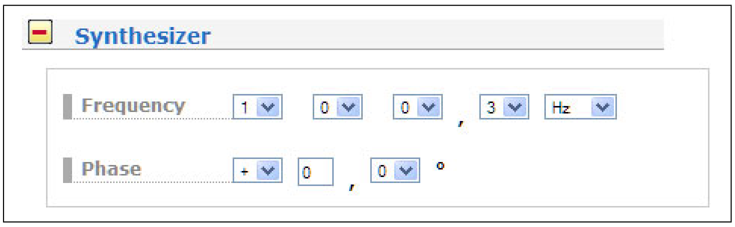
Each reference clock can be assigned a specific precision which will reflect the accuracy of the reference clock. This precision value will determine the hold over time when switching to the next reference clock if the current master is not available anymore. If the precision is 0 the next reference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

The parameter „constant“ depends on the quality of the internal oscillator!

Example: the external PPS with an precision of 100ns is the current master. If this master is no longer available it will switch to the next reference source of the priority order – in this case the IRIG input with an precision of

10us. With the formula ((10000ns/100ns)*11.4) we get hold over time of 19min. The online display of the MRS status will show the remaining time and the calculated time. The hold over time will be recalculated if the status of the reference clocks will change.

8.9.4 Synthesiser



Synthesizer

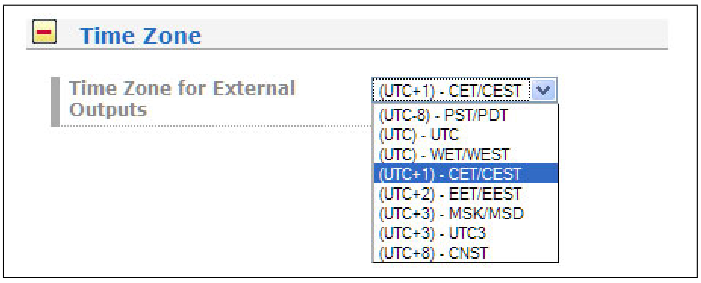
Frequency: 1 0 0 , 3 Hz

Phase: + 0 , 0 °

Here you can edit the frequency and phase to be generated by the on-board synthesizer. Frequencies from 1/8 Hz up to 10 MHz can be entered using four digits and a range. If frequency is set to 0 the synthesizer is disabled.

With "Phase" you can enter the phase of the generated frequency from -360° to +360° with a resolution of 0.1°. Increasing the phase lets the signal come out later. Phase affects frequencies less than 10.00 kHz only!

8.9.5 Time Zone

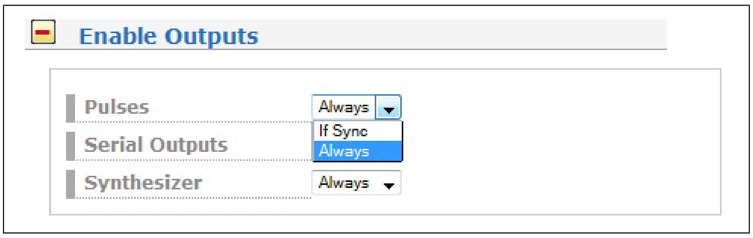


Time Zone

Time Zone for External Outputs: (UTC+1) - CET/CEST

With the dropdown list you can select the local time zone. You can add more values to the list with the menu you find in "System -> Display -> Edit Time Zone Table".

8.9.6 Enable Outputs



Enable Outputs

Pulses: Always

Serial Outputs

Synthesizer: Always

This menu lets the user configure at which time after power up the serial ports are enabled. Outputs which are enabled "always" will be enabled immediately after power up. Outputs which are enabled "if sync" will be enabled after the integrated receiver is running in normal operation mode.

8.9.7 Miscellaneous

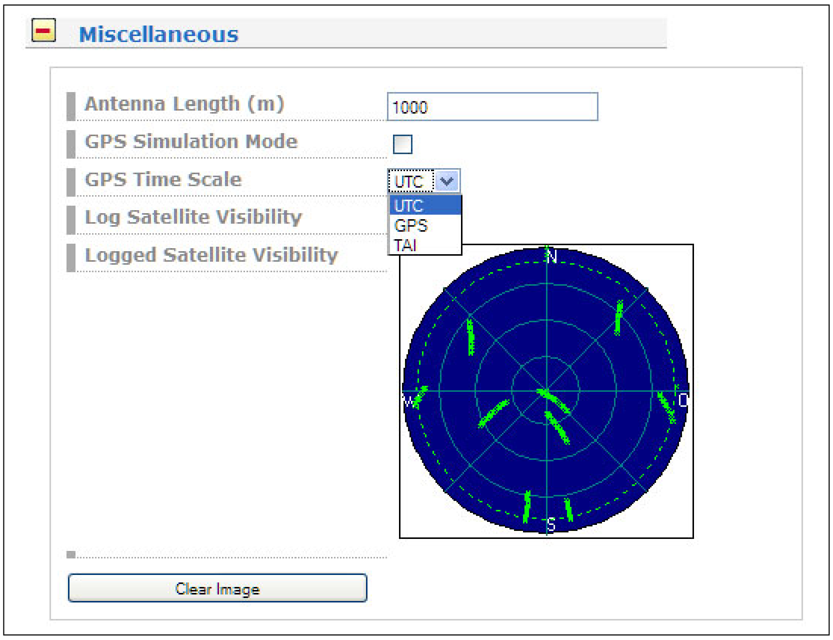
GPS Receiver:

1. Antenna Cable Length:
Enter the length of the antenna cable here. The received time frame is delayed by approx. 5 ns per meter antenna cable. The receiver is able to compensate this delay if the exact cable length is given. The default value is 20 m. The maximum value you can enter in this field is 500m. In case of longer cable runs you have to use an amplifier or a fiber optic connection.

2. GPS Simulation Mode (GPS Receiver)
Enabling this menu lets the user run the LANTIME without antenna. Normally the NTPD loses synchronisation with the GPS when the antenna is disconnected or the GPS did not receive enough satellites (red FAIL LED is turned on). So it is possible to set the NTPD with any other time. If this option is enabled an "*" will be shown behind the time string in the root menu of the display.

3. GPS Time Scale (GPS Receiver)
You can select between the following values:
UTC - Coordinated Universal Time (including leap seconds)
GPS - since 1th of January 1980 - equivalent to TAI Time Scale with the difference from a constant value of 19 seconds (this time scale includes the leap seconds from 1980 until today).
TAI - since 1968, 1th of January 1900 as reference start time - International Atomic Time (without Leap Seconds)

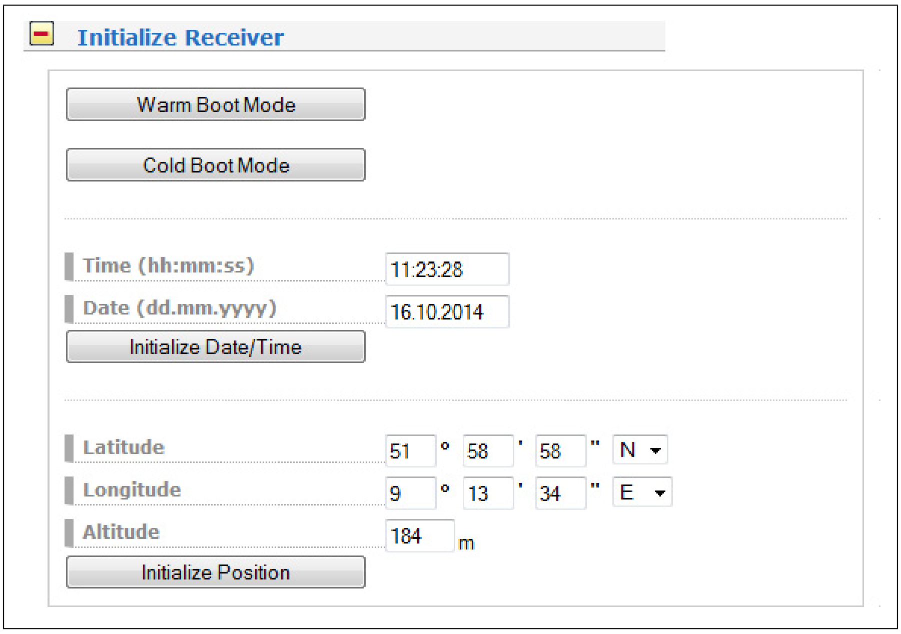
4. Logged Satellite Visibility (GPS Receiver)
If this checkbox is activated, the system generates a graphic from the constellation of the visible satellites.



Miscellaneous

Antenna Length (m): 1000
GPS Simulation Mode: □
GPS Time Scale: UTC
Log Satellite Visibility
Logged Satellite Visibility

Init Receiver (GPS Receiver)



Time (hh:mm:ss) 11:23:28

Date (dd.mm.yyyy) 16.10.2014

Latitude 51 ° 58 ' 58 " N

Longitude 9 ° 13 ' 34 " E

Altitude 184 m

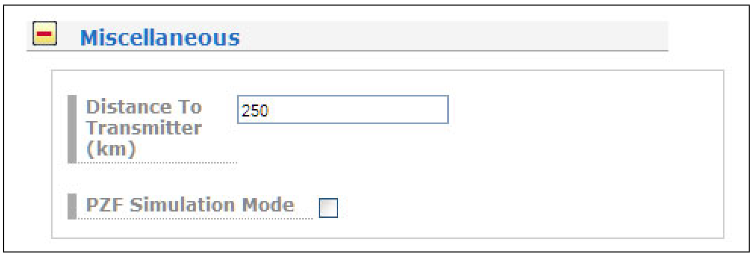
Warm Boot Mode (GPS Receiver)

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

Cold Boot Mode (GPS Receiver)

With this button you can initialize all GPS data, i.e. all saved satellite data will be cleared. You have to confirm this operation before the initialisation starts. The system starts operating in the COLD BOOT mode and seeks for a satellite to read its actual parameters. Please note, that the GPS receiver needs approximately 15 minutes for the initiated COLD BOOT!

Long Wave Receiver (DCF77, MSF, WWVB):



Distance To Transmitter (km) 250

PZF Simulation Mode □

Distance to Transmitter

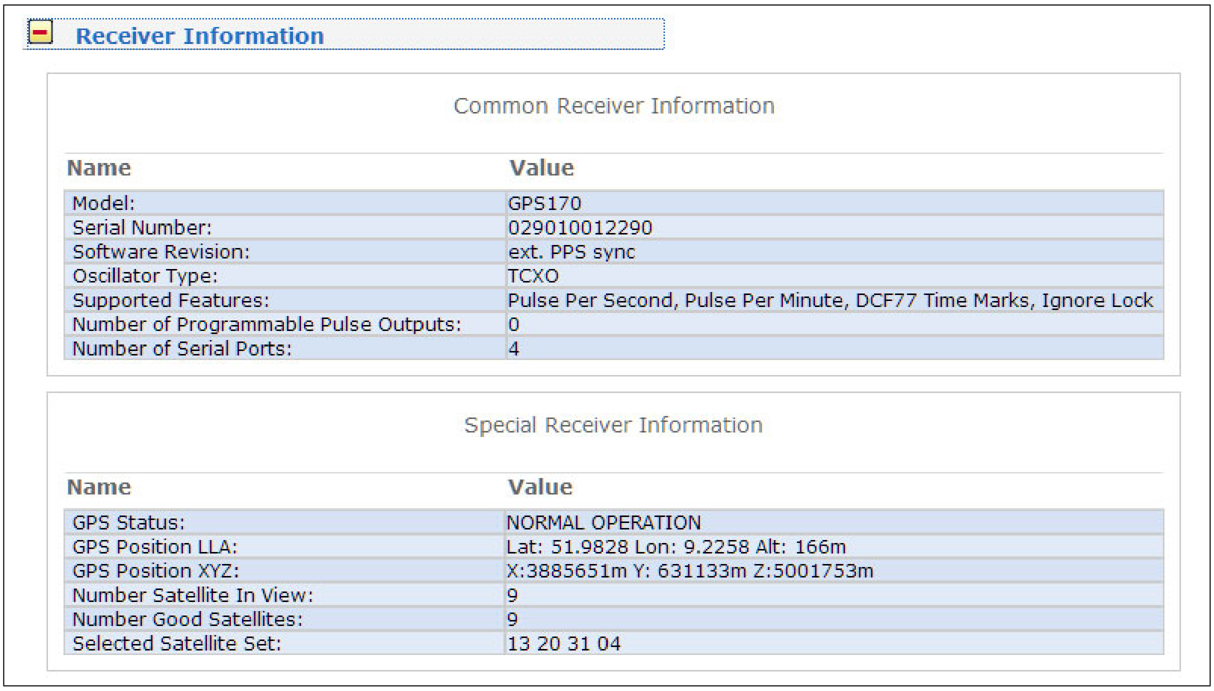
In this submenu the distance to the transmitter is entered for compensating the propagation delay of the received pseudo-random code. This setting should be done as exact as possible because the absolute precision of the time frame is influenced by this value.

Simulation Mode

With "Simulation Mode" the user enable or disable the SYNC simulation mode. If you want to use the receiver without connecting an antenna this mode will simulate a valid output for the NTP daemon. This is only for test purposes. "Simulation Mode" should be disabled under normal operating conditions.

8.9.8 Receiver Information

Here you can indicate all important and relevant information about the used receiver and its internal oscillator



Receiver Information

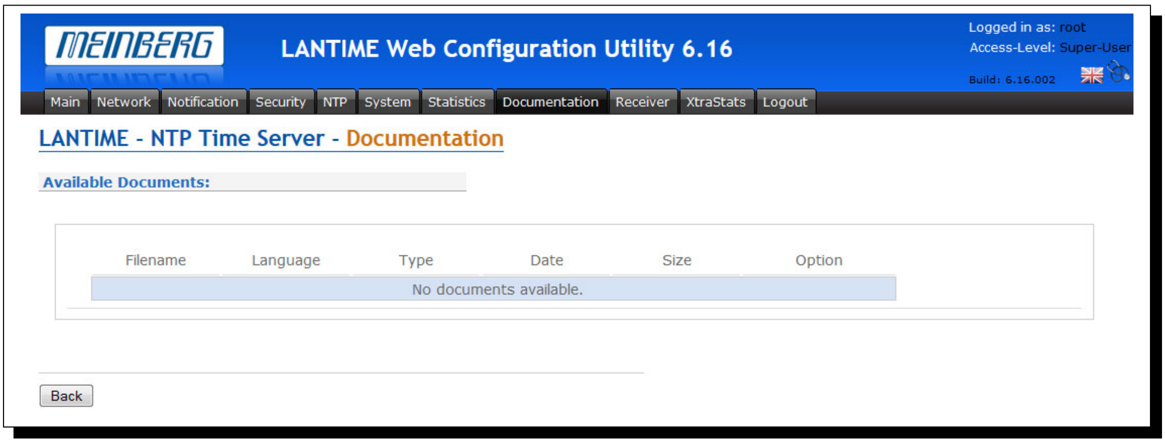
Common Receiver Information

Name	Value
Model:	GPS170
Serial Number:	029010012290
Software Revision:	ext. PPS sync
Oscillator Type:	TCXO
Supported Features:	Pulse Per Second, Pulse Per Minute, DCF77 Time Marks, Ignore Lock
Number of Programmable Pulse Outputs:	0
Number of Serial Ports:	4

Special Receiver Information

Name	Value
GPS Status:	NORMAL OPERATION
GPS Position LLA:	Lat: 51.9828 Lon: 9.2258 Alt: 166m
GPS Position XYZ:	X:3885651m Y: 631133m Z:5001753m
Number Satellite In View:	9
Number Good Satellites:	9
Selected Satellite Set:	13 20 31 04

8.10 Configuration: Documentation

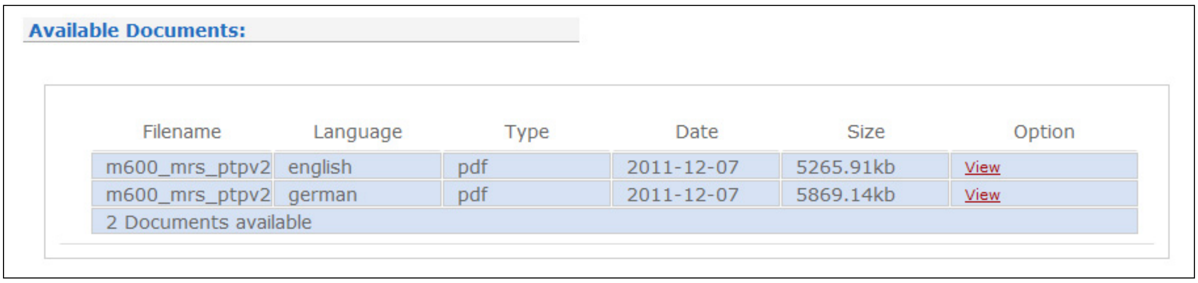


LANTIME - NTP Time Server - Documentation

Available Documents:

Filename	Language	Type	Date	Size	Option
No documents available.					

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.



Available Documents:

Filename	Language	Type	Date	Size	Option
m600_mrs_ptpv2	english	pdf	2011-12-07	5265.91kb	View
m600_mrs_ptpv2	german	pdf	2011-12-07	5869.14kb	View
2 Documents available					

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

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

9 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).

9.1 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 - LANTIME Services" (V5) or "System - Services and Functions" (V6) 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.

9.1.1 Examples for the usage of the SNMP configuration features

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

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

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

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

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

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

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

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

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

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

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

root@testhost:/#
```

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

9.1.2 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.

9.1.3 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, winpopup, 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.

9.1.4 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 syslogserver
	mbgLtCfgSyslogserver2	string (IPv4 or IPv6-address or hostname)	IP-address or hostname of second syslogserver
	mbgLtCfgTelnetAccess	integer (0 = disabled, 1 = enabled)	Telnet access activated?
	mbgLtCfgFTPAccess	integer (0 = disabled, 1 = enabled)	FTP-access activated?
	mbgLtCfgHTTPAccess	integer (0 = disabled, 1 = enabled)	Webinterface activated?
	mbgLtCfgHTTPSAccess	integer (0 = disabled, 1 = enabled)	Encrypted webinterface activated?
	mbgLtCfgSNMPAccess	integer (0 = disabled, 1 = enabled)	SNMP-daemon activated?

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

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

SNMP branch	Variable	Data type	Description
mbgLtCfgWalldisplay	mbgLtCfgVP100Display1IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the first wall-mount display used for showing notifications
	mbgLtCfgVP100Display 1SN	string (Hexstring)	The serial number of the first wall mount display used for showing notifications (can be found in the setup menu of the display)
	mbgLtCfgVP100Display 2IP	string (IPv4 or IPv6-address or hostname)	hostname or IP-address of the second wall mount display used for showing notifications
	mbgLtCfgVP100Display 2SN	string (Hexstring)	The serial number of the first wall mount display used for showing notifications (can be found in the setup menu of the display)

mbgLtCfgNotify	mbgLtCfgNotifyNTPNot Sync	string(combination)	Exactly one, none or a combination of the following notification types:
			email = sending an email
			wmail = sending a winpopup-message
			snmp = sending a SNMP-trap,
			disp = showing on wall mount display,
			syslog = sending a syslog-entry
			for the event „NTP not synchronized“

	mbgLtCfgNotifyNTP Stopped	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „NTP Daemon stopped“
	mbgLtCfgNotifyServer Boot	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Timeserver reboot“
	mbgLtCfgNotifyRefclock NotResponding	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not ready“
	mbgLtCfgNotifyRefclock NotSync	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Refclock not synchron“
	mbgLtCfgNotifyAntenna Faulty	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna not connected or dammaged“
	mbgLtCfgNotifyAntenna Reconnect	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „GPS antenna reconnected“
	mbgLtCfgNotifyConfig Changed	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Configuration changed“
	mbgLtCfgNotifyLeapSecond Announced	string (combination)	(see mbgLtCfgNotifyNTPNotSync) for the event „Leap second announced“

SNMP branch	Variable	Data type	Description
mbgLtCfgEthernet	mbgLtCfgEthernetIf0IPv4 IP	string (IPv4 IP-address)	IPv4-address of first network interface of the timeserver
	mbgLtCfgEthernetIf0IPv4 Netmask	string (IPv4 Netzmaske)	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!

9.2 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.

9.2.1 SNMP Trap Reference

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

- **mbgLtTrapNTPNotSync (mbgLtTraps.1):** Whenever the NTP daemon (ntpd) looses sync, it will generate this trap and send it to the configured SNMP trap receivers.
- **mbgLtTrapNTPStopped (mbgLtTraps.2):** This trap is sent when the NTP daemon stopped, manually or because of an error condition.
- **mbgLtTrapServerBoot (mbgLtTraps.3):** After finishing the boot process, this trap is generated.
- **mbgLtTrapReceiverNotResponding (mbgLtTraps.4):** Trap to be sent when the internal receiver of the timeserver is not responding.
- **mbgLtTrapReceiverNotSync (mbgLtTraps.5):** If the internal receiver looses sync, the SNMP trap receivers will receive this trap.
- **mbgLtTrapAntennaFaulty (mbgLtTraps.6):** This trap will be sent whenever the timeserver recognises a broken connection to the antenna of the receiver.
- **mbgLtTrapAntennaReconnect (mbgLtTraps.7):** After the connection to the antenna has been reestablished, 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.

10 Attachment: Technical Information

10.1 Technical Specifications LCES

HOUSING:	Metal 19"Modular chassis, Schroff EUROPAC lab HF
PROTECTION RATING:	IP20
INPUT VOLTAGE:	100 ... 240 V AC (+/- 10%),50/60Hz 100 ... 240 V DC (+/- 10%)
CURRENT CONSUMPTION	max 70 W
AMBIENT TEMPERATURE:	0 ... 50°C
PHYSICAL DIMENSIONS:	483 mm wide x 132 mm high x 275 mm deep

10.2 Front and rear panel connectors

Name	**Type**	**Signal**	**Cable / connection**
Front panel			
Terminal	9pin. D-SUB male	RS-232	shielded data line
USB	USB Port	USB Stick	
Network LAN	RJ-45	Ethernet	shielded data line
Rear panel			
Power supply	IEC (power) connector	100-240VAC	power cord
Refclock In	9pin. D-SUB male	RS-232	shielded data line
PPS In	BNC female	Pulse Per Second	shielded data line

10.3 LNE: Additional ethernet ports for LANTIME time servers

LANTIME Network Expansion LNE, additional network ports for LANTIME Time Server

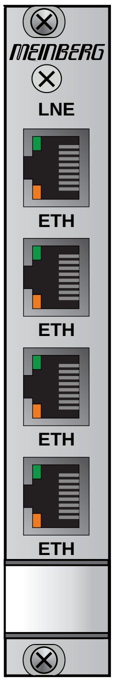
Key Features

- Lantime Expansion for two additional 10/100MBIT Network Connections
- Status LEDs: Connect, Activity, Speed
- RJ45 Network Connectors in the Front Panel

Description

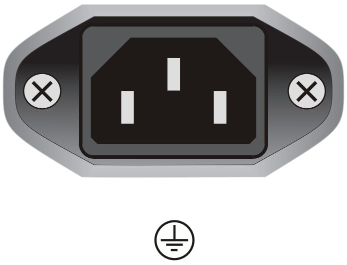
The module LNE extends a LANTIME NTP time server (3U models) with additional network connections. LANTIME models in 1U cases can be ordered with two additional network ports, too.

The additional ports can be used to provide time synchronization to additional separate networks or - by using a feature called "bonding" - to configure redundant network connections (note: the involved active network components like switches have to support this).



10.4 Power connect

Input Voltage Range:	100-240 V AC / 50 - 60Hz 100-240 V DC, (+/- 10%)
Input Current:	1 A$_{max}$
Fuse:	internal, T2.5 A / 250 V
Connector:	input IEC320 AC inlet with cord grips

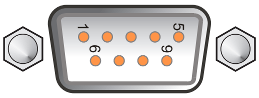


10.5 Refclock In

Signal:	Reference, RS-232
Connector:	D-SUB male 9pol.
Cabel:	shielded data line PC connector (serial port) 1:1

Assignment:

Pin 1:	PPS (optional)
Pin 2:	TxD
Pin 5:	GND



Refclock In

10.6 PPS In

Cable:	shielded coaxial line
pulse length:	5μs, active high
Connector:	BNC female

PPS In

11 Declaration of Conformity

Konformitätserklärung

Doc ID: LCES/NTP/RPS/BGT-2015-07-27

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

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

Produktbezeichnung *Product Designation*	**LCES/NTP/RPS/BGT**

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

EN55022:2010, Class B	Limits and methods of measurement of radio interference characteristics of information technology equipment
EN55024:2010	Limits and methods of measurement of Immunity characteristics of information technology equipment
EN 61000-3-2:2006 (+A1:2009 +A2:2009)	Electromagnetic Compatibility (EMC) Limits for harmonic current emissions
EN 61000-3-3:2008	Electromagnetic Compatibility (EMC) Limitation of voltage fluctuation and flicker in low-voltage supply systems
EN 60950-1:2006 (+A1:2010 +A11:2009 +A12:2011)	Safety of information technology equipment
EN 50581:2012	Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances

gemäß den Richtlinien 2014/30/EU (Elektromagnetische Verträglichkeit), 2014/35/EU (Niederspannungsrichtlinie), 2011/65/EU (Beschränkung der Verwendung bestimmter gefährlicher Stoffe) und 93/68/EWG (CE Kennzeichnung) sowie deren Ergänzungen.
following the provisions of the directives 2014/30/EU (electromagnetic compatibility), 2014/35/EU (low voltage directive), 2011/65/EU (restriction of the use of certain hazardous substances) and 93/68/EEC (CE marking) and its amendments.

Bad Pyrmont, 2015-07-27

Günter Meinberg
Managing Director