



The Synchronization Experts.



## MANUAL

### LANTIME Firmware 6.24

### Configuration and Management Manual

December 1, 2022

Meinberg Funkuhren GmbH & Co. KG



# Table of Contents

<b>1</b>	<b>Imprint</b>	<b>1</b>
<b>2</b>	<b>Important Safety Information</b>	<b>2</b>
2.1	Important Safety Information and Safety Precautions	2
2.2	Used Symbols	3
2.3	Product Documentation	4
2.4	Safety During Installation	5
2.5	Connection of Protective Earth Conductor/Grounding	8
2.6	Safety During Operation	9
2.7	Safety During Maintenance	10
2.8	Handling of Batteries	11
2.9	Cleaning and Care	12
2.10	Prevention of ESD Damage	12
2.11	Return of Electrical and Electronic Equipment	13
<b>3</b>	<b>Before you start</b>	<b>14</b>
3.1	Text and Syntax Conventions	14
3.2	Required Tools	15
3.3	Abbreviation List	16
<b>4</b>	<b>Introduction</b>	<b>18</b>
4.1	Network Configuration Concept	19
4.2	Additional Features	19
4.3	User Interface	19
4.4	Input and Output Options	20
4.5	Network Time Protocol (NTP)	21
4.5.1	NTP Clients	21
4.6	Option: Precision Time Protocol (PTP) / IEEE 1588	22
4.6.1	General Information	23
4.6.2	Functionality in Master Systems	24
4.6.3	Functionality in Slave Systems	25
4.6.4	PTPv2 IEEE 1588–2008 Configuration Guide	26
<b>5</b>	<b>Unboxing</b>	<b>32</b>
<b>6</b>	<b>LANTIME Installation</b>	<b>34</b>
<b>7</b>	<b>Security User Guide / Security Advisories</b>	<b>37</b>
7.1	General Informations	37
7.2	Securing Management	38
7.3	User Management/Administration	38
7.3.1	LANTIME User Management	45
7.3.2	External User Authentication: Radius and TACACS+	45
7.4	Securing Time Service NTP	47
7.5	Event Log Delivery	47
7.6	Update And Backup LANTIME Firmware	47
<b>8</b>	<b>Antenna and Receiver Information</b>	<b>53</b>
8.1	Reference Time Sources	53
8.1.1	Meinberg GPS Receiver	53
8.1.2	Meinberg GNSS Receiver (GPS, GLONASS, Galileo, BeiDou)	54
8.1.3	PZF - DCF77 Long Wave Receiver	55
8.1.4	MSF Receiver	56

8.1.5	WWVB Receiver . . . . .	58
8.1.6	TCR Receiver . . . . .	59
8.2	GNSS Signal Reception . . . . .	60
8.2.1	Meinberg GPS Antenna/Converter . . . . .	61
8.2.2	General GNSS Antennae . . . . .	64
8.2.3	Powering up a GNSS Receiver . . . . .	67
8.3	Long Wave Signal Reception . . . . .	68
8.3.1	Introduction . . . . .	68
8.3.2	Mounting and Installation of a Longwave Antenna . . . . .	69
8.3.3	DCF77 / PZF Receiver . . . . .	71
8.4	Cable Types . . . . .	71
<b>9</b>	<b>LTOS6 Management and Monitoring</b>	<b>72</b>
9.1	Via Web GUI . . . . .	72
9.1.1	Main Menu . . . . .	72
9.1.2	Network . . . . .	77
9.1.3	Notification . . . . .	87
9.1.4	Security . . . . .	97
9.1.5	NTP . . . . .	107
9.1.6	PTP . . . . .	120
9.1.7	FDM - Frequency Deviation Monitoring . . . . .	137
9.1.8	System . . . . .	152
9.1.9	Statistics . . . . .	169
9.1.10	Clock . . . . .	177
9.1.11	I/O Configuration . . . . .	195
9.1.12	Sync Monitoring . . . . .	210
9.1.13	XtraStats . . . . .	236
9.1.14	Documentation & Support . . . . .	238
9.2	Via CLI . . . . .	240
9.2.1	Introduction . . . . .	240
9.2.2	Accessing and Using the CLI . . . . .	241
9.2.3	Command Reference . . . . .	243
9.2.4	Sync Monitor Status and Configuration via CLI . . . . .	282
9.2.5	Text Editors . . . . .	283
9.3	Via Front Panel Display . . . . .	286
9.3.1	LANTIME Display Types . . . . .	286
9.3.2	Front Display - Root Menu . . . . .	291
9.3.3	Menu: Reference Time . . . . .	293
9.3.4	Menu: Time Service . . . . .	310
9.3.5	Menu: Network . . . . .	331
9.3.6	Menu: System . . . . .	336
9.3.7	USB Stick Menu . . . . .	343
9.4	Via Serial Connection . . . . .	346
9.5	Via SNMP . . . . .	347
9.5.1	The Simple Network Management Protocol . . . . .	347
9.5.2	MIB Objects of a LANTIME . . . . .	348
9.5.3	SNMP Traps . . . . .	353
<b>10</b>	<b>Troubleshooting and Alarming</b>	<b>362</b>
10.1	NTP Messages . . . . .	362
10.2	Ref. Clock Messages . . . . .	363
10.3	Network Messages . . . . .	367
10.4	Miscellaneous Messages . . . . .	368
<b>11</b>	<b>Support Information</b>	<b>370</b>
11.1	Basic Customer Support . . . . .	371
11.2	Support Ticket System . . . . .	371
11.3	How to download a Diagnostic File . . . . .	372
11.3.1	Download via Web GUI . . . . .	372
11.3.2	Download via USB Stick . . . . .	372
11.4	Self-Help Online Tools . . . . .	373

11.5	NTP and IEEE 1588-PTP online tutorials . . . . .	373
11.6	The Meinberg Academy introduction and offerings . . . . .	374
11.7	Meinberg Newsletter . . . . .	374
<b>12</b>	<b>Appendix</b>	<b>375</b>
12.1	LANTIME CPU - Central Processing Unit . . . . .	375
12.1.1	Technical Specifications LAN CPU . . . . .	376
12.2	Description of Time String Formats . . . . .	377
12.2.1	Format of the Meinberg Standard Time String . . . . .	377
12.2.2	Format of the Meinberg GPS Time String . . . . .	377
12.2.3	Format of the Meinberg Capture String . . . . .	379
12.2.4	Format of the SAT Time String . . . . .	380
12.2.5	Format of the Uni Erlangen String (NTP) . . . . .	381
12.2.6	Format of the NMEA 0183 String (RMC) . . . . .	383
12.2.7	Format of the NMEA 0183 String (GGA) . . . . .	384
12.2.8	Format of the NMEA 0183 String (ZDA) . . . . .	385
12.2.9	Format of the ABB SPA Time String . . . . .	386
12.2.10	Format of the Computime Time String . . . . .	387
12.2.11	Format of the RACAL Standard Time String . . . . .	388
12.2.12	Format of the SYSPLEX-1 Time String . . . . .	389
12.2.13	Format of the ION Time String . . . . .	390
12.2.14	Format of the ION Blanked Time String . . . . .	391
12.2.15	Format of the IRIG-J Timecode . . . . .	392
12.3	SyncMon Formats . . . . .	393
12.4	Third party software . . . . .	394
12.4.1	Operating System GNU/Linux . . . . .	394
12.4.2	Samba . . . . .	394
12.4.3	Network Time Protocol Version 4 (NTP) . . . . .	395
12.4.4	lighttpd . . . . .	396
12.4.5	GNU General Public License (GPL) . . . . .	397
12.5	List of Literature . . . . .	401

# 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 - 230

Website: <https://www.meinbergglobal.com>

Email: [info@meinberg.de](mailto:info@meinberg.de)

Date: December 1, 2022

## 2 Important Safety Information

### 2.1 Important Safety Information and Safety Precautions

The following safety information must be observed whenever the device is being installed or operated. Failure to observe this safety information and other special warnings or operating instructions in the product manuals constitutes improper usage and may violate safety standards and the manufacturer's requirements.



Depending on the configuration of your device or installed options, some information may not specifically apply to your device.



The device satisfies the requirements of the following EU regulations: EMC Directive, Low Voltage Directive, RoHS Directive and—where applicable—the Radio Equipment Directive.

If a procedure is marked with the following signal words, you may only proceed with it if you have understood and fulfilled all requirements. Hazard notices and other relevant information are classified and indicated as such in this manual according to the following system:



#### **DANGER!**

This signal word indicates a hazard with a high risk level . Such a notice refers to a procedure or other action that will very likely result in serious injury or even death if not observed or if improperly performed.



#### **WARNING!**

This signal indicates a hazard with a medium risk level . Such a notice refers to a procedure or other action that may result in serious injury or even death if not observed or if improperly performed.



#### **CAUTION!**

This signal word indicates a hazard with a low risk level . Such a notice refers to a procedure or other action that may result in minor injury if not observed or if improperly performed.















#### **ATTENTION!**

This signal word refers to a procedure or other action that may result in product damage or the loss of important data if not observed or if improperly performed.

## 2.2 Used Symbols

The following symbols and pictograms are used in this manual. Pictograms are used in particular to indicate potential hazards in all hazard categories.

Symbol	Beschreibung / Description
	IEC 60417-5031 Gleichstrom / <i>Direct current</i>
	IEC 60417-5032 Wechselstrom / <i>Alternating current</i>
	IEC 60417-5017 Erdungsanschluss / <i>Earth (ground) terminal</i>
	IEC 60417-5019 Schutzleiteranschluss / <i>Protective earth (ground) terminal</i>
	ISO 7000-0434A Vorsicht / <i>Caution</i>
	IEC 60417-6042 Vorsicht, Risiko eines elektrischen Schlages / <i>Caution, risk of electric shock</i>
	IEC 60417-5041 Vorsicht, heiße Oberfläche / <i>Caution, hot surface</i>
	IEC 60417-6056 Vorsicht, Gefährlich sich bewegende Teile / <i>Caution, moving parts</i>
	IEC 60417-6172 Trennen Sie alle Netzstecker / <i>Disconnect all power connectors</i>
	IEC 60417-5134 Elektrostatisch gefährdete Bauteile / <i>Electrostatic Discharge Sensitive Devices</i>
	IEC 60417-6222 Information generell / <i>General information</i>
	2012/19/EU Dieses Produkt fällt unter die B2B Kategorie. Zur Entsorgung muss es an den Hersteller übergeben werden. <i>This product is handled as a B2B-category product. To ensure that the product is disposed of in a WEEE-compliant fashion, it must be returned to the manufacturer.</i>



## 2.3 Product Documentation

Detailed product documentation is provided on a USB flash drive delivered with the Meinberg system. The manuals can also be downloaded from the Meinberg website at <https://www.meinbergglobal.com>, where you can enter your system name into the search box at the top of the page to find the relevant manual. Alternatively, contact Meinberg Support for further assistance.

The "Docs & Support" menu on the Web Interface also provides user manuals for time server administrators.



This manual contains important safety instructions for the installation and operation of the device. Please read this manual thoroughly before using the device.

This device may only be used for the purpose described in this manual. In particular, the specified operating limits of the device must be heeded. The person setting up the device is responsible for safety matters in relation to any larger system in which the device is installed!

Failure to observe these instructions may have an adverse impact on device safety!

Please keep this manual in a safe place.

### Target Readership

This manual is only intended to be used by qualified electricians, or by persons who have been appropriately instructed by a qualified electrician and who are familiar with applicable national standards and with safety rules & regulations. This device may only be installed, set up, and operated by qualified personnel.

## 2.4 Safety During Installation



### WARNING!

#### Pre-Operation Procedures and Preparation for Use

This mountable device has been designed and examined in accordance with the requirements of the standard IEC 62368-1 "Audio/Video, Information and Communication Technology Equipment - Part 1: Safety Requirements".

When the mountable device is to be used as part of a larger unit (e.g., electrical enclosure), there will be additional requirements in the IEC 62368-1 standard that must be observed and complied with. General requirements regarding the safety of electrical equipment (such as IEC, VDE, DIN, ANSI) and applicable national standards must be observed in particular.

The device has been developed for use in the industrial sector or in home environments and may only be used in such environments. In environments at risk of high environmental conductivity ("high pollution degree" according to IEC 60664-1), additional measures such as installation of the device in an air-conditioned electrical cabinet may be necessary.

#### Transport, Unpacking, Installation

If the unit has been brought into the usage area from a cold environment, condensation may develop; in this case, wait until the unit has adjusted to the temperature and is completely dry before setting it up.

When unpacking & setting up, and before operating the equipment, be sure to read the information on installing the hardware and the specifications of the device. These include, for example, dimensions, electrical characteristics, or necessary environmental conditions.

Fire safety standards must be upheld with the device in its installed state.

The device must not be damaged in any way when mounting it. In particular, holes must not be drilled into the housing.

For safety reasons, the device with the highest mass should be installed at the lowest position in the rack. Further devices should be installed from the bottom, working your way up.

The device must be protected against mechanical & physical stresses such as vibration or shock.



### Connecting Data Cables

Do not connect or disconnect data cables during a thunderstorm, as doing so presents a risk in the event of a lightning strike.

The device cables must be connected or disconnected in the order specified in the user documentation for the device. Cables should always be held by the connector body when connecting or disconnecting them. Never pull a connector out by pulling on the cable. Doing so may cause the plug to be detached from the cable or cause damage to the plug itself.

Cables must be installed so that they do not represent a health & safety hazard (e.g., tripping) and are not at risk of damage (e.g., kinks).

### Connecting the Power Supply

This equipment is operated at a hazardous voltage. Failure to observe the safety instructions in this manual may result in serious injury, death or property damage.

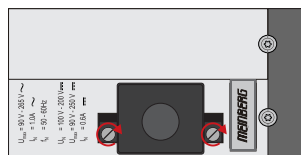
Before the device is connected to the power supply, a grounding conductor must be connected to the earth terminal of the device.

The power supply should be connected with a short, low-inductance cable.

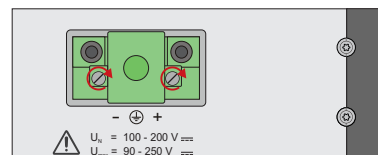
Before operation, check that all cables and lines work properly and are undamaged. Ensure in particular that the cables do not have kinks, that they are not wound too tightly around corners, and that no objects are placed on the cables.

Ensure that all connections are secure—make sure that the lock screws of the power supply plug are tightened when using a 3-pin MSTB or 5-pin MSTB connector (see diagram, LANTIME M300 power supply).

5-Pin MSTB Connector



3-Pin MSTB Connector



Faulty shielding or cabling and improperly connected plugs are a health & safety risk (risk of injury or death due to electrical shock) and may damage or even destroy your Meinberg device or other equipment.

Ensure that all necessary safety precautions have been taken. Connect all cables to the device only while the device is de-energized before turning on the power. Observe the safety instructions on the device itself (see safety symbols).

The metal chassis of the device is grounded. When installing the device in an electrical enclosure, it must be ensured that adequate clearance is provided, creepage distances to adjacent conductors are maintained, and that there is no risk of short circuits.

In the event of a malfunction or if servicing is required (e.g., damage to the chassis or power cable, ingress of fluids or foreign objects), the power supply may be cut off.

Please address any questions regarding your building's electrical, cable or antenna installations to the person or department responsible for that installation within your building.

AC Power Supply	DC Power Supply
<ul style="list-style-type: none"> <li>• The device is a Protection Class 1 device and may only be connected to a grounded outlet (TN system).</li> <li>• For safe operation, the installation must be protected by a fuse of a rating not exceeding 16 A and equipped with a residual-current circuit breaker in accordance with applicable national standards.</li> <li>• The disconnection of the appliance from the mains power supply must always be performed from the mains socket and not from the appliance itself.</li> <li>• Mains-powered appliances are equipped with a safety-tested mains cable designed for use in the country of operation and may only be connected to a grounded shockproof socket, otherwise electric shock may occur.</li> <li>• Make sure that the mains socket on the appliance or the mains socket of the house installation is readily accessible for the user so that the mains cable can be pulled out of the socket in an emergency.</li> </ul>	<ul style="list-style-type: none"> <li>• In accordance with IEC 62368-1, it must be possible to disconnect the appliance from the supply voltage from a point other than the appliance itself (e.g., from the primary circuit breaker).</li> <li>• The power supply plug may only be fitted or dismantled while the appliance is isolated from the power supply (e.g., disconnected at the primary circuit breaker).</li> <li>• Supply cables must be adequately secured and have an adequate wire gauge size.</li> </ul> <p style="text-align: center;"><i>Connection Cable Wire Gauge:</i>  <math>1\text{ mm}^2 - 2.5\text{ mm}^2</math>  17 AWG – 13 AWG</p> <ul style="list-style-type: none"> <li>• The power supply of the device must have a suitable disconnection mechanism such as a switch. This disconnection mechanism must be readily accessible in the vicinity of the appliance and marked accordingly as a cut-off mechanism for the appliance.</li> </ul>

## 2.5 Connection of Protective Earth Conductor/Grounding



ATTENTION!



In order to ensure that the device can be operated safely and to meet the requirements of IEC 62368-1, the device must be correctly connected to the protective earth conductor via the protective earth connection terminal.



If an external ground connection is provided on the housing, it must be connected to the grounding busbar (earthing busbar) for safety reasons before connecting the power supply. Like this, any possible leakage current on the housing is safely discharged to earth.

The screw, washer and toothed lock washer necessary for mounting the grounding cable are located at the grounding point of the housing. A grounding cable is not included in the contents of delivery.

**Note:**

Please use a grounding cable with cross-section  $\geq 1.5 \text{ mm}^2$ , as well as a suitable grounding clamp/lug. Always ensure that the connection is properly crimped!

## 2.6 Safety During Operation



### WARNING!

#### Avoiding Short-Circuits

Protect the device against all ingress of solid objects or liquids. Ingress presents a risk of electric shock or short-circuiting!

#### Ventilation Slots

Ensure that ventilation slots are clean and uncovered at all times. Blocked ventilation slots may cause heat to be trapped in the system, resulting in overheating. This may cause your device to malfunction or fail.

#### Appropriate Usage

The device is only deemed to be appropriately used and EMC limits (electromagnetic compatibility) are only deemed to be observed if the chassis cover is properly fitted (thus ensuring that the device is properly cooled, fire-safe, and shielded against electrical, magnetic and electromagnetic fields).



#### Switching the Device Off in the Event of a Malfunction or when Repairs are Required

It is not sufficient to simply switch off the device itself in order to disconnect the power supply. If the device is malfunctioning, or if repairs become necessary, the device must be isolated from all power supplies immediately.

#### **To do so, follow the procedure below:**

- Switch off the device from the unit itself.
- Pull out all power supply plugs.
- Inform the person or department responsible for your electrical installation.
- If your device is connected to an Uninterruptible Power Supply (UPS), it will remain operational even after pulling the UPS power cable from the mains socket. In this case, you will need to shut down your UPS in accordance with the user documentation of your UPS system.

## 2.7 Safety During Maintenance



### WARNING!

The device must never be opened. Repairs to the device may only be performed by the manufacturer or by authorized personnel. Improper repairs may expose the user to considerable safety risks (electric shock, fire hazard).

Opening the device or individual device components in an unauthorized fashion may also expose the user to considerable risks and invalidate your warranty. Meinberg Funkuhren accepts no liability for consequences arising from such unauthorized actions.



Danger from moving parts—do not touch moving parts.



Parts of the device may become very hot during operation. Do not touch these surfaces! If necessary, switch off the device before installing or removing any equipment, and allow it to cool down.

## 2.8 Handling of Batteries



### WARNING!

The lithium battery on the receiver modules has a life of at least ten years. Should it be necessary to replace it, please note the following:

Improper handling of the battery can lead to an explosion or to a leakage of flammable liquids or gases.

- Never short-circuit the battery.
- Never attempt to recharge the battery.
- Never throw the battery into a fire.
- The battery must only be exposed to the barometric pressure range specified by the battery manufacturer.
- The battery must only ever be replaced with one of the same type or a comparable type recommended by the manufacturer. The battery must only be replaced by the manufacturer or an authorized technician.
- Never dispose of the battery in a mechanical crusher or shredder, or in an open fire or furnace.

Please consult your local waste disposal regulations for information on how to dispose of hazardous waste.



### IMPORTANT!

The battery is used to power components such as the RAM and the reserve real-time backup clock for the reference clock.

If the battery voltage drops below 3 V DC, Meinberg recommends having the battery replaced. If the battery voltage drops below the specified minimum, the following behavior may be observed in the reference clock:

- The reference clock may have the wrong date or wrong date upon power-up
- The reference clock repeatedly starts in Cold Boot mode
- Some of the configurations saved for the reference clock may be lost



## 2.9 Cleaning and Care



### ATTENTION!

Never clean the device using liquids! Water ingress is a significant safety risk for the user (e.g., electric shock).

Liquids can cause irreparable damage to the electronics of the device! The ingress of liquids into the device chassis may cause short circuits in the electronic circuitry.

Only clean with a soft, dry cloth. Never use solvents or cleaners.

## 2.10 Prevention of ESD Damage



### ATTENTION!

An ESDS device (electrostatic discharge-sensitive device) is any device at risk of damage or malfunction due to electrostatic discharges (ESD) and thus requires special measures to prevent such damage or malfunction. Systems and modules with ESDS devices usually bear the following symbol:



### Symbol Indicating Devices with ESDS Components

The following measures will help to protect ESDS components from damage and malfunction.

#### When preparing to dismantle or install devices:

Ground your body (for example, by touching a grounded object) before touching sensitive devices.

Ensure that you wear a grounding strap on your wrist when handling such devices. These straps must in turn be attached to an uncoated, non-conductive metal part of the system.

Use only tools and devices that are free of static electricity.

#### When transporting devices:

Devices must only be touched or held by the edges. Never touch any pins or conductors on the device.

#### When dismantling or installing devices:

Avoid coming into contact with persons who are not grounded. Such contact may compromise your connection with the earth conductor and thus also compromise the device's protection from any static charges you may be carrying.

#### When storing devices:

Always store devices in ESD-proof ("antistatic") bags. These bags must not be damaged in any way. ESD-proof bags that are crumpled or have holes cannot provide effective protection against electrostatic discharges.

ESD-proof bags must have a sufficient electrical resistance and must not be made of conductive metals if the device has a lithium battery fitted on it.

## 2.11 Return of Electrical and Electronic Equipment



### ATTENTION!

**WEEE Directive on Waste Electrical and Electronic Equipment 2012/19/EU**  
(WEEE Waste Electrical and Electronic Equipment)

#### Waste Separation

Product Category: According to the device types listed in Annex I of the WEEE Directive, this product is classified as "IT and Telecommunications Equipment".



This product satisfies the labeling requirements of the WEEE Directive. The product symbol on the left indicates that this electronic product must not be disposed of in domestic waste.

#### Return and Collection Systems

When disposing of your old equipment, please use the national return or collection systems available to you. Alternatively, you may contact Meinberg, who will provide further assistance.

The return of electronic waste may not be accepted if the device is soiled or contaminated in such a way that it potentially presents a risk to human health or safety.

#### Return of Used Batteries

The EU Battery Directive prohibits the disposal of batteries marked with the WEEE trashcan symbol above in household waste.

## 3 Before you start

### 3.1 Text and Syntax Conventions

This chapter briefly describes the text and syntax conventions used in this manual.

**Web Interface:** example "Menu Network"

Submenu "Network → Network Interfaces"

Items in Submenu "Network → Network Interfaces → IPv4"

The menu navigation is logically separated by an right arrow (→).

**Directory names / Paths** Example: Lantime configuration file

The directory names and paths are displayed in italics.

#### Code and CLI Commands

```
- cmd/www-upload.htm
```

```
#Program code and CLI commands are displayed in a grey box with monospace font.
```

#### User passwords:

The following characters are currently allowed for user passwords and shared secret:

Allowed character set for both:

```
validchars[] = abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNopQRSTUVWXYZ  
0123456789  
=-_:#*?@/+![]
```

## 3.2 Required Tools

LANTIME IMS SERIES							
	LANTIME M1000	LANTIME M1000S	LANTIME M2000S	LANTIME M3000	LANTIME M3000S	LANTIME M4000	LANTIME M500
Mounting Rackears	TORX T20	TORX T20	TORX T20	TORX T20	TORX T20	TORX T20	X
Mounting DIN rail	X	X	X	X	X	X	Phillips PH1 x 80
Replacing IMS modules	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8	TORX T8
FAN Installation	TORX T8	TORX T8	TORX T8	TORX T8	X	TORX T8 Flat head Screwdriver	X

LANTIME SERIES							
	LANTIME M100	LANTIME M200	LANTIME M300	LANTIME M400	LANTIME M600	LANTIME M900	SyncFire
Mounting Rackears	X	TORX T20	TORX T20	X	TORX T20	TORX T20	X
Mounting DIN rail	Phillips PH1 x 80	X	X	Phillips PH1 x 80	X	X	X
Replacing Modules	X	X	X	X	X	TORX T8	TORX T10



Figure: Required tools from left to right - INBUS 2,5mm, Phillips PH1 x 80, Flat head Screwdriver, TORX T20, TORX T8

### 3.3 Abbreviation List

AFNOR	Association Francaise de Normalisation time codes	IP	range (PTP) Internet Protocol
AC	Alternating Current	IP 20	Protection Class 20
ASCII	American Standard Code for Information Interchange	IRIG	Inter-range instrumentation group time codes
BMC	Best Master Clock	LCD	Liquid Crystal Display
BNC	Bayonet Neil Councilman connector	LDAP(S)	Lightweight Directory Access Protocol
Bps	Bytes per second	LED	Light-Emitting Diode
bps	Bits per second	LINUX	Unix-like multi-user computer operating system
CAT5	Standard Network Cable	LIU	Line Interface Unit- an module for generation E1/T1 Signals, both MBit/s (framed) and Clock (unframed)
CET	Central European Time	LNE	Local Network Extension, additional Ethernet Ports
CLI	Command Line Interface	MAC	Media Access Control
DB9	Connector do type D-subminiature	MD5	Message-Digest cryptographic hash function
DC	Direct Current	MESZ	Middle European Summer Time
DCF77	Is a longwave time signal. DCF77 stands for D=Deutschland (Germany), C=long wave signal, F=Frankfurt, 77=frequency: 77.5 kHz.	MEZ	Middle European Time
DCFMARK	Single pulse with a programmable date and time	MIB	Management Information Base
DHCP	Dynamic Host Configuration Protocol	MRS	Multi Reference Source
DNS	Domain Name Server	MSF	Time signal transmitter in Anthorn, UK
DSCP	Differentiated Services Code Points	NIST	National Institute of Standards and Technology
DST	Daylight Saving Time	NMEA	Communication standard from National Marine Electronics Association
E1	European digital transmission signal at 2.048 MHz used in telecommunication networks.	NTP	Network Time Protocol
E2E	End-to-end	NTPD	NTP Daemon
ETH	Ethernet	OSV	Original Shipped Version (Firmware)
FTP	File Transfer Protocol	OUT	Output
FW	Firmware	P2P	Peer-to-Peer
GE / GbE	Gigabit Ethernet	PLC	Programmable Logic Controller
GLONASS	GLOBal NAVigation Satellite System from Russian Aerospace Defense Forces	PLL	Phase Locked Loop
GND	Ground (Connector)	PPM	Pulse per Minute
GNSS	Global Navigation Satellite System (GPS, GLONASS, Galileo, Beidou)	PRP	Parallel Redundancy Protocol
GOAL	GPS Optical Antenna Link	PPS	Pulse per Second
GPS	Global Positioning System (USA)	PPH	Pulse per Hour
GSM	Global System for Mobile Communications	PTB	Physical - Technical Institute Braunschweig / Germany
HMI	Human-Machine Interface	PTP	Precision Time Protocol
HP	Horizontal Pitch - is a unit measure the horizontal width of rack mounted electronic equipment	RAM	Random Access Memory
HPS	High Performance Synchronization PTP/NTP/SyncE GBit module	RF	Frequency of radio waves, from 3kHz to 300GHz
HSR	High-availability Seamless Redundancy	RG58	Standard coaxial cable used to connect an antenna and a receiver
HTTP	Hypertext Transfer Protocol	RJ45	Ethernet Connector with 8 conductors
HTTPS	Hypertext Transfer Protocol Secure	RMC	Remote Monitoring Control
IEC	International Electrotechnical Commission	RoHS	Restriction of Hazardous Substances
IED	Intelligent Electronic Devices	RPS	Redundant Power Supply
IEEE	Institute of Electric and Electronic Engineers	RS232/485	Serial port levels
IEEE 1588	Protocol for high-precision synchronization in nanosecond	RSC	Redundant Switch Control unit
		RX	Receiving Data
		SBC	Single Board Computer
		SDU	Signal Distribution Unit

---

SHA-1	Secure Hash Algorithm 1		AFNOR or IEEE1344 codes
SMB	Subminiature coaxial connector	T1	North American telecommunication signal at 1.544 MHz frequency
SNMP	Simple Network Management Protocol		Transmission Control Protocol
SNTP	Simple Network Time Protocol	TCP	Transistor-to-Transistor Logic
SMTP	Simple Mail Transfer Protocol	TTL	Data Transmission
SPS	Standard Positioning System	TX	Unit - is a unit measure the vertical height of rack mounted electronic equipment.
SSH	Secure SHell network protocol	U	User Datagram Protocol
SSU	Synchronization Supply Unit, specific clock used in telecommunication networks	UDP	Universal Mobile Telecommunications System
SSM	Sync Status Messages, clock quality parameters in telecommunication networks.	UMTS	Multitasking, multi-user computer operating system
ST	Bayonet-lock connector	UNIX	Universal Time Coordinate
Stratum	Value defines the NTP hierarchy	UTC	Virtual Local Area Network
SYSLOG	Standard for computer data logging	VLAN	Time signal radio station Fort Collins, Colorado (USA)
TACACS	Terminal Access Controller Access Control System	WWVB	
TCG	Time Code Generator		
TCR	Time Code Receiver for IRIG A/B,		

## 4 Introduction

A LANTIME is a multi-purpose time and frequency synchronization solution with a flexible approach to support a large number of synchronization requirements in different applications and network environments. The system combines a powerful CPU with dedicated hardware like reference clocks or I/O modules, creating a powerful network appliance that supports almost all commonly used time and frequency synchronization protocols and signals.

The basic installation of a LANTIME Server is a very easy and straightforward process. After installing the hardware, the network address, the netmask and the default gateway have to be configured to be able to access the web GUI. If everything is set up correctly, as soon as the device is reachable over the network, it can start serving time via NTP and/or PTP.

In addition to the time sync protocols NTP and PTP, the LANTIME system supports a number of additional network protocols primarily used for remote management of the system: HTTP(S), FTP, SSH and Telnet. Remote configuration, status checks and other maintenance procedures like firmware updates or configuration backups can be controlled from any WEB browser. For security reasons, every protocol can be enabled or disabled for each configured IP address, allowing to reduce potential attack vectors and effectively control access to the device.

Status changes, alarms or other important events are logged in local log files and additionally can be forwarded to external SYSLOG servers. A number of notification protocols are supported to integrate the LANTIME system into already existing IT monitoring solutions. For example, SNMP traps or automatically generated e-mails are two potential options for notifying IT administrators about important events.

Installing multiple LANTIME devices in one network is a way to create redundancy for important network time synchronization services.

## 4.1 Network Configuration Concept

The LANTIME OS6 Firmware system supports a wide range of different network environments due to its flexible and powerful network configuration concept. A separation between physical and logical ("virtual") interface configurations covers almost all possible requirements for datacenters, telecommunication backhaul networks and industrial network environments.

Each LANTIME server has at least one physical ethernet interface which is provided by the CPU module (lan0). Additional network interfaces can be provided by network expansion cards (LNE or TSU cards) or on backplanes (depending on model). These additional physical interfaces can be used to provide synchronization services to multiple physical network segments, to separate management and synchronization networks or to combine multiple ethernet interfaces to form redundant connections ("bonding"). The 6th generation of LANTIME OS6 Firmware firmware (LTOS7) can manage up to 99 physical network interfaces as a theoretical maximum.

Configuration of IPv4 and IPv6 addresses is done based on logical interface configurations. Each logical interface is assigned to one physical ethernet port and can be configured to use one IEEE 802.1q VLAN ID. The current firmware version supports up to 99 logical interfaces per server and all of those could be theoretically assigned to a single physical port.

The network ports of TSU modules (for PTP and Hardware-NTP) are not providing this logical interface functionality and are limited, at least in the current firmware version, to one IPv4/IPv6 address and one VLAN ID per physical interface. Redundancy and connectivity to multiple network segments and VLANs can be achieved by adding multiple TSU cards in a system.

For each logical interface the available network services for synchronization (NTP, TIME, ..) and management (HTTP, HTTPS, SSH, SNMP, TELNET, ...) can be enabled/disabled individually. This allows to only provide synchronization on one IP address and remote access the unit for management tasks over a different IP address.

## 4.2 Additional Features

- external NTP timeserver
- free configuration of NTP: thereby MD5 authentication and access control via address & mask restriction
- extended menu guidance for configuration and monitoring via Telnet, SSH or serial terminal interface
- optional up to 3 RJ45/10/100 MBit Ethernet interfaces
- extended HTTP statistic support with long-term graphic and access statistic to NTP
- alarm messages can be displayed on external large display VP100/20/NET
- USB memory stick slot for extended functionality: software update, transfer of secure certificates, log files and configurations, keypad locking

## 4.3 User Interface

- Terminal connection via serial interface, status LED
- Web browser interface with graphical statistic of the one-day cycle offsets
- Telnet or Secure Shell Login for password protected operation of the Linux operating system
- FTP access for updating the operating system and downloading log files
- Simple Network Management Protocol for automatically SNMP-Traps in case of alarm
- SYSLOG messages can be passed to different computers
- Configurable e-mail notification
- Simulation of a synchronous radio clock in order to operate without antenna



## 4.4 Input and Output Options

- Additional Ethernet RJ45 connectors available (eight in 3U housing, four in 1U housing and eight additional connectors in HS - XL railmount housing)
- Frequency and pulse outputs via BNC connectors (e.g. 10 MHz, 2.048 MHz, PPS)
- Higher free running accuracy with optional oscillators (OCXO)
- IRIG-B outputs
- ANZ14NET or VP100/20/NET as display connected via network

### Additional Ethernet RJ45 connectors available:

System Type	CPU-C05F1	CPU-C15G2 (Q7)
LANTIME M4000	up to 25 (+24) Network Ports	up to 26 (+24) Network Ports
LANTIME M3000	up to 25 (+24) Network Ports	up to 26 (+24) Network Ports
LANTIME M1000	up to 17 (+16) Network Ports	up to 18 (+16) Network Ports
LANTIME M500	up to 9 (+8) Network Ports	up to 10 (+8) Network Ports
LANTIME M900	up to 9 (+8) Network Ports	
LANTIME M600	up to 5 (+1) Network Ports	
LANTIME M400	up to 5 (+4) Network Ports	
LANTIME M300	up to 6 (+4) Network Ports	

## 4.5 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.

### 4.5.1 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>

## 4.6 Option: Precision Time Protocol (PTP) / IEEE 1588

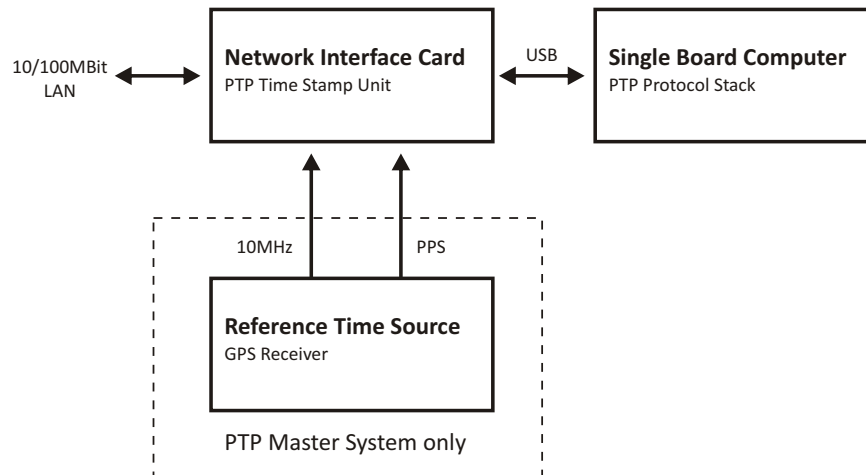
Precision Time Protocol (PTP or IEEE 1588) is a time synchronization protocol that offers sub-microsecond accuracy over a standard Ethernet connection. This accuracy can be achieved by adding a hardware timestamping unit to the network ports that are used for PTP time synchronization. The timestamping unit captures the exact time when a PTP synchronization packet is sent or received. These timestamps are then taken into account to compensate for transfer delays introduced by the Ethernet network.

In PTP networks there is only one recognized active source of time, referred to as the Grandmaster Clock. If two or more Grandmaster Clocks exist in a single network, an algorithm defined in the PTP standard is used to determine which one is the „best“ source of time. This „Best Master Clock“ algorithm must be implemented on every PTP/IEEE1588 compliant system to insure that all clients („Slave Clocks“) will select the same Grandmaster. The remaining deselected Grandmaster Clocks will „step back“ and enter a passive mode, meaning that they do not send synchronization packets as long as that is being done by the designated Grandmaster.

The existing network infrastructure components play a big role in a PTP network and directly influence the level of accuracy that can be achieved by the clients. Asymmetric network connections degrade the accuracy, therefore classic layer 2 and 3 Ethernet switches with their “store and forward” technology are not suitable for PTP networks and should be avoided. With activating the HQ-Filter (see chapter HQ-Filter) the Jitter can be eliminated. Simple Ethernet hubs with fixed pass-through times are not a problem. In large networks, special switches with built-in PTP functionality help to maintain high accuracy even over several subnets and longer distances. These components act as "Boundary Clocks" (BC) or "Transparent Clocks" (TC). They compensate their internal packet processing times by using timestamping units on each port. When acting as a Boundary Clock, they synchronize to the Grandmaster clock, and in turn act as a Master to the other subnets they are connected to. When acting as a Transparent Clock, then the "residence time" of the Masters' Sync-Packet is measured and added to the packet as a correction value. Internally the PTP timescale TAI (see chapter Timescale in Global Parameters).

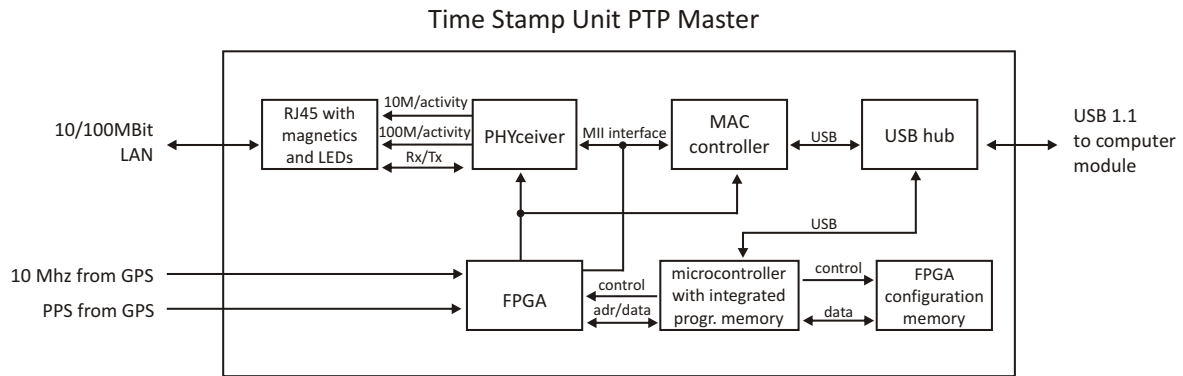
### 4.6.1 General Information

The internal PTP card acts as a network interface card (10/100MBit) with an integrated hardware time stamp unit to obtain time stamps in PTP compatible networks. In conjunction with a single board computer running the PTP protocol stack and a reference time source (PTP master only) the module is capable of building a PTP Master or Slave system:



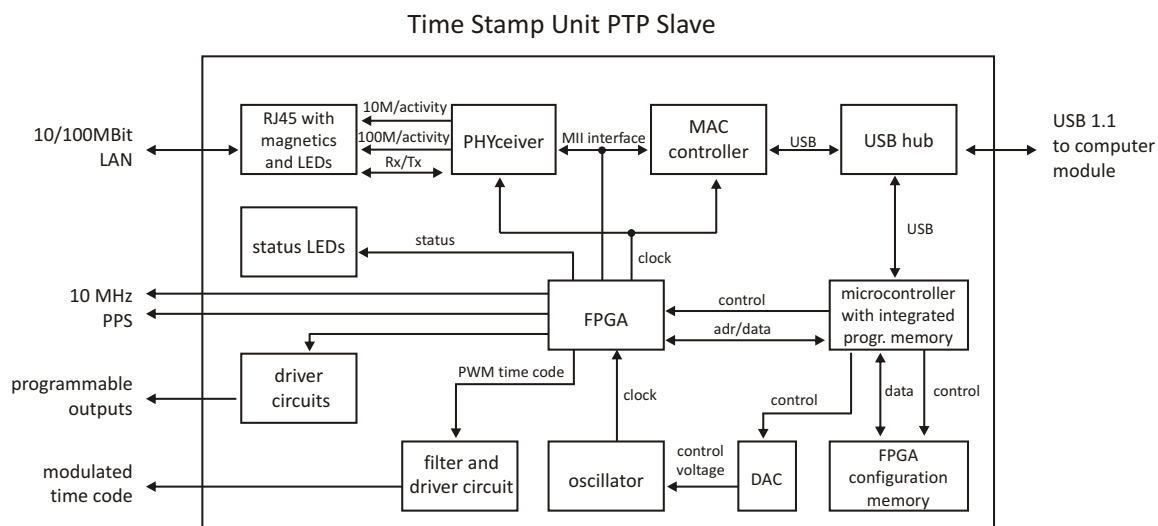
The Time Stamp Unit, integrated in an FPGA (Field Programmable Gate Array, a programmable logic device), checks the data traffic on the MII-interface between the PHY receiver (physical connection to the network) and the Ethernet controller (MAC) on the PTP module. If a valid PTP packet is detected, the time stamp unit takes a time stamp of that packet which is read by a single board computer (SBC) running the PTP software. The configuration and status traffic between the PTP board and main SBC is done over a USB connection.

## 4.6.2 Functionality in Master Systems



After power up, the module accepts the absolute time information (PTP seconds) of a reference time source (e.g. GPS reference clock) only once, and the PTP nanoseconds are set to zero. If the oscillator frequency of the reference time source has reached its nominal value, the nanoseconds are reset again. This procedure leads to a maximum deviation of 20 nsec of the pulse per second (1PPS) of the PTP Master compared to the 1PPS of the GPS reference clock. The reference clock of the PTP board's time stamp unit (50 MHz) is derived from the GPS disciplined oscillator of the reference time source using a PLL (Phase Locked Loop) of the FPGA. The achieves a direct coupling of the time stamp unit to the GPS system.

### 4.6.3 Functionality in Slave Systems



After decoding valid time information from a PTP Master, the system sets its own PTP seconds and nanoseconds accordingly. The PTP offset calculated by the PTP driver software of the single board computer is used to adjust the master oscillator of the TSU-USB. This allows the PTP Slave to generate very high accuracy output signals (10 MHz/1PPS/IRIG).

## 4.6.4 PTPv2 IEEE 1588-2008 Configuration Guide

Setting up all devices in a PTP synchronization infrastructure is one of the most important parts in a network time synchronization project. The settings of the involved Grandmaster clocks as the source of time and the end devices ("Slaves") have to match in order to allow them to synchronize and avoid problems later, when the PTP infrastructure is deployed to production environments. In addition to that, the use of PTP aware network infrastructure components, namely network switches, introduces another set of parameters that have to be harmonized with the masters and slaves in a PTP setup.

It is therefore very important to start with making decisions how the to-be-installed PTP synchronization solution should operate, e.g. should the communication between the devices be based on multicast or unicast network traffic or how often should the masters send SYNC messages to the slaves.

This chapter lists the most important options and their implications on a synchronization environment in general. A detailed explanation of the configuration settings within the LANTIME configuration interfaces can be found later within this documentation.

### 4.6.4.1 General Options

The following general mode options have to be decided before deploying the infrastructure:

- 1) Layer 2 (Ethernet) or Layer 3 (UDP/IPv4) connections
- 2) Multicast or Unicast
- 3) Two-Step or One-Step Operation
- 4) End-to-End or Peer-to-Peer Delay Mechanism

The above options need to be defined for the whole setup, if devices do not stick to the same settings, they will not be able to establish a working synchronization link.

### 4.6.4.2 Network Layer 2 or Layer 3

PTP/IEEE 1588-2008 offers a number of so-called mappings on different network communication layers. For Meinberg products you can choose between running PTP over IEEE 802.3 Ethernet connections (network Layer 2) or UDP/IPv4 connections (Layer 3).

Layer 3 is the recommended mode, because it works in most environments. For Layer 2 mode the network needs to be able to provide Ethernet connections between master and slave devices, which is often not the case when your network is divided into different network segments and you have no layer 2 routing capabilities in your network infrastructure.

The only benefit of using Layer 2 mode would be a reduced traffic load, because the transmitted network frames do not need to include the IP and UDP header, saving 28 bytes per PTP packet/frame. Due to the fact that PTP is a low traffic protocol (when compared to other protocols), the reduced bandwidth consumption only plays a role when low-bandwidth network links (e.g. 2Mbit/s) have to be used or in pay-per-traffic scenarios, for example over leased-line connections.

#### 4.6.4.3 Multicast or Unicast

The initial version of PTP (IEEE 1588-2002 also known as PTPv1) was a multicast-only protocol. Multicast mode has the great advantage that the master clock needs to send only one SYNC packet to a Multicast address and it is received by all slave devices that listen to that multicast address.

In version 2 of the protocol (IEEE 1588-2008) the unicast mode was introduced in addition to the multicast mode. In unicast mode, the master has to send one packet each to every slave device, requiring much more CPU performance on the master and producing orders of magnitudes more traffic.

On the other hand, some switches might block multicast traffic, so that in certain environments, Unicast mode has to be used.

#### 4.6.4.4 Two-Step or One-Step

The PTP protocol requires the master to periodically send SYNC messages to the slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by either sending this time stamp in a separate packet (a so-called FOLLOW-UP message) or by directly manipulating the outgoing SYNC message, writing the hardware time stamp directly into the packet just before it leaves the network port.



#### 4.6.4.5 End-To-End (E2E) or Peer-To-Peer (P2P) Delay Measurements

In addition to receiving the SYNC/FOLLOWUP messages a PTP slave device needs to be able to measure the network delay, i.e. the time it took the SYNC message to traverse the network path between the master and the slave. This delay is required to correct the received time information accordingly and it is measured by the slave in a configured interval (more about the message intervals later). A delay measurement is performed by sending a so-called DELAY\_REQUEST to the master which timestamps it and returns the timestamp in a DELAY\_RESPONSE message.

IEEE 1588-2008 offers two different mechanisms for performing the delay measurements. A slave can either measure the delay all the way to the master, this is called End-To-End (or E2E in short) or to its direct network neighbors (which would in almost all cases be a switch – or two in a redundant setup), using the Peer-To-Peer delay measurement mechanism (P2P). The delay measurements of all links between the master and the slave are then added and accumulated while a SYNC packet is traversing the network.

The advantage of this method is that it can dramatically reduce the degradation of accuracy after topology changes. For example: in a redundant network ring topology the network delay will be affected when the ring breaks open and network traffic needs to be redirected and flows into the other direction. A PTP slave in a sync infrastructure using E2E would in this case apply the wrong delay correction calculations until it performs the next delay measurement (and finds out that the network path delay has changed). The same scenario in a P2P setup would see much less time error, because the delay of all changed network links were already available.

The drawback: the P2P approach requires that all involved PTP devices and all switches support this mechanism. A switch/hub without P2P support would in the best case simply pass the so-called PDELAY messages through and as a result degrade the accuracy of the delay measurements. In the worst case it would block/drop the PDELAY messages completely, which effectively would result in no delay measurements at all.

So, E2E is the only available choice if you are running PTP traffic through non-PTP-aware switches. It is a reasonable choice if you are not using redundant network topologies or can accept that the delay measurements are wrong for a certain amount of time.

#### 4.6.4.6 Message Rate Settings

The decision between the different general mode options is mainly dictated on the network environment in which the PTP infrastructure is installed. In addition to the mode selection, a number of intervals for certain types of PTP network messages needs to be defined. In most cases, the default values as defined in the standard are a safe bet, but there are applications and scenarios where a custom message rate is required.

A possible example is a situation where the PTP infrastructure is integrated within an environment with high network load. In this case, the PTP packets can be affected by the effect of packet delay variation (PDV). An increase of the PTP message rate(s) can avoid synchronization problems due to packet queuing within non-PTP compliant switches which might cause false measurements. At higher rates, these false measurements can be detected and corrected faster as compared to lower rates at the cost of increased traffic.

The message rates for the following message types can be changed:

- 1) ANNOUNCE messages
- 2) SYNC/FOLLOWUP messages
- 3) (P)DELAY\_REQUEST messages

#### 4.6.4.7 ANNOUNCE Messages

These PTP messages are used to inform the PTP network participants about existing and available master clock devices. They include a number of values that indicate the potential synchronization accuracy.

The procedure used to decide which of the available devices (that could become masters) is selected is called the "best master clock algorithm" (BMCA). The values that are used in this BMCA are read from the ANNOUNCE messages that potential masters send out periodically.

The rate at which these messages are sent out are directly affecting the time that is required by a slave device to select a master and to switch to a different master in case the selected one fails.

Multiple devices can simultaneously transmit ANNOUNCE messages during periods in which no master has been selected (yet). This happens for example when a PTP network is powered up, i.e. all devices are starting to work at the same time. In this case all devices that consider themselves (based on their configuration and status) being capable of providing synchronization to all the other PTP devices will start to send out ANNOUNCE messages. They will receive the other candidates' ANNOUNCE messages as well and perform the BMCA. If they determine that another candidate is more suitable to become the master clock, they stop sending ANNOUNCE messages and either become slave devices or go into "PASSIVE" mode, waiting for the selected master to stop sending ANNOUNCE messages. This is determined to be the case when no ANNOUNCE message is received within 3 ANNOUNCE message intervals.

As an example, if the ANNOUNCE interval has been configured to be 2 seconds (one message every 2 seconds, the default value), the master is considered to have failed when no message has been received for 6 seconds.

In order to choose a master (a backup master clock or the primary one during initialization) the devices require to receive at least two consecutive ANNOUNCE messages. Continuing our example, it would take the 6 seconds to determine that the current master has failed and another 4 seconds to select the new one. That means an ANNOUNCE interval of 2 seconds translates into at least 10 seconds of "switching time" and 4 seconds of "initial master clock selection time". So, choosing a shorter ANNOUNCE message interval will allow a faster switching to a backup master clock, but it can lead to false positives when the chosen interval is too short for the network environment.

#### 4.6.4.8 SYNC/FOLLOWUP Messages

The selected master clock sends out SYNC (and, in Two-Step environments, the corresponding FOLLOWUP) messages in a configured interval. This interval (default value is one SYNC/FOLLOWUP packet every second) determines how often the slave devices receive synchronization data that allows them to adjust their internal clocks in order to follow the master clock time. Between receiving two SYNC messages, a slave clock runs free with the stability determined by its own internal time base, for example a crystal oscillator. One important factor for deciding on the SYNC interval is the stability of this oscillator. A very good oscillator requires a lower SYNC message rate than a cheaper, low-accuracy model. On the other hand you directly affect the required network bandwidth by changing the SYNC interval.

For Meinberg slave devices, the default one-SYNC-every-second setting is more than enough to achieve the highest possible synchronization accuracy.

#### 4.6.4.9 (P)DELAY\_REQUEST Messages

As explained in the General Mode Options chapter (see the “End-To-End or Peer-to-Peer” section), the delay measurements are an important factor for achieving the required accuracy. Especially in E2E mode, the network path delay measurements play a crucial part in the synchronization process. Per default, the slaves will perform delay measurements every 8 seconds, resulting in sending and receiving one packet. This can be increased in case the network path delay variation in the network is relatively large (i.e. the time it takes for the SYNC message to reach the slave varies a lot) or the slave devices have to tightly follow the master and adjust their time base (oscillator) very often due to its instability.

Meinberg slave devices will limit the effect of an outdated path delay measurement by using filters and optimized PLL algorithms. This avoids that a clock “jumps around” and basically monitors the time difference to the master clock carefully for a certain amount of time before adjusting its own clock. With a low cost time base this is not possible, because the instability (i.e. temperature-dependent drift and overall short term stability/aging effects) and therefore these slaves would require to perform as many delay measurements and receive as many SYNC/FOLLOWUP messages as possible.

For P2P mode the delay request interval is not as critical, simply because the delay variation on a single-hop link (i.e. from your slave device to its switch) is very stable and does not change dramatically in typical environments.

Current firmware versions of Meinberg Grandmaster clocks (V5.32a and older) do not offer changing the Delay message rate in Multicast mode, it is fixed to one delay request every 8 seconds. Since this is actually a value that is transmitted in the DELAY\_RESPONSE message as a maximum value, the slave devices are not allowed to perform delay measurements more often.

#### 4.6.4.10 HQ Filter

If you use non PTP aware switches in a network where PTP should be used then the timing accuracy of the offset depends on the characteristic of the switches. Non PTP switches will cause time jitters (due to non deterministic delays in each path direction) in PTP measurement. In this section, the term "jitter" is used to describe the maximum deviation of the measured offsets around a certain mean value. This time jitter of standard non-PTP compliant switches can be in the range of 100 ns up to 10000 ns. When using routers this jitter can be even higher. To reduce this time jitter the HQ filter can be activated to achieve a better PTP slave synchronization quality. With Layer2 switches the accuracy can be achieved in the range of submicro seconds. Also Jitter caused by high network load and faulty measurements will be eliminated

##### Functionality

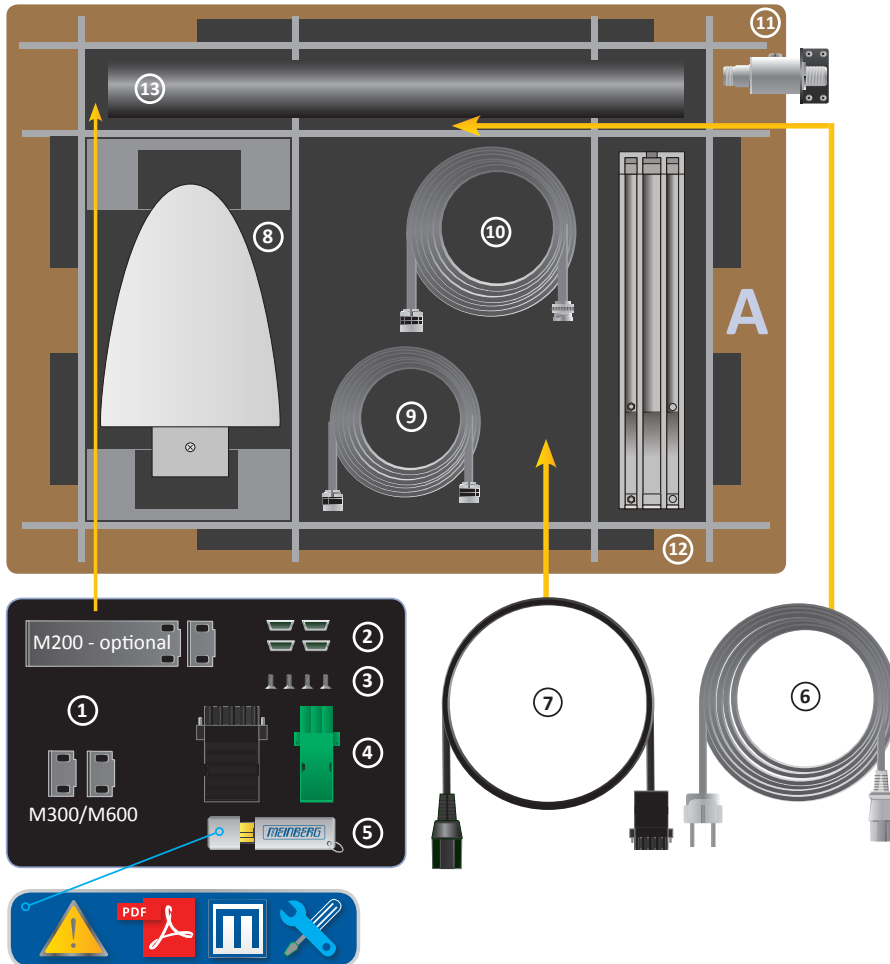
After activating the HQ-Filter some PTP measurements will be done first without controlling the timing of the PTP slave. This phase will be indicated by an extra hint "init" in the current status of the PTP slave. During this phase the maximum jitter of the PTP offset, the path delay and the current drift of the internal oscillator will be calculated by statistical methods. The only filter parameter which can be set by the user is the **estimated accuracy** which will set the maximum expected range of the incoming time jitter. All input values that are out of this range will be dropped. The maximum jitter of the input will be updated continuously during normal operation. By default **estimated accuracy** will be set to 1s to determine the maximum jitter automatically.

##### PDSC

PDSC means "Path Delay Step Compensation". The PDSC feature tries to eliminate jumps of the PTP path delay, so that there will be no effect on the timing accuracy. Such a jump of the PTP path delay (which should be usually constant) will be caused by changing the topology of the PTP network which could happen in SDH networks for example. The change of the PTP path delay is only detected, if the step is larger than the measured time jitter. This feature is an extension of the HQ-Filter and therefore the HQ-Filter has to be activated.

## 5 Unboxing

After unpacking the LANTIME time server, please check the contents for completeness – regarding to the included packing list.

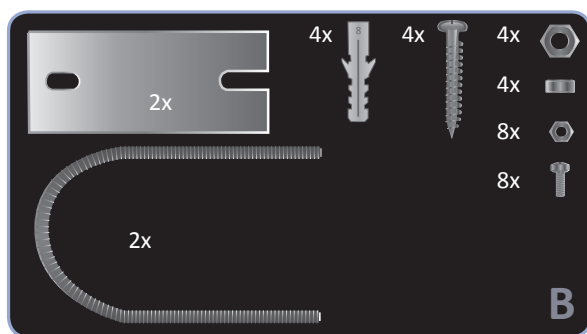


### A LANTIME Package Contents

1. Assembly brackets for 19 Inch rack mounting (optional for LANTIME M200)
2. Protection spacer (M200 / M300 / M600)
3. Screws for brackets (M200 / M300 / M600)
4. 3-pin DFK connector or 5-pin DFK connector (additional connector in case of AC/DC or DC power supply)
5. USB stick with software and documentation
6. Power cord (only in case of AC power supply)
7. Option: power cable with 5-pin connector

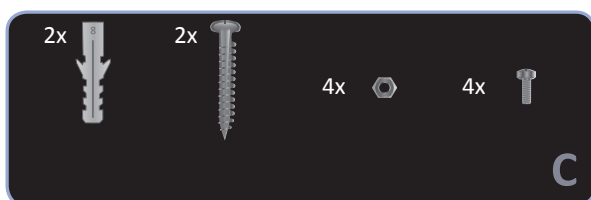
#### Only with delivered Antenna

8. Antenna
9. Optional: cable for surge voltage protector
10. Antenna cable
11. Optional: surge voltage protector with bracket
12. Brackets for pole or wall mounting
13. Pole for antenna mounting (GPS Antenna)



**B** Mounting Kit for GPS Antenna  
(wall or pole mounting)

---



**C** Mounting Kit for Long Wave Antenna  
(wall mounting)

---

**Note:** Please read the safety instructions and the manual carefully to familiarize yourself with the safe and proper handling of electronic devices. The product documentation can be found on the USB Flash Memory.

## 6 LANTIME Installation

- Connecting the LANTIME
- Entering the IP Address
- Connecting the Antenna
- Configuration via the Web Interface

### Connecting the LANTIME

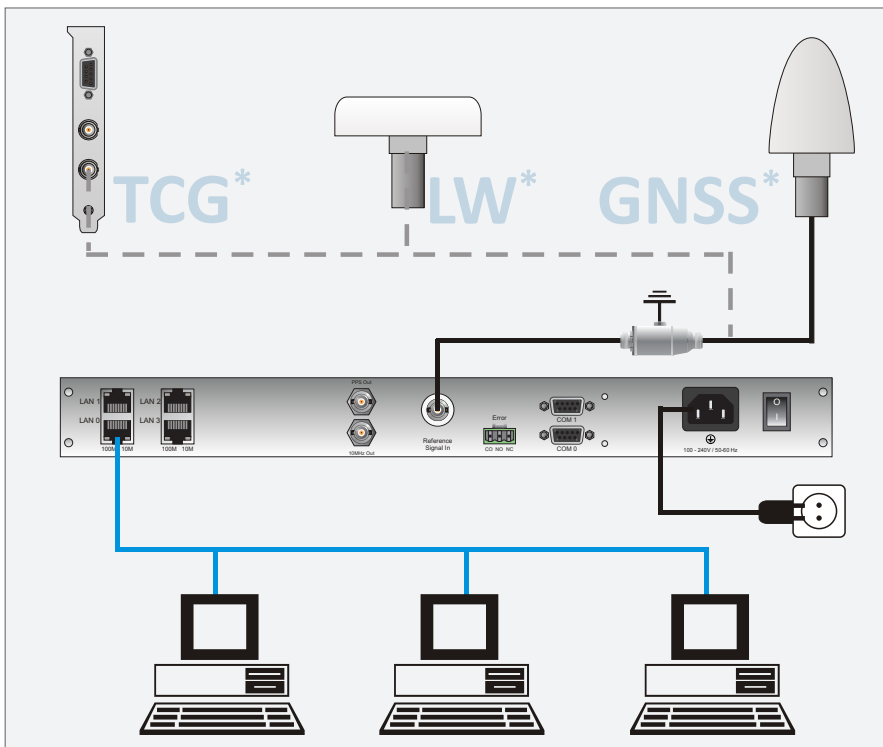


Figure: LANTIME Connection diagram \* TCG = Time Code Generator, LW = Long Wave Receiver, GNSS = Global Navigation Satellite System

Make sure that the power switch (if available) is in the "0" position (off), and plug the power cord into the power socket of your LANTIME. Then connect the device to your computer network using a suitable network cable. After switching on power, the following message is displayed:

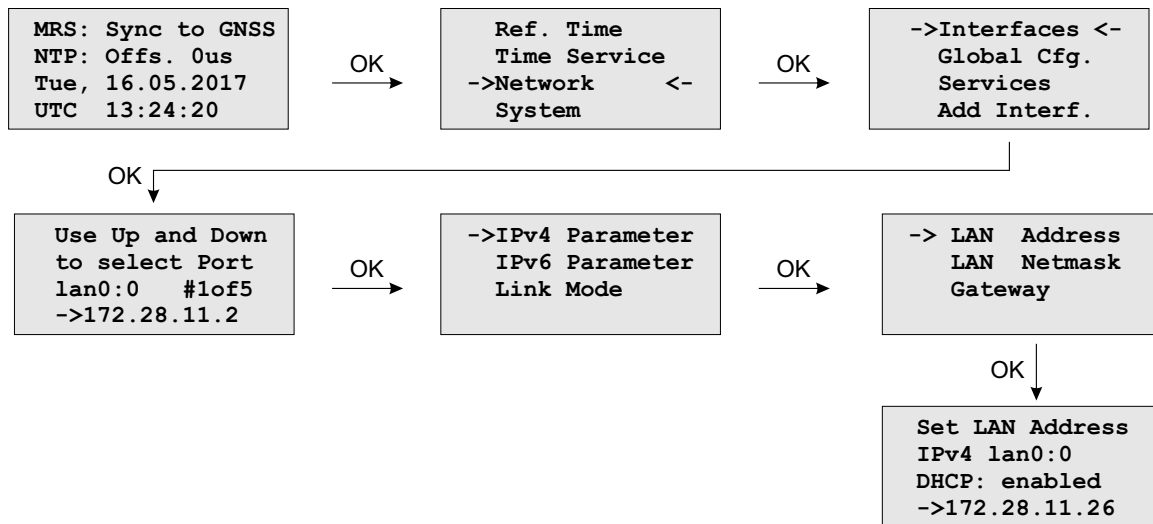
```

MEINBERG LANTIME
is booting ...
please wait ...
.....
    
```

After running a number of power-on self tests, the time server is in operation mode and the main screen appears.

### Entering the IP Address

Initial installation requires setting up an IP address, netmask and (in most network environments) a default gateway. To get an overview of the current configuration, press F2. Press F2 again to enter the Network SETUP screen:



Navigate to "Interfaces" using the arrow keys and press OK to change to the configuration menu of the connected network interface. You can select the network port with the "Down" and "Up" arrow keys (↓ | ↑).

### Entering the IP Address manually (not using DHCP)

Deactivate DHCP and set up a valid IP address, netmask and (if required) a default gateway. This can be done by selecting a field with the arrow keys. Then press OK to switch to edit mode.

The cursor can be moved using the ← | → arrow keys, the value underneath the cursor can be modified with ↓ | ↑. Confirm your changed values with OK and F2.

### Connecting the Antenna

Connect the antenna cable with the antenna socket of your LANTIME. In case of a short-circuit, the following message appears in the display:

```

ANTENNA
SHORT-CIRCUIT
DISCONNECT POWER
!!!
  
```

In such a case, switch off the device and check the antenna cable. Instructions for installing the antenna are included in the corresponding chapter „Mounting the Antenna“ of the manual which is available in the „Manual“ folder of the USB flash drive.



### Configuration via the Web Interface

The system configuration can now be changed via the network using a WEB browser or a Telnet / SSH client.

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

1. Accessing the Web Interface  
Type in the IP of your LANTIME into the address field `http://xxx.xxx.xxx.xxx`
2. LOGIN  
user: root  
password: timeserver

## 7 Security User Guide / Security Advisories

This Chapter describes the configuration of a LANTIME series operating system (LTOS) in terms of security features. It is divided in the following sections: general overview, securing the management, securing the time services and additional information about event log delivery. Finally, some advisories for the update process of a LANTIME are given.

The general knowledge about public key infrastructures, RSA, symmetric keys and the protocols SSL, SSH, NTP and SNMP is assumed.

### 7.1 General Informations

Before starting with the configuration, take a look at [Figure 7.1](#) to identify the possible services that can be configured to be secure.

In general, a secure management of the LANTIME is possible with SSH, HTTP and SNMP. If the configuration via SNMP is desired, the usage of version 3 is the only way to get a secure connection to manage the system. It is a good practice to deactivate all services that are not in use, to minimize the attack surface. So if possible, only enable one of the services (SNMP has not the full configuration support, but you can activate the other services over SNMP)!

The delivery of secured time information is only available for NTP. Please note, that the NTP protocol only supports integrity and authenticity but no confidentiality. On the other hand, PTP can not be configured to be secure. The next protocol standard of PTP will also provide some security features, but at the moment you still have to fall back to NTP for secure time delivery.

Another important advisory is to use the newest browsers and service clients to support the selection of the best security algorithms for server and client communication. Also the existence of known vulnerabilities can be reduced by a fast patch conduct.

The TSU cards of Meinberg take a special case you have to deal with. Their opportunity to get connected via ssh over the network and their possibility to internally connect to the Meinberg CPU card leads to a back door, if not configured well. The [Figure 7.2](#) shows this constellation. If SSH is not desired on the TSU, just deactivate the SSH client on the PTP webpage like in [Figure 7.3](#). If SSH is desired, change the standard SSH public and private key on both sides (CPU and TSU). This can only be done by hand with a SSH connection. The keys are under `"/config/ssh/usb0_rsa_key"` on CPU and `"/root/.ssh/authorized_keys"` on TSU. When you have changed the keys, be aware that new additional TSU cards can not be accessed without credentials.

Services	Confi.	Integ.	Avail.	Auth.	Account.
https	x	x	o	x	(x)
ssh	x	x	o	x	(x)
ntp	-	x	o	x	(x)

Table 7.1: Table of security targets

Table 7.1 shows the security goals of the protocols in short. The accountability is given through a detailed syslog of the actions performed by every user or process. It is not guaranteed that entries are not manipulated by admins and for that, the system can not prove the non-repudiation. The most, possible availability of the services is realized through current updates and IP banning. For more protection, implement web application firewalls and traditional firewalls in the network, that are able to identify and prevent DOS/DDOS attacks.

## 7.2 Securing Management

The most secure way to configure a LANTIME is to connect the client directly to the LANTIME, until only secure channels are established. This guide uses the web interface over ssl as example. After connecting a reference clock and the following start procedure of a LANTIME, an IP address can be configured via the front panel (see chapter "LTOS Management and Monitoring -> Via Front Panel Display"). Now it is possible to connect to the web interface. Use the initial credentials to login.

After you connected successfully, the first thing to do is to check, if it exists a new firmware version (see section 7.6 for update instructions). After the update is performed, generate or inject a ssl certificate. This example uses a new one. Figure 7.4 shows the button to start the generation. On the next step you have to enter the informations needed for the certificate (see also chapter "LTOS Management and Monitoring -> Via Web Gui -> Security"). Figure 7.5 shows the form. As key length, use 2048 or higher. Shorter durations of the period of validity are better than longer. In this example we select three years as a good trade of short duration and an acceptable management cost. You can view the generated certificate with the show ssl certificate button. Use it to compare it with the certificate provided by the browser on your next https connection to the LANTIME. Both should be identical! The import process is illustrated in Figure 7.7. The numbers in the figure describe the sequence of actions to perform. Number four represents the comparison with the previously downloaded certificate of the LANTIME. If both certificates are identical, you can go ahead with step five to confirm the confidence of the LANTIME certificate. Modern browser configurations will show you that the connection is not safe when you use a self signed certificate. Because of this behavior, we recommend the implementation of a public key infrastructure to avoid the warning. For this purpose, you can generate a certificate request, download it, sign it and upload the signed certificate again via the web front end on Figure 7.4.

If the connection over https is possible, you can deactivate all other unused services like on Figure 7.8. Additionally, in this example only one network interface provides the https web interface. Thus, scenarios like a dedicated configuration network are possible, too.

For the next step, one other super user than root is needed. Go to section 7.3 to create one. After creation of the new super user, log in with its credentials and disable the root login under Security->Login/Access->Disable \_Root\_Login. Deactivate the front panel, USB port and local console under Security->Front\_Panel if desired. In addition, you can set the remote access control to white listed IP addresses that are allowed to connect to the web interface (Hint: The Remote Access Control does not take effect for SSH connections). Figure 7.9 shows the menus. The timeout for web sessions is configured on the system tab under general setting which is displayed in Figure 7.10. Shorter durations minimize the security risk.

From now on, the LANTIME is well configured to be managed secure. Keep in mind to check if the IP configuration and remote access control work in the productive network environment.

Optionally, you can configure SNMP to manage the LANTIME. The security options can be found under Security->SNMP. Figure 7.11 shows the menu. To establish a secure connection via SNMP you have to use version 3 and the authPriv mode. The additional parameters of version 3 are the user name (security name), the access rights, the authentication and privacy protocol/algorithms. Use SHA and AES as algorithms. As usual, longer passwords are preferred. Start the SNMP service on Network->Network\_Services tab afterwards.

## 7.3 User Management/Administration

This section describes the administration of user and authentication management. Therefore, it is divided in LANTIME origin and external user authentication. The LANTIME OS supports the two external authentication servers, Radius and TACACS+. You can also see "LTOS Management and Monitoring ->Via Web GUI -> System -> External Authentication Options" for further information.

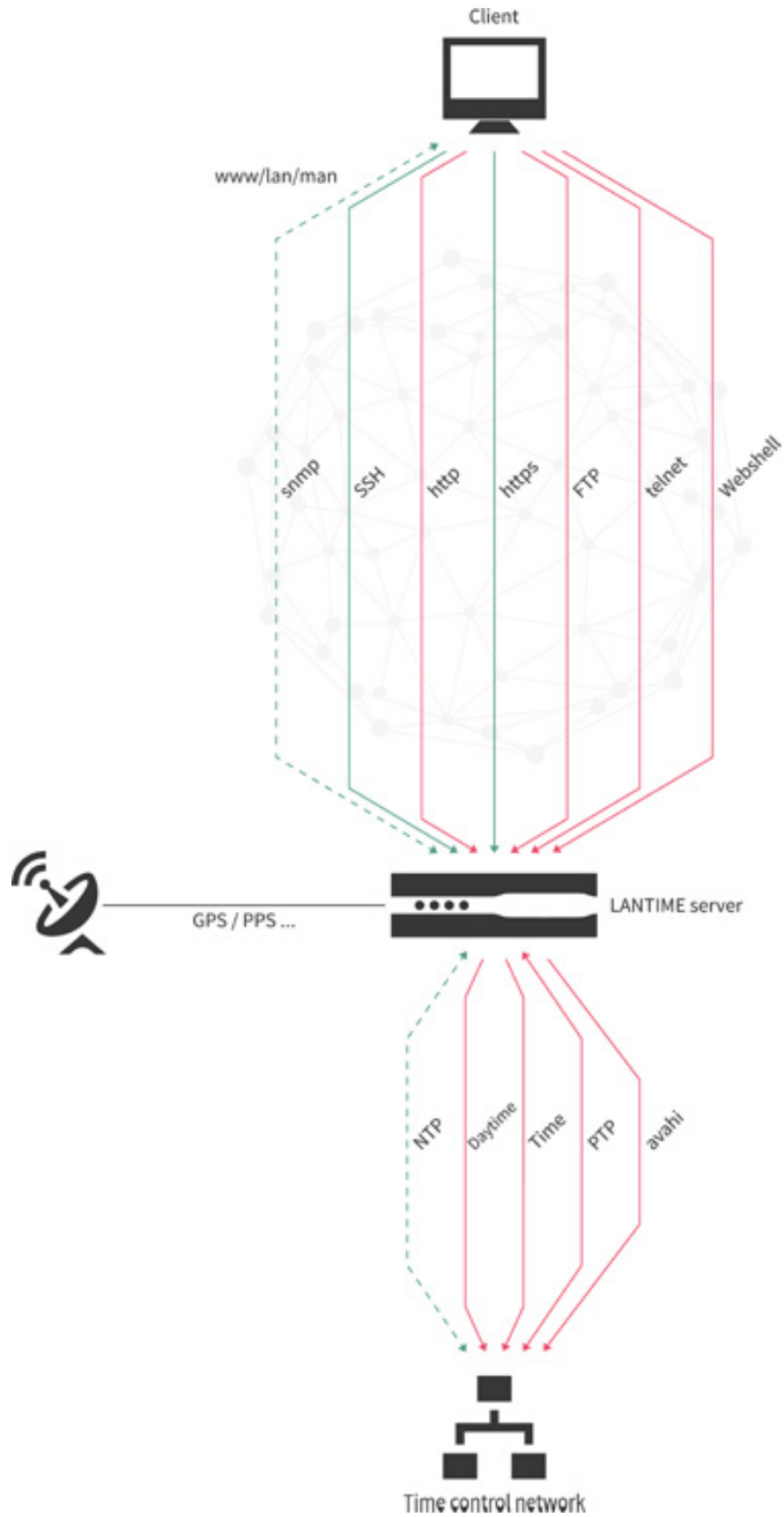


Figure 7.1: LANTIME services

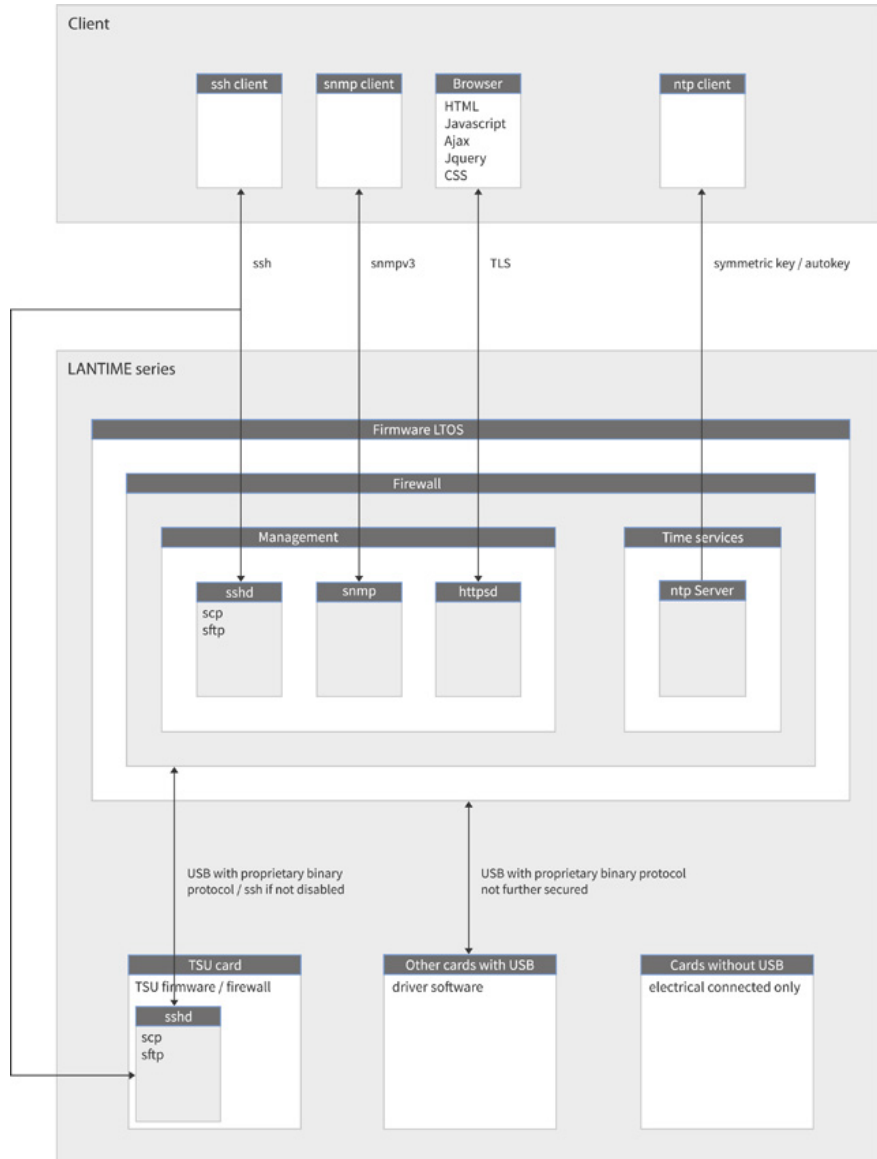


Figure 7.2: Secure protocols in detail

**LANTIME - PTP**

**PTP V2 Status**

**PTP V2 Configuration**

Interface 01 (Slot: MRI1): Network Global SyncE Misc Outputs

Interface 02 (Slot: MRI2): Network Global SyncE Misc Outputs

**Network:**

Monitor Interface

Net Link Mode Autoneg

Hostname PTPv2 Domainname

Nameserver 1 0.0.0.0 Nameserver 2 0.0.0.0

Enable DHCP-Client No

TCP/IP Address 172.27.84.103 Netmask 255.255.0.0

Default Gateway 172.27.0.1

IPv6 Mode Static

IPv6 Address

IPv6 Multicast Scope FF01 - Interface-Local Scope

Enable VLAN Option

VLAN-Tag (0-4094) 0 Priority 0

**Disable SSH Service**

Figure 7.3: Disable SSH on TSU

**LANTIME - Security**

**Login/Access**

**Front Panel**

**SSH**

**HTTPS Certificate**

**Generate SSL Certificate** Show SSL Certificate Download SSL Certificate

Durchsuchen... Keine Datei ausgewählt. Upload SSL Certificate Paste SSL Certificate

Optional Passphrase

Generate Certificate Request Show Certificate Request Download Certificate Request

**SNMP**

Save Settings Reset Changes Back

Figure 7.4: Generate SSL certificate step 1

**LANTIME - Security**

**Generate SSL Certificate**

Country Name (2 letter code)

State or Province

Locality Name

Organization Name

Organizational Unit

Common Name

Email Address

Key Length (bits)

Period of Validity

Please note: depending on the selected key length this could take several minutes.

Figure 7.5: Generate SSL certificate step 2

**Hint:**  
 Current configuration is not marked as startup configuration.

**LANTIME - Security**

**Show SSL Certificate:**

```

Certificate information:
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    ce:80:38:bb:b2:a3:56:a6
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=DE, ST=Some-State, L=Bad Pyrmont, O=testorga, OU=software,
CN=myLantime1/emailAddress=info@testorga.com
  Validity:
    Not Before: Jul  9 12:17:47 2018 GMT
    Not After : Jul  8 12:17:47 2021 GMT
  Subject: C=DE, ST=Some-State, L=Bad Pyrmont, O=testorga, OU=software,
CN=myLantime1/emailAddress=info@testorga.com
  Subject Public Key Info:
    
```

Figure 7.6: Show generated SSL certificate

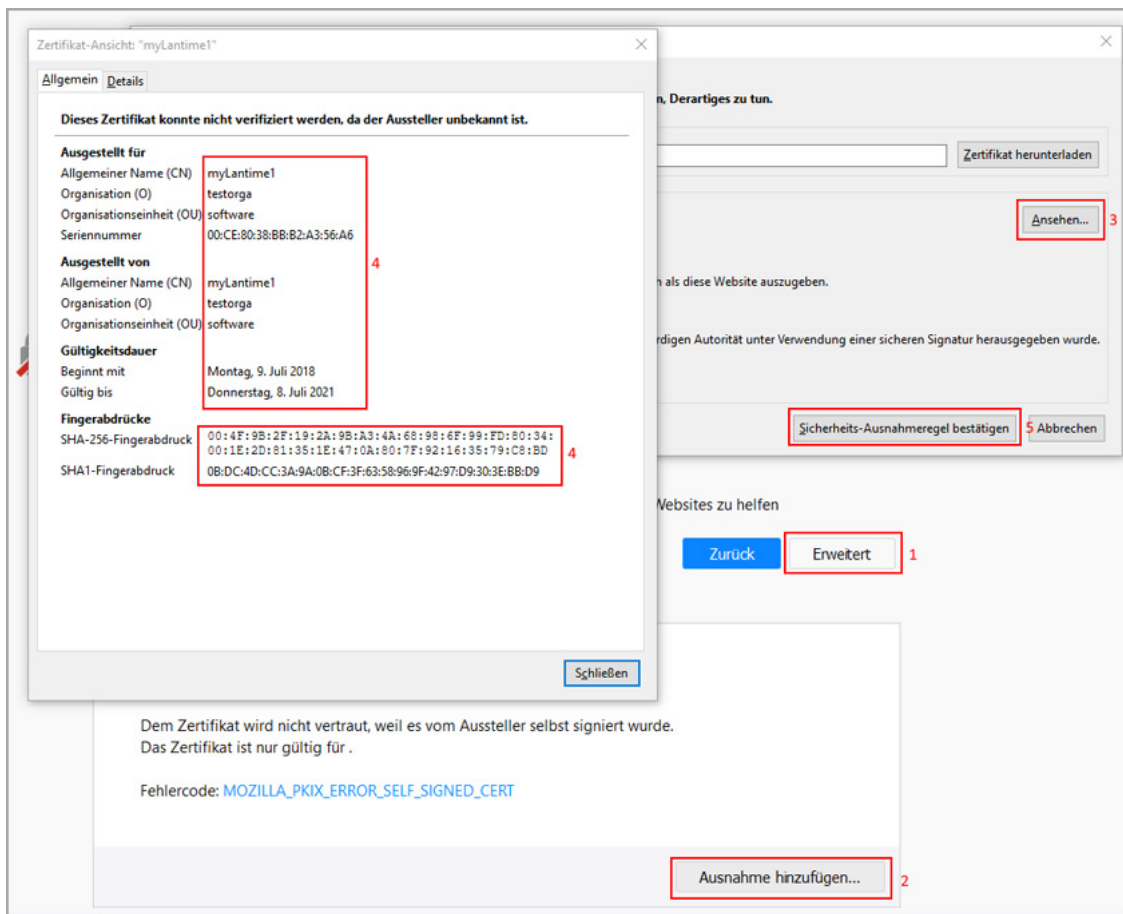


Figure 7.7: Import process of the new SSL certificate in the browser

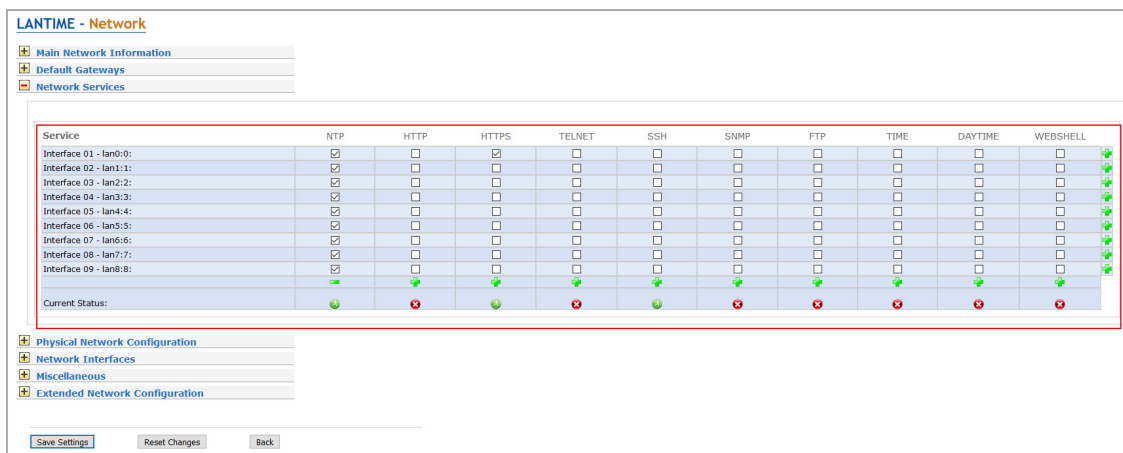


Figure 7.8: Deactivating services



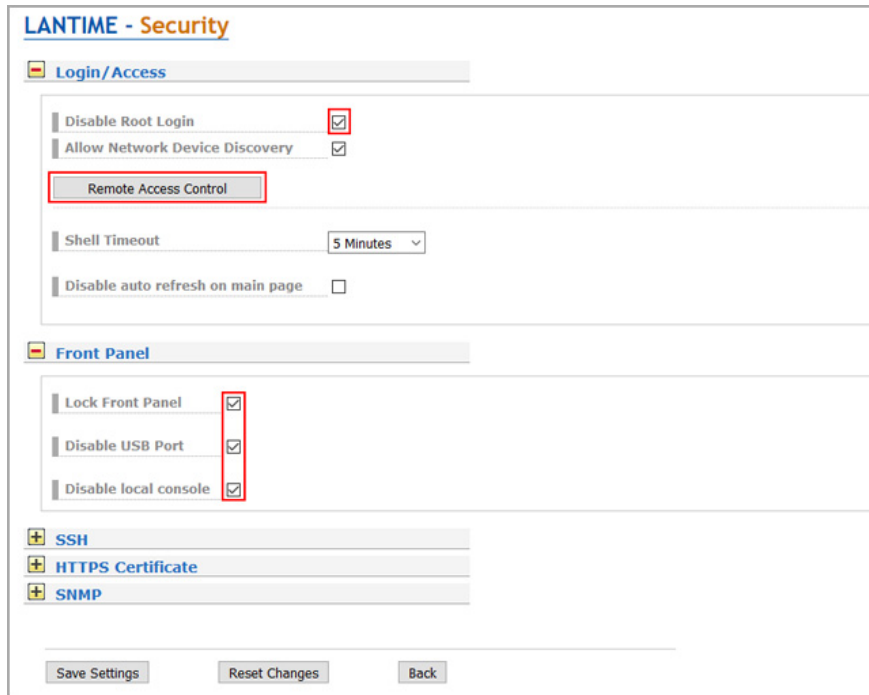


Figure 7.9: Deactivation of root and front panel

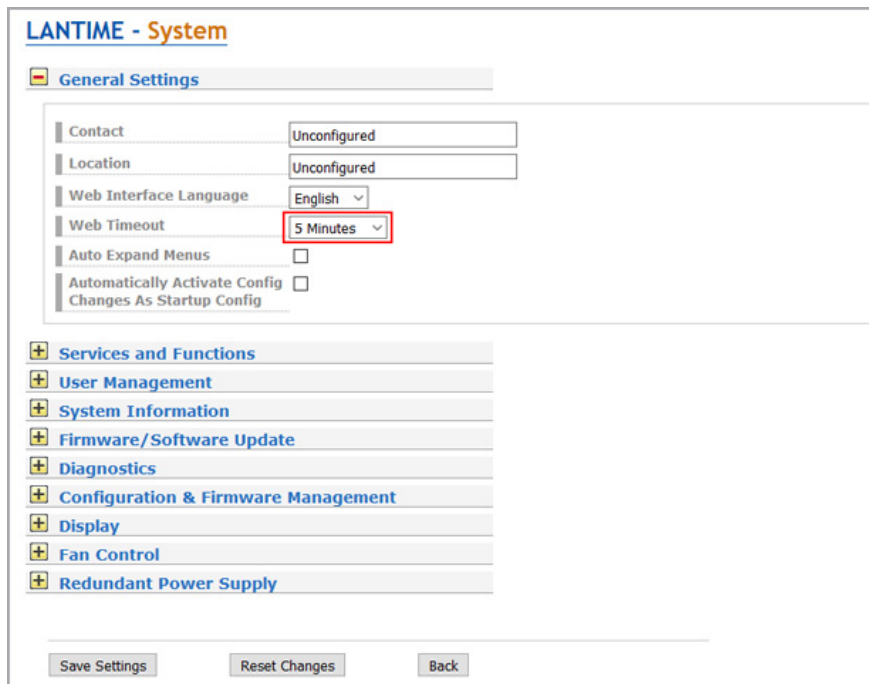


Figure 7.10: Set timeout of web interface

**LANTIME - Security**

- Login/Access
- Front Panel
- SSH
- HTTPS Certificate
- SNMP

**General Information**

SNMP Contact: Lantime1 | SNMP Location: Bad Pymont  
Please edit these values on the system page (General Settings).

Activated Protocol Versions: V3 only

**V1 & V2C Parameter**

Read Community: public | Write Community: private

**V3 Parameter**

Security Name: root2 | Security Level: authPriv  
 Engine-ID: tSNMP\_M0013952ecd8  
 Rights: Readonly Access

Authentication Protocol: SHA  
 Authentication Passphrase: [masked] | Re-Enter Passphrase: [masked]

Privacy Protocol: AES  
 Privacy Passphrase: [masked] | Re-Enter Passphrase: [masked]

Save Settings | Reset Changes | Back

Figure 7.11: SNMP options

### 7.3.1 LANTIME User Management

The LANTIME delivers a build in user configuration. The options are located under System→User\_Management. There are three different user groups: Super-User, Admin-User and Info-User. Super-Users are allowed to do everything, bash access included. Admin-Users are allowed to do everything that is on the web interface, but no operations that would grant super user rights. Info-Users are just allowed to see all non security relevant informations in the web interface. To create a User, use the form that is shown on Figure 7.12. Super-Users can create all user types. The Admin-User can create other Admin-Users and Info-Users. Enter a name, a password and the group of the user, then press the button Create User. If successful, the new user is displayed in the User List, right under the create user form. Choose the user names and passwords in a way that they are not predictable (the users on Figure 7.12 are negative examples).

For passwords, there are some additional options that are depicted in Figure 7.13. Choose a long password length and a periodical change interval. Additionally, you can use the secure password modifier to force a password containing many different character sets.

### 7.3.2 External User Authentication: Radius and TACACS+

In Addition to the users managed by LANTIME itself, a Radius or TACACS connection can be used to authenticate users. This configuration is also located in the User Administration under Add External Authentication Server. Look at Figure 7.14 for the input options. You have to enable External Authentication first. Afterwards, choose radius or TACACS+ from the drop down menu and insert the hostname, the pre shared secret and the right port. From now on, you are ready to login with the external authentication mechanism. At first the system checks the external server for the user. If no user exists with that credentials, the system checks the local users. It is described in "LTOS Management and Monitoring ->Via Web GUI -> External Authentication Options" how to configure the external authentication server.

**LANTIME - System**

**User Administration**

+ Change Current User Password

+ Create User

User Name:

Password:

Confirm Password:

Group Membership:

+ User List

User Name	Group Membership	Option
root	Super-User	Delete User
info	Info-User	Delete User
root2	Super-User	Delete User

+ External Authentication Options

+ Add External Authentication Server

+ External Authentication Server List

+ Password Options

Figure 7.12: User creation

**LANTIME - System**

**User Administration**

+ Change Current User Password

+ Create User

+ User List

+ External Authentication Options

+ Add External Authentication Server

+ External Authentication Server List

- Password Options

Minimum Password Length:

Allow secure passwords only:

Users must change password periodically:  Interval:

Disable password autocompletion in browser:

Figure 7.13: Password options

**LANTIME - System**

**User Administration**

- Change Current User Password
- Create User
- User List
- External Authentication Options

Enable External Authentication

Timeout (ms)

**Add External Authentication Server**

Authentication Method

Authentication Server

Shared Secret

Port

**Add Authentication Server**

External Authentication Server List

Password Options

Figure 7.14: Radius and TACACS+ options

## 7.4 Securing Time Service NTP

The time service NTP provides an authenticated and integrity secured packet transmission. Currently, NTP autokey is considered to be not as secure as the symmetric key procedure. Therefore, this guide will use the symmetric key configuration. The chapter "LTOS Management and Monitoring ->Via Web GUI -> NTP Symmetric Keys" describes all configuration options in detail.

To configure a connection, the system needs a key. Either use newly generated or add existing keys in the key file over the button Edit NTP Keys under NTP->NTP\_Symmetric\_Keys. If you automatically generate the keys by the system, MD5 and SHA1 keys will exist in the key file. Use the SHA1 keys for a better security. Figure 7.15 shows example keys. The key IDs have to be added to the trusted keys on "General Settings" menu point of NTP tab (see Figure 7.16). You can also deactivate mode 6 and 7 packet support. Optionally, activate access restriction to grant access only to known IP addresses. The symmetric keys are used for every connection type, i.e. server to client, external NTP server, broadcasting, multicasting and multicasting.

The insertion points for the right key IDs are marked on Figure 7.17, 7.18 and 7.19. If the system is a MRS System, only one key can be configured for all external server (also see "LTOS Management and Monitoring ->Via Web GUI -> NTP -> External NTP Server"). The configuration file of a client is shown in Figure 7.20. It contains the path to the keyfile, the trusted key IDs and the server IP which uses the key with ID 5 in this example.

## 7.5 Event Log Delivery

The LANTIME offers many transport channels for event log informations and a fine grained notification selection for each of them. Currently, no channel can be configured to be secure, except SNMP. It is a good practice to collect event log informations on a central server to correlate and check them for anomalies, but be aware of potential security relevant information leakage if you do so. The chapter "LTOS Management and Monitoring ->Via Web GUI -> Notification" describes the configuration options for the transport channels. If you use SNMP v3 with selected authPriv security level, also SNMP traps are securely transported. Configure SNMP authPriv level under Security->SNMP like in section 7.2 explained.

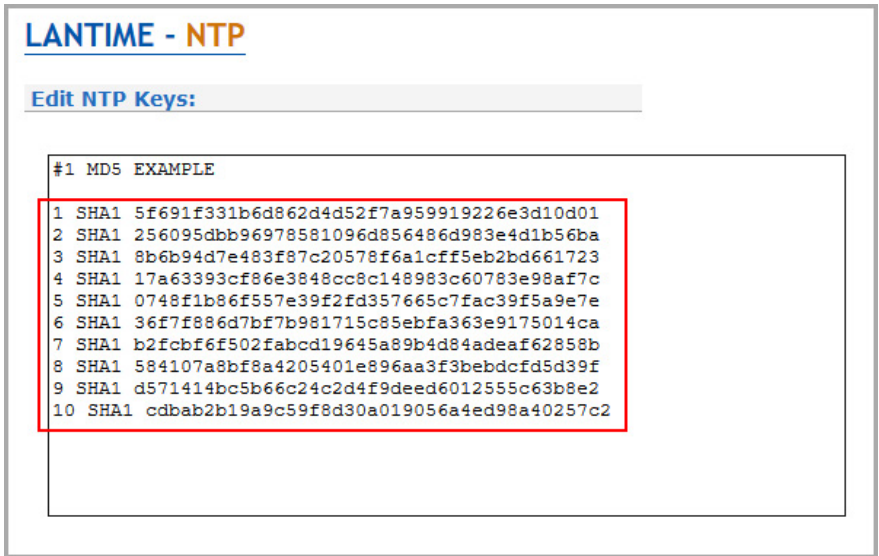


Figure 7.15: Generated symmetric NTP keys

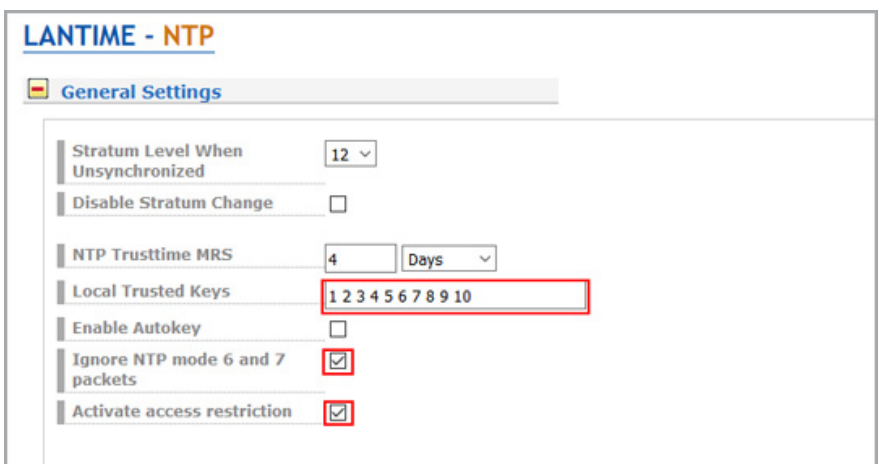


Figure 7.16: Trusted key IDs

**LANTIME - NTP**

**General Settings**

**External NTP Server**

Server Address 1	<input type="text" value="x.x.x.1"/>	Symmetric Key	<input type="text" value="1"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>
Server Address 2	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>
Server Address 3	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>
Server Address 4	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>
Server Address 5	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>
Server Address 6	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>
Server Address 7	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Minpoll	Auto	Maxpoll	Auto	Use iburst	<input type="checkbox"/>

Figure 7.17: External server configuration

**LANTIME - NTP**

**General Settings**

**External NTP Server**

**Broadcast Settings**

Broadcast Address 1	<input type="text" value="x.x.x.x"/>	Symmetric Key	<input type="text" value="1"/>	Use Autokey	<input type="checkbox"/>
Broadcast Interval	Auto				
Broadcast Address 2	<input type="text" value="x.x.x.x"/>	Symmetric Key	<input type="text" value="2"/>	Use Autokey	<input type="checkbox"/>
Broadcast Interval	Auto				
Broadcast Address 3	<input type="text" value="x.x.x.x"/>	Symmetric Key	<input type="text" value="4"/>	Use Autokey	<input type="checkbox"/>
Broadcast Interval	Auto				
Broadcast Address 4	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Broadcast Interval	Auto				
Broadcast Address 5	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Broadcast Interval	Auto				
Broadcast Address 6	<input type="text"/>	Symmetric Key	<input type="text"/>	Use Autokey	<input type="checkbox"/>
Broadcast Interval	Auto				

Figure 7.18: Broadcast configuration

**LANTIME - NTP**

- General Settings
- External NTP Server
- Broadcast Settings
- NTP Multicast & Manycast

---

Enable Multicast  
 Multicast Address:   
 Broadcast Interval:  Seconds  
 Symmetric Key:  Use Autokey:   
 TTL:

---

Enable Manycast  
 Manycast Address:   
 Symmetric Key:  Use Autokey:

Figure 7.19: Multi and many cast configuration

```

# restrict <IP OF REMOTE HOST>

# Use drift file
driftfile "C:\Program Files (x86)\NTP\etc\ntp.drift"
keys "C:\Program Files (x86)\NTP\etc\ntp.key"
trustedkey 5

# your local system clock, could be used as a backup
# (this is only useful if you need to distribute time no matter how good or bad it is)
#server 127.127.1.0
# but it should operate at a high stratum level to let the clients know and force them to
# use any other timesource they may have.
#fudge 127.127.1.0 stratum 12

# Use specific NTP servers
server x.x.x.x .1 iburst minpoll 6 maxpoll 7
server x.x.x.x .2 minpoll 4 maxpoll 4 iburst key 5

# End of generated ntp.conf --- Please edit this to suite your needs

```

Figure 7.20: NTP client configuration

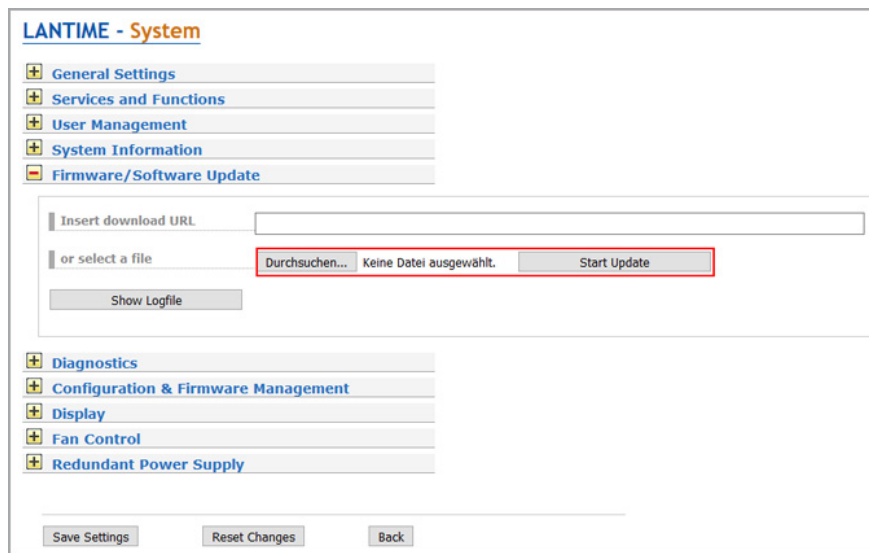


Figure 7.21: Upload firmware

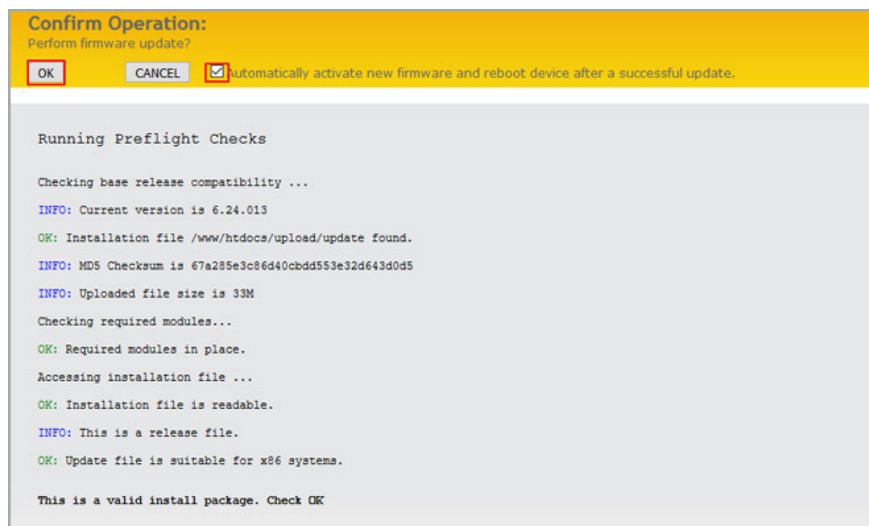


Figure 7.22: Update process of the firmware

## 7.6 Update And Backup LANTIME Firmware

Download the latest LTOS on <https://www.meinbergglobal.com/english/sw/firmware.htm>. The downloaded LTOS file has to be uploaded via the LANTIME web interface under System→Firmware/Software\_Update like on Figure 7.21. In the next step, you have to confirm the update and activate the new firmware like in Figure 7.22. The update was successful if Figure 7.23 is displayed.

To take account of changes made by the customer, configuration files are not overridden automatically by a firmware update. Unfortunately, this also includes a few security relevant configuration files. For this reason, a manual action is required. There are two ways to get the new configuration entries working. The fast way to do this, is to reset the factory defaults like on Figure 7.24. Be aware that all custom configurations will be lost, except the network configuration. You are still able to reach the LANTIME over the current IP after the update. But this also means, that your certificates and SSH keys are lost (it exists a backup on the flash memory) and you have to reconfigure everything else. The slow but most accurate way, is to look in every configuration and to make a difference (diff command) to get information about the changes that will modify the security parameters. Subsequently, you have to edit the existing (current) configurations over a SSH connection. The most important configuration files and their equivalents in the new firmware are the following:

- new: `/mnt/firmware/fw_x.xx.xxx/flash/firmware/OSV/packages/web/files/con.fig/default/etc/httpsd.conf`  
current: `/etc/httpsd.conf`



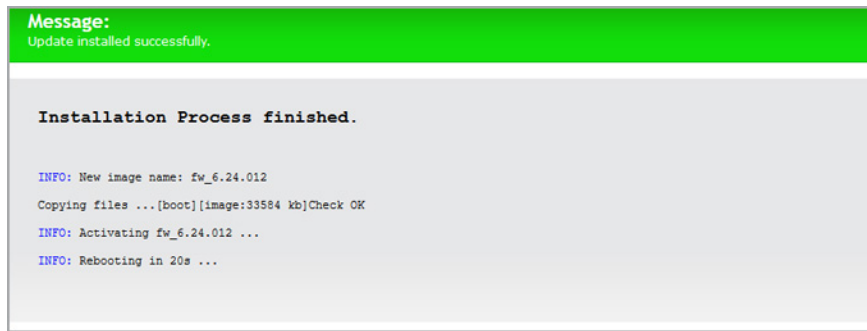


Figure 7.23: Successful firmware update

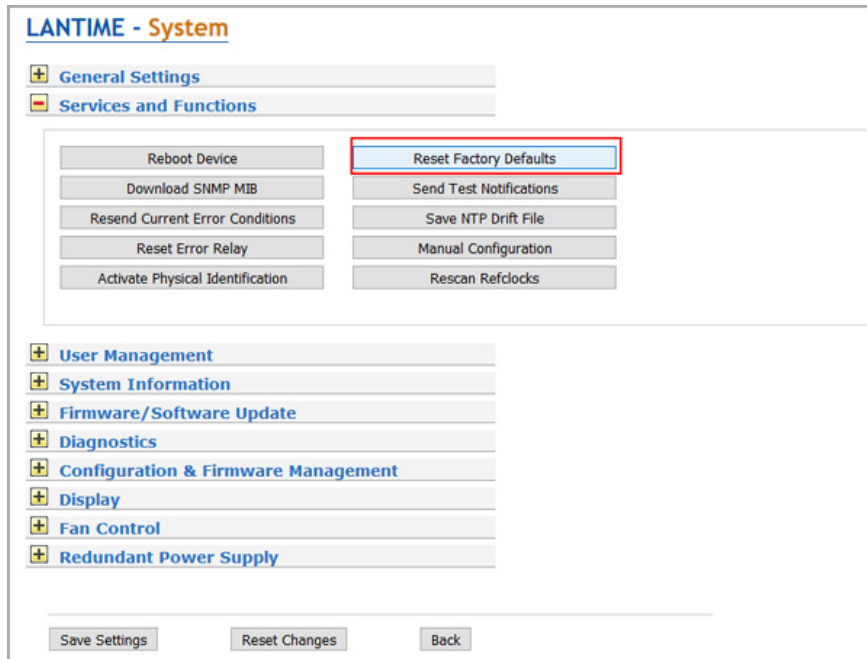


Figure 7.24: Reset factory defaults

- new: `/mnt/firmware/fw_x.x.x.x/flash/firmware/OSV/packages/web/files/config/default/etc/http - global.conf`  
current: `/etc/http - global.conf`
- new: `/mnt/firmware/fw_x.x.x.x/flash/firmware/OSV/packages/web/files/config/default/etc/http - redirect.conf`  
current: `/etc/http - redirect.conf`
- new: `/mnt/firmware/fw_x.x.x.x/flash/firmware/OSV/packages/web/files/config/default/etc/ssl/openssl.cnf`  
current: `/etc/ssl/openssl.cnf`
- new: `/mnt/firmware/fw_x.x.x.x/flash/firmware/OSV/packages/network/files/config/default/etc/portauth/portauth_default.conf`  
current: `/etc/portauth/portauth_default.conf`
- new: `/mnt/firmware/fw_x.x.x.x/flash/firmware/OSV/packages/lantime/files/config/default/config/ssh/sshd_config`  
current: `/etc/ssh/sshd_config`

This list has no claim of completeness! It is only the minimum amount you should always check. We can not give you a complete list, because we do not know which configuration will be changed due to security enhancements in the future.

After the reset over the web interface, all certificates are exchanged to the factory defaults. You have to re-inject your own company signed certificate, the certificate you used before or a newly generated. Also the settings and keys for SSH, SNMP and NTP must be set again as explained in the sections before.

A backup of the LANTIME firmware, if downloaded or saved on flash of the LANTIME, is in clear text form. For this reason make sure, that no unauthorized person has access to it. The same takes effect for a diagnostic file.

## 8 Antenna and Receiver Information

There are 2 types of radio signals commonly used for timing applications: **satellite signals from Global Navigation Satellite Systems (GNSS)**, and **long wave signals** from specific time code transmitters operated by some countries.

Most GNSS signals can be received world-wide, while long wave signals can only be received up to a certain distance around the transmitting station. Also, GNSS receivers can usually track the signals from several satellites at the same time, so the signal propagation delay can be determined and compensated automatically, while long wave receivers usually receive only the signal from a single station. Last but not least the available bandwidths and signal propagation characteristics are another reason why GNSS reception usually yields a higher degree of time accuracy than long wave reception.

### 8.1 Reference Time Sources

#### 8.1.1 Meinberg GPS Receiver

The satellite radio clock was developed with the aim of providing users with a highly accurate time and frequency reference. High accuracy and the possibility of worldwide use, 24 hours a day, are the main features of this system, which receives its time information from the satellites of the Global Positioning System. The Global Positioning System (GPS) is a satellite-based system for radio-positioning, navigation, and time-transfer.

This system has been installed by the United States Department of Defense (Defense Department) and provides two levels of accuracy: the Standard Positioning Services (SPS) and the Precise Positioning Services (PPS).

The structure of the sent data of the PLC has been released and the reception has been made available for general use, while the time and navigation data of the even more accurate PPS are transmitted encrypted and therefore only accessible to certain users (mostly military). The principle of location and time determination with the aid of a GPS receiver is based on the most possible accurate measurement of the signal propagation time from the individual satellites to the receiver.

The GPS satellites orbit the earth on six orbital tracks in 20,000 km of altitude once in about 12 hours. This ensures that at any time at least four satellites are in sight at any point on the earth. Four satellites must be received at the same time so that the receiver can determine its spatial position (x, y, z) and the deviation of its clock from the GPS system time.

Control stations on earth measure the orbits of the satellites and record the deviations of the atomic clocks carried on board from the GPS system time. The determined data are sent to the satellites and sent to earth as navigation data by the satellites. The highly precise track data of the satellites, called ephemerides, are needed so that the receiver can calculate the exact position of the satellites in space at any time. A set of track data with reduced accuracy is called almanac. With the aid of the almanacs, the receiver calculates at approximately known position and time, which of the satellites are visible from its location. Each of the satellites transmits its own ephemerides as well as the almanacs of all existing satellites. The GPS clock operates with the "Standard Positioning Service". The data stream of the satellites are decoded and evaluated by the microprocessor of the system, like that the GPS system time is reproduced with a deviation of less than 100 nsec. Different running times of the signals from the satellites to the receiver are automatically compensated by determining the receiver position. By tracking the main oscillator, a frequency accuracy of  $1e-12$  is achieved, depending on the oscillator type. At the same time, the age-related drift is compensated. The current correction value of the oscillator is stored in a non-volatile memory of the system.

### 8.1.2 Meinberg GNSS Receiver (GPS, GLONASS, Galileo, BeiDou)

High accuracy and the possibility of the world wide operation around the clock are the main features of the system, which receive his time information from the satellites of the American GPS (Global Positioning System), the European Galileo, the Russian GLONASS (Global Navigation Satellite System) and the Chinese BeiDou.

The Global Positioning System (GPS) is a GNSS operated by the US department of defense. Its purpose is to provide position, velocity and time for civilian and defense users on a global basis. The system currently consists of 32 medium earth orbit satellites and several ground control stations.

**GLONASS** is a GNSS operated by Russian Federation department of defense. Its purpose is to provide position, velocity and time for civilian and defense users on a global basis. The system consists of 24 medium earth orbit satellites and ground control stations. The GLONASS satellites circle the earth once on three orbital lanes in height of 19100km in about 12 hours.

**Galileo** is a GNSS operated by the European Union. Its purpose is to provide position, velocity and time for civilian users on a global basis. The system is currently not fully operational. It is eventually expected to consist of 30 medium earth orbit satellites. At the time of writing (early 2016), the Galileo system was still under development with only a few fully operational SVs. Therefore, the precise performance and reliability of u-blox receivers when receiving Galileo signals is effectively impossible to guarantee.

**BeiDou** is a GNSS operated by China. Its purpose is to initially provide position, velocity and time for users in Asia. In a later stage when the system is fully deployed it will have worldwide coverage. The full system will consist of five geostationary, five inclined geosynchronous and 27 medium earth orbit satellites, as well as control, upload and monitoring stations.

#### Characteristics

The GNS module is a combined GPS / Galileo / GLONASS / BeiDou receiver and operates with the "Standard Positioning Service" (GPS) or "Standard Precision" (Galileo, GLONASS, BeiDou). The data stream from the satellites is decoded by the microprocessor of the system. By analyzing the data, the GNSS system time can be reproduced very precisely. Different running times of the signals from the satellites to the receiver are automatically compensated by determining the receiver position. By tracking the main oscillator (Oven Controlled Xtal Oscillator, OCXO) a high frequency accuracy is achieved. At the same time, the aging-induced drift of the quartz is compensated. The current correction value for the oscillator is stored in a non-volatile memory of the system. This receiver is suitable not only for stationary operation but also for mobile use.

The Meinberg GLN receiver is the predecessor of the GNS clock and receives GPS, Glonass and BeiDou.

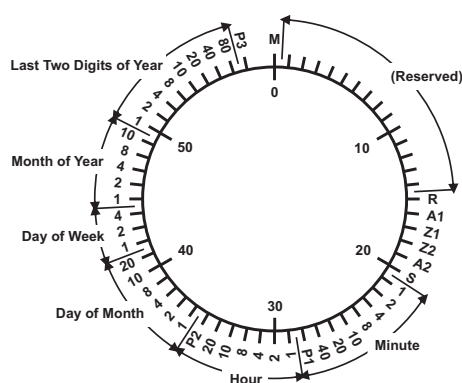
### 8.1.3 PZF - DCF77 Long Wave Receiver

The German long wave transmitter DCF77 started continuous operation in 1970. The introduction of time codes in 1973 build the basic for developing modern radio remote clocks. The DCF77 frequency and signal is derived from the atomic clocks of the Physikalisch-Technische Bundesanstalt (PTB) in Braunschweig, Germany, the national institute for science and technology and the highest technical authority of the Federal Republic of Germany for the field of metrology and physical safety engineering.

The carrier frequency of 77.5 kHz is amplitude modulated with time marks each second. The BCD-coding of the time telegram is done by shifting the amplitude to 25% for a period of 0.1s for a logical '0' and for 0.2s for a logical '1'. The receiver reconstructs the time frame by demodulating this DCF-signal. Because the AM signal is normally superimposed by interfering signals, filtering of the received signal is required. The resulting bandwidth-limiting causes a skew of the demodulated time marks which is in the range of 10 ms. Variations of the trigger level of the demodulator make the accuracy of the time marks worse by additional +/-3 ms. Because this precision is not sufficient for lots of applications, the PTB (Physical and Technical Institute of Germany) began to spread time information by using the correlation technique.

The DCF-transmitter is modulated with a pseudo-random phase noise in addition to the AM. The pseudo-random sequence (PZF) contains 512 bits which are transmitted by phase modulation between the AM-time marks. The bit sequence is built of the same number of logical '0' and logical '1' to get a symmetrical PZF to keep the average phase of the carrier constant. The length of one bit is 120 DCF-clocks, corresponding to 1.55 ms. The carrier of 77.5 kHz is modulated with a phase deviation of +/-10 per bit. The bit sequence is transmitted each second, it starts 200ms after the beginning of an AM second mark and ends shortly before the next one. Compared to an AM DCF77-receiver, the input filter of a correlation receiver can be dimensioned wideband width. The incoming signal is correlated with a reconstructed receiver-PZF. This correlation analysis allows the generation of time marks which have a skew of only some microseconds. In addition, the interference immunity is increased by this method because interference signals are suppressed by averaging the incoming signal. By sending the original or the complemented bit sequence, the BCD-coded time information is transmitted.

The absolute accuracy of the generated time frame depends on the quality of the receiver and the distance to the transmitter, but also on the conditions of transmission. Therefore, the absolute precision of the time frame is better in summer and at day than in winter and at night. The reason for this phenomenon is a difference in the portion of the sky wave which superimposes the ground wave. To check the accuracy of the time frame, the comparison of two systems with compensated propagation delay is meaningful.



M	Start of Minute (0.1 s)
R	RF Transmission via Secondary Antenna
A1	Announcement of a Change in Daylight Saving Time
Z1, Z2	Time Zone Identification
	Z1, Z2 = 0, 1: Daylight Saving Time Disabled
	Z1, Z2 = 1, 0: Daylight Saving Time Enabled
A2	Announcement of a Leap Second
S	Start of Time Code Information
P1, P2, P3	Even Parity Bits

The PZF radio clock is a precision receiver system for the time signal transmitter DCF77. It is available as a module for use in systems such as Meinberg IMS, LANTIME M300 models and as a computer plug-in card. The microprocessor of the system performs the correlation of a reproduced pseudo-random bit sequence with the PZF of the transmitter side and simultaneously decodes the AM time and date information of the DCF telegram. By evaluating the pseudo-random phase noise, a time raster can be generated which is up to a factor of a thousand more accurate than the ones of conventional AM radio clocks. In this way, an exact adjustment of the main oscillator of the radio-controlled clock is also possible, this allows it to be also used as a normal frequency generator, in addition to being used as a pure time receiver. If the PZF signal is temporarily unavailable for some reason, i.e. because a source of interference is in the vicinity, the radio clock will automatically switch to the AM signal - provided this is still receivable. The correlation receiver has a battery-buffered hardware clock, which takes over the time and date in the event of failure of the supply voltage.

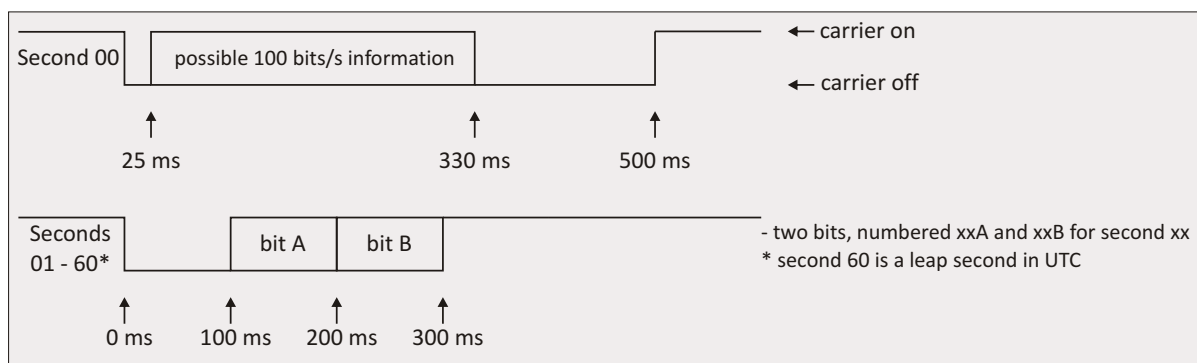
### 8.1.4 MSF Receiver

The transmission of the MSF signal from Anthon serves to distribute the British standard of the time and frequency signals. These standards are set by the National Physical Laboratory (NPL). The MSF signal provides sufficient field strength for use in the UK and can also be received in large parts of North and Western Europe. A simple on-off modulation of the carrier frequency (60kHz) is used to transmit BCD encoded time and date information. Each UTC second is marked with "off", preceded by at least 500 ms of carrier. This second marker is transmitted with an accuracy of  $\pm 1$  ms. The time code format is displayed via a minute frame, which is used to transfer the data to the next minute. The bits "A" and "B" are used to send the information (see graphic code format below).

The first second of the minute begins with a period of 500 ms with the carrier "off", to serve as a minute marker. The other 59 (or, exceptionally, 60 or 58) seconds of the minute always begin with at least 100 ms "off" and end with at least 700 ms of carrier "on". Seconds 01-16 carry information for the current minute about the difference (DUT1) between astronomical time and atomic time, and the remaining seconds convey the time and date code. The time and date code information is always given in terms of UK clock time and date, which is UTC in winter and UTC+1h when Summer Time is in effect, and it relates to the minute following that in which it is transmitted.

The MSF radio clock is a radio clock receiver system for the time signal transmitter MSF. It is available as a module for use in systems such as Meinberg IMS and LANTIME M300 models. The microprocessor of the system decodes the time and date information of the incoming AM signal. In this way, an exact adjustment of the main oscillator of the radio-controlled clock is also possible. The MSF receiver is equipped with a battery-buffered hardware clock, which takes over the time and date in the event of failure of the supply voltage.

#### Code Format



#### DUT Code

The DUT1 is signaled to the nearest 100ms in the range of  $\pm 800$ ms. A positive figure means that GMT is at a higher count than UTC. Bits 01B to 16B are used to signal the DUT code in the following way.

## Time and Date Code

Time and date information is transmitted and coded in the following way:

		Binary-Coded-Decimal Year (00-99)													
order		80	40	20	10	8	4	2	1						
bit		17A	18A	19A	20A	21A	22A	23A	24A						
		BCD month (01-12)					BCD day-of-month (01-31)					BCD day-of-week (0-6)			
order		10	8	4	2	1	20	10	8	4	2	1	4	2	1
bit		25A	26A	27A	28A	29A	30A	31A	32A	33A	34A	35A	36A	37A	38A
		BCD hour (00-23)					BCD minute (00-59)								
order		20	10	8	4	2	1	40	20	10	8	4	2	1	
Bit		39A	40A	41A	42A	43A	44A	45A	46A	47A	48A	49A	50A	51A	

## Other Codes

### Minute Identifier

Bits 53A to 58A are all set permanently at '1' and are always preceded by bit 52A at '0' and followed by bit 59A at '0'. This sequence '01111110' never appears elsewhere in bit xxA, so it uniquely identifies the following second 00 minute marker. In minutes lengthened or shortened by a positive or negative leap second all these numbers are correspondingly increased or decreased by one (i.e. during these 61- or 59-second minutes the position of the time and date code is shifted by one second relative to the start of minute).

### Parity Bits

The parity bits are providing and odd number of 1's.

Bit 54B taken with bits 17A to 24A

Bit 55B taken with bits 25A to 35A

Bit 56B taken with bits 36A to 38A

Bit 57B taken with bits 39A to 51A

### Summer Time

When UK civil time is subject to an one-hour positive offset during part of the year, this period is indicated by setting bit 58B to '1'. Bit 53B is set to '1' during the 61 consecutive minutes immediately before a change, the last being minute 59, when bit 58B changes.

### Unused Bits

The unused bits are currently set to '0', but may be used in the future.

### 8.1.5 WWVB Receiver

NIST radio station WWVB is located near Fort Collins, Colorado, on the same site as station WWV. The WWVB broadcast is used by millions of people throughout North America to synchronize consumer electronic timing products such as wall clocks, clock radios, and wristwatches. In addition, WWVB is used for high level applications including network time synchronization and frequency calibration. The WWVB transmission is maintained by the National Institute of Standards and Technology (NIST).

WWVB continuously broadcasts a time and frequency signal at 60 kHz. The carrier frequency provides a stable frequency reference traceable to the national standard. There are no voice announcements on the station, but a time code is synchronized with the 60 kHz carrier and broadcast continuously at the rate of 1 bit per second using pulse width modulation. The carrier power level is modulated to encode the time data. The carrier power is reduced by 17 dB at the start of each second, so that the leading edge of every negative going pulse is on time. Full power is restored 0.2 s later for a binary #0#, 0.5 s later for a binary #1#, or 0.8 s later to convey a position marker. The binary coded decimal (BCD) format is used, which combines binary digits to represent decimal numbers. The time code contains the year, day of year, hour, minute, second, and flags that indicate the status of Daylight Savings Time, leap year, and leap seconds. WWVB identifies itself by advancing its carrier phase 45 degrees at 10 minutes after the hour and returning to normal phase at 15 minutes after the hour. If you plot WWVB phase, this results in a phase step of approximately 2.08 microseconds.



### 8.1.6 TCR Receiver

The Board Meinberg TCR (Time Code Receiver) was designed for the decoding of unmodulated and modulated IRIG- and AFNOR-Timecodes. Modulated codes transport the time information by modulating a sinusoidal carrier signals amplitude whereas unmodulated signals employ a pulse width modulated DC signal.

The receivers automatic gain control allows the reception of signals within a range from abt. 600mVpp up to 8Vpp. The potential free input can be jumper selectable terminated in either 50 Ohm, 600 Ohm or 5 kOhm. Modulated codes are applied to the board via an on board SMB connector.

#### Abstract of Time Code

The transmission of coded timing signals began to take on widespread importance in the early 1950's. Especially the US missile and space programs were the forces behind the development of these time codes, which were used for the correlation of data. The definition of time code formats was completely arbitrary and left to the individual ideas of each design engineer. Hundreds of different time codes were formed, some of which were standardized by the "Inter Range Instrumentation Group" (IRIG) in the early 60's.

Except these "IRIG Time Codes", other formats like NASA36, XR3 or 2137 are still in use. The TCR receiver generates the IRIG-B, AFNOR NFS 87-500 code as well as IEEE1344 code which is an IRIG code, extended by information for time zone, leap second and date.

## 8.2 GNSS Signal Reception

The satellites of most **Global Navigation Satellite Systems (GNSS)** like **GPS**, **GLONASS**, and **Galileo** are not stationary but circle round the globe in periods of several hours. Only few GNSS systems like the Chinese **Beidou** system work with stationary satellites. Such systems can only be received in certain regions of the Earth.

GNSS receivers need to track at least four satellites to determine their own position in space ( $x, y, z$ ) as well as their time offset from the GNSS system time ( $t$ ). Only if the receiver can determine its own position accurately the propagation delay of the satellite signals can also be compensated accurately, which is requirement to yield an accurate time. If the receiver position can only be determined less accurately then the accuracy of the derived time is also degraded.

GNSS satellite signals can only be received directly if no building is in the line-of-sight from the antenna to the satellite. The signals can eventually be reflected at buildings, etc., and the reflected signals can then be received. However, in this case the true signal propagation path is longer than expected, which causes a small error in the computed position, which in turn yields less accurate time.

Since most of the satellites are not stationary, the antenna has to be installed in a location with as much clear view of the sky as possible (e.g. on a rooftop) to allow for continuous, reliable reception and operation. Best reception is achieved when the antenna has a free view of  $8^\circ$  angular elevation above the horizon. If this is not possible then the antenna should be installed with the best free view to the sky in direction of the equator. Since the satellite orbits are located between latitudes  $55^\circ$  North and  $55^\circ$  South, this allows for the best possible reception.

Meinberg provides their own GPS receivers which operate with an antenna/converter unit and thus allow for very long antenna cables, but some devices also include GNSS receivers which support other satellite systems like GLONASS, or Galileo in addition to GPS. These receivers usually require a different type of antenna equipment which is described in chapter (4.1.2).

## 8.2.1 Meinberg GPS Antenna/Converter

### 8.2.1.1 Introduction

The Meinberg **GPS antenna/converter unit** combines a standard GPS patch antenna with a frequency converter which translates the original 1.5 GHz signal received from the GPS satellites to an intermediate frequency, so a standard coaxial cable type like RG58 can be used for antenna cable lengths up to 300 meters (1000 ft). If a low-loss cable type like RG213 is used then even 700 meters (2300 ft) between receiver and antenna are possible without requirement for an additional amplifier.

**Surge protectors** are optionally available and should be used in the antenna line to protect the receiver from high voltages spikes e.g. due to lightning strikes close to the antenna. The antenna/converter unit is remotely powered by the connected GPS receiver via the antenna cable, so no external power supply is required near the location of the antenna if a coaxial cable is used.

If more than a single GPS receiver are to be operated then a **GPS antenna splitter** can be used to distribute the GPS signal from a single antenna. The GPS antenna splitter provides 4 outputs and can be cascaded to supply even more than 4 receivers with the GPS signal.

Alternatively there is also a **GPS Optical Antenna Link (GOAL)** available which uses a fiber optic connection between the antenna and the receiver which allows for a length up to 2000 meters (6500 ft), and provides a high level of insulation and surge protection due to the optical transmission. Since the fiber optic connection is unable to provide the antenna with DC current, an extra power supply is required in this case at the location of the antenna.

Due to the specific requirements for remote powering and frequency conversion the Meinberg GPS equipment is not necessarily compatible with GPS equipment from 3rd party manufacturers.

### 8.2.1.2 Mounting and Installation of the GPS Antenna

Proper installation of the GPS antenna/converter unit is illustrated in the figure below:

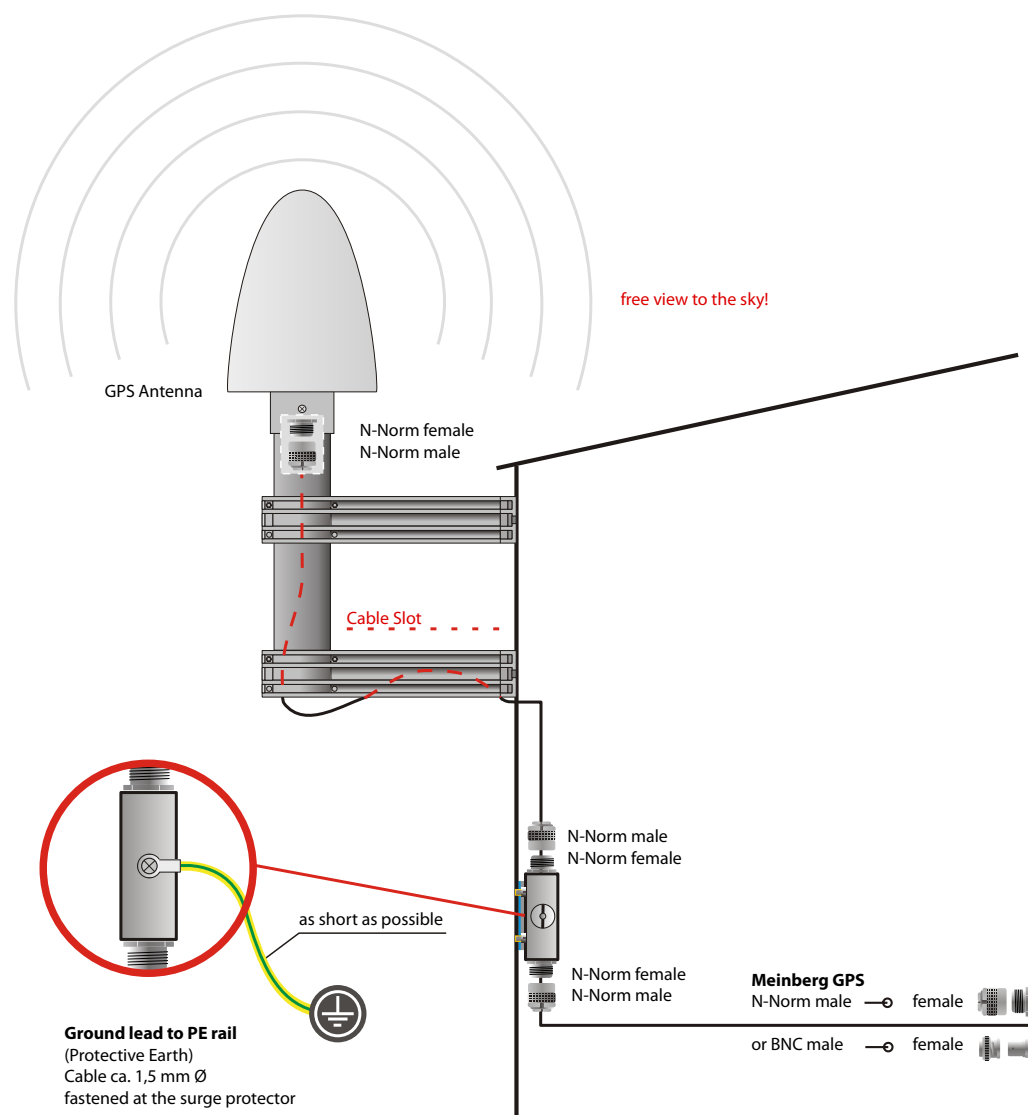


Figure: GPS Antenna mounted on a pole with a free view of the sky. The optional surge protector keeps high voltage strikes through the antenna cable away from the receiver.

Mounting material (plastic pole and holders, clamps for wall or pole mounting) is shipped with all Meinberg GPS antennae for easy installation. A standard RG58 antenna cable of 20 meters length is included by default. If a different cable length is required then this can be ordered accordingly.

Surge protectors should be installed indoors, directly where the antenna cable comes in. The optionally delivered protection kit is not for outdoor usage. The ground lead should be kept as short as possible and has to be connected to building's ground rod.

Up to four GPS receivers can be fed by a single antenna/down-converter unit by using an antenna splitter which can optionally be cascaded. The total length of an antenna cable from the antenna to each receiver must not exceed the specified maximum length according to the cable type. The position of the splitter in the antenna line does not matter.

**Note:**

If the antenna cable is assembled locally instead of using a cable shipped with the GPS receiver it has to be made sure that the connectors have been soldered and assembled properly, and that there is no short-circuit in the cable or in one of the connectors. Otherwise GPS reception may be degraded, or the GPS receiver can even be damaged. Mount the antenna at a distance of at least 50 cm from other antennas.

**WARNING!**

Do not mount the antenna without an effective fall arrester!

**Danger of death from falling!**

- Ensure that you work safely when installing antennas!
- Never work without an effective fall arrester!

**WARNING!**

Do not work on the antenna system during thunderstorms!

**Danger of death from electric shock!**

- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.



## 8.2.2 General GNSS Antennae

Some Meinberg devices use alternate GNSS receivers which support other satellite systems like GLONASS, Galileo or BeiDou, in addition to GPS. These receivers can't be operated directly with the standard Meinberg antenna/converter unit described in chapter "Meinberg GPS Receiver", so they require a different kind of antenna.

There are two different antenna versions available, one of which is more suited for stationary installation, while the other one should be preferred for mobile applications.

### 8.2.2.1 GNSS Antenna for Fixed-Location Installation

The **Multi-GNSS Antenna** is an active GNSS L1 antenna capable of receiving signals from the GPS, GLONASS, Galileo and BeiDou satellite systems. It is very well-suited to fixed-location installations. It is powered by a 5 V DC power supply from the receiver and offers integrated surge protection.

The antenna cable can be up to 70 meters in length if using a suitable low-loss coaxial cable such as Belden H155.

## Installation of the GNSS/L1 Antenna

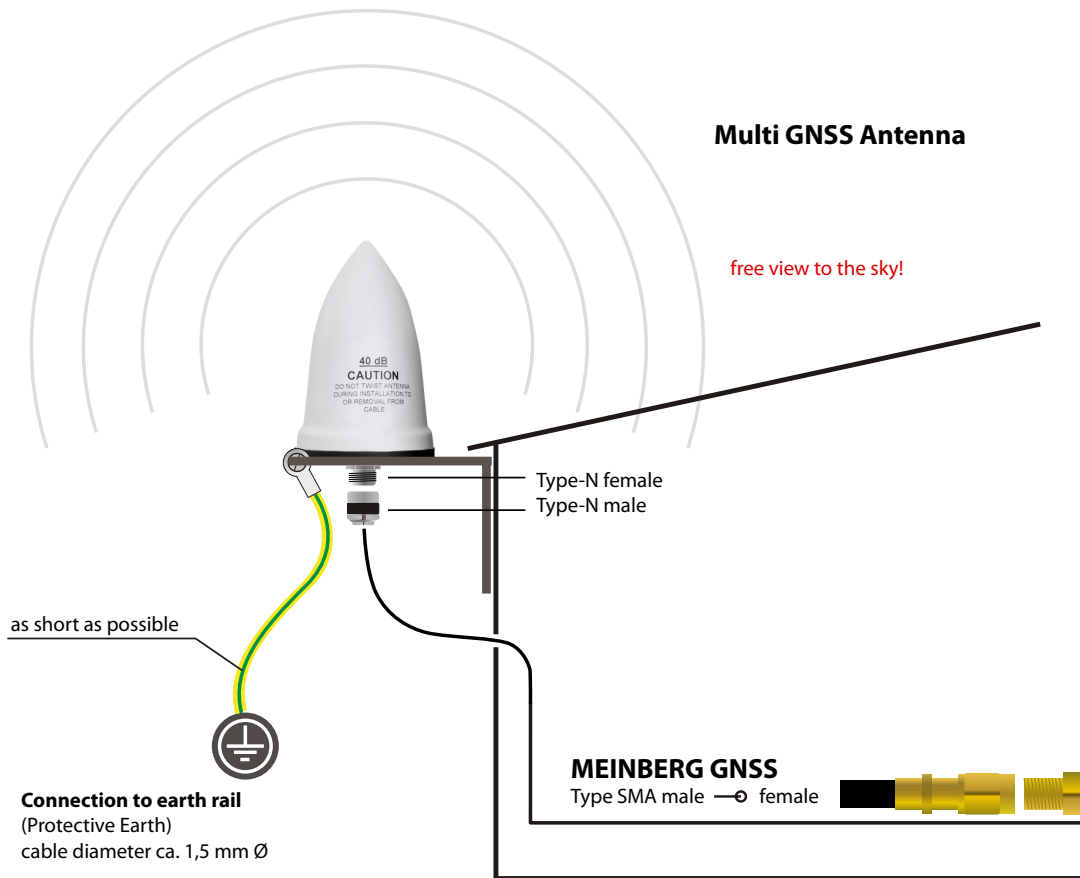


Image: Diagram Showing the Installation of the Multi-GNSS Antenna

### Danger!



Do not mount the antenna without an effective fall arrester!

**Danger of death from falling!**

- Ensure that all necessary safety measures are taken when installing an antenna!
- In particular, never work without an effective fall arrester!

### Danger!



Do not work on the antenna system during thunderstorms!

**Danger of death from electric shock!**



- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.

### 8.2.2.2 GNSS Antenna for Mobile Applications

The RV-76G is an active GNSS antenna which can receive the signals of the GPS, GLONASS, and Galileo satellite systems. It operates with a 5V DC supply voltage provided by the receiver, and should be preferred for mobile applications. However, the maximum length of the antenna cable is limited depending on the cable type, e.g. 5 meters with RG174/U cable, so this antenna is less suitable for stationary installations.

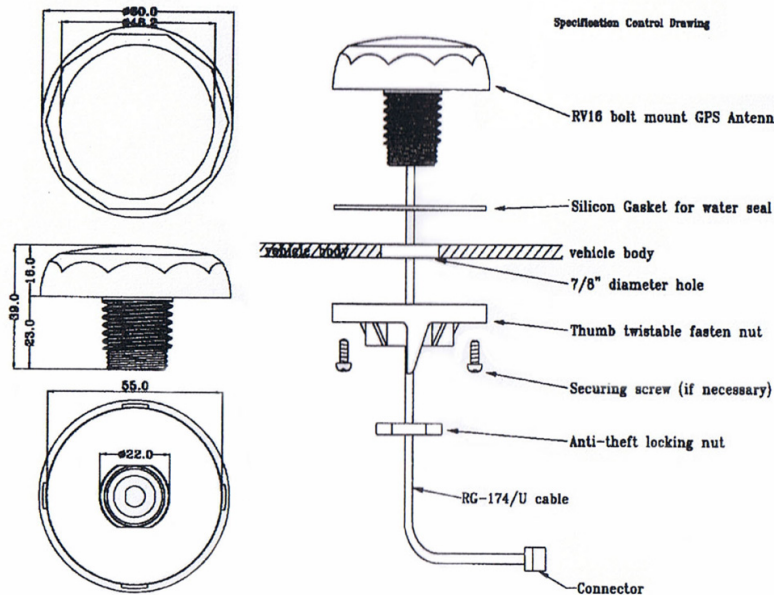


Figure: Installation drawing RV-76G antenna

#### Danger!



Do not mount the antenna without an effective fall arrester!

Danger of death from falling!

- Ensure that all necessary safety measures are taken when installing an antenna!
- In particular, never work without an effective fall arrester!

#### Danger!



Do not work on the antenna system during thunderstorms!

Danger of death from electric shock!

- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.



### 8.2.3 Powering up a GNSS Receiver

If both the antenna and the power supply have been connected the system is ready to operate. Depending on the type of oscillator installed in the receiver it takes about 10 seconds (OCXO-LQ) until 3 minutes (OCXO-MQ / HQ) until the oscillator has warmed up and reached the required frequency accuracy.

If the receiver has some valid almanac data in its battery buffered memory and the receiver's position has not changed significantly since its last operation the receiver can determine which satellites are in view. Only a single satellite needs to be received to synchronize and generate output pulses, so synchronization can be achieved at least one minute (OCXO-LQ) until 10 minutes (OCXO-MQ / HQ) after power-up. After 20 minutes of operation the OCXO is fully adjusted and the generated frequencies are within the specified tolerances.

If the receiver position has changed by some hundred kilometers since last operation, the expected satellites may not be in view after power-up. In this case the receiver switches to **Warm Boot** mode where it starts scanning for all possible satellites one after the other. Once the receiver can track at least 4 satellites at the same time it updates its own position and switches to **Normal Operation**.

If no valid data can be found in the battery buffered memory, e.g. because the battery has been disconnected or replaced, the receiver has to scan for satellites and collect the current almanac and ephemeris data first. This mode is called **Cold Boot**, and it takes at least 12 minutes until all required data have been collected. The reason is that the satellites send all data repeatedly once every 12 minutes. After data collection is complete the receiver switches to **Warm Boot** mode to scan for more satellites, and finally enters **Normal Operation**.

In the default configuration neither pulse and synthesizer outputs, nor the serial ports are enabled after power-up until synchronization has been achieved. However, it is possible to configure some or all of those outputs to be enabled immediately after power-up.

If the system starts up in a new environment (e. g. receiver position has changed or new power supply has been installed) it can take some minutes until the oscillator's output frequency has been adjusted properly. In this case the accuracy of the output frequency and pulses is also reduced until the receiver's control loops have settled again.

On the frontpanel ("Reference Time → Info GPS → GPS Satellites") as well as via the Web GUI ("Clock → Receiver Information") you can check the number of satellites that are in view (i.e. above the horizon) and considered good (i.e. are healthy and can be tracked).

## 8.3 Long Wave Signal Reception

### 8.3.1 Introduction

The longwave antenna **AW02** is a weatherproof and temperature resistant active antenna for outdoor use. It includes a ferrite antenna for reception of the longwave signal, and an amplifier, both assembled in a plastic housing. The standard version has been designed to receive the signal from the German longwave transmitter **DCF77** whose carrier frequency is 77.5 kHz. The DCF77 transmitter is operated by the German Physikalisch-Technische Bundesanstalt (PTB), and is located in Mainflingen near Frankfurt / Main. Its signal can be received in Germany and adjacent countries.

The variant **AW02-MSF** is available for the longwave transmitter **MSF** which is located in Anthorn / U.K., and transmits the time and frequency maintained by the U.K. National Physical Laboratory (NPL). The signal can be received throughout the U.K., and in wide parts of Northern and Western Europe.

Another variant is the **AW02-WWVB** which has been adapted for the **WWVB** radio station which is located in the United States near Fort Collins, Colorado, and is maintained by U.S. National Institute of Standards and Technology (NIST).

Even though these antenna variants are slightly different according to the characteristics of the associated transmitter, the basic requirements for installation are identical.

The longwave antennae can be operated with a cable length up to 300 meters (1000 ft) if standard RG58 coaxial cable is used. They are remotely powered by the receiver via the antenna cable, so no external power supply is required near the location of the antenna if a direct coaxial cable is used.

**Surge protectors** are optionally available and should be used in the antenna line to protect the receiver from high voltages spikes e.g. due to lightning strikes close to the antenna.

For longer distances from the antenna to the receiver an optional amplifier can be used, which requires an extra power supply. The **BLV** device is an amplifier with integrated surge protector.

Alternatively there is a **DCF Optical Antenna Link (DOAL)** available which uses a fiber optic connection between the antenna and the receiver which allows for a length up to 2000 meters (6500 ft), providing a high level of insulation and surge protection due to the optical transmission. Again, the default device has been designed for DCF77, but there are also variants for MSF and WWVB available. Since the fiber optic connection is unable to provide the antenna with DC current, an extra power supply is required in this case at the location of the antenna.

Longwave receiver equipment from Meinberg has specifically been designed for Meinberg devices and is not necessarily compatible with receivers from 3rd party manufacturers.

### 8.3.2 Mounting and Installation of a Longwave Antenna

The careful selection of the antenna location should be at the beginning of each antenna installation. It determines the reception quality and therefore the availability of the DCF77 reception signal decisively. In principle, a DCF77 reception within buildings is possible, however, the DCF77 reception may deteriorate due to metallic objects (e.g. reinforced concrete walls, metal facades, heat protection glazing etc.) that shield or attenuate the reception.

For this reason we always recommend to mount the antenna outside of buildings. This has the advantage that the signal interference distance to electronic devices in buildings is usually enhanced and the reliability of the synchronisation is thus significantly increased.

Proper installation of an antenna for DCF77, MSF, or WWVB is illustrated in the figure below:

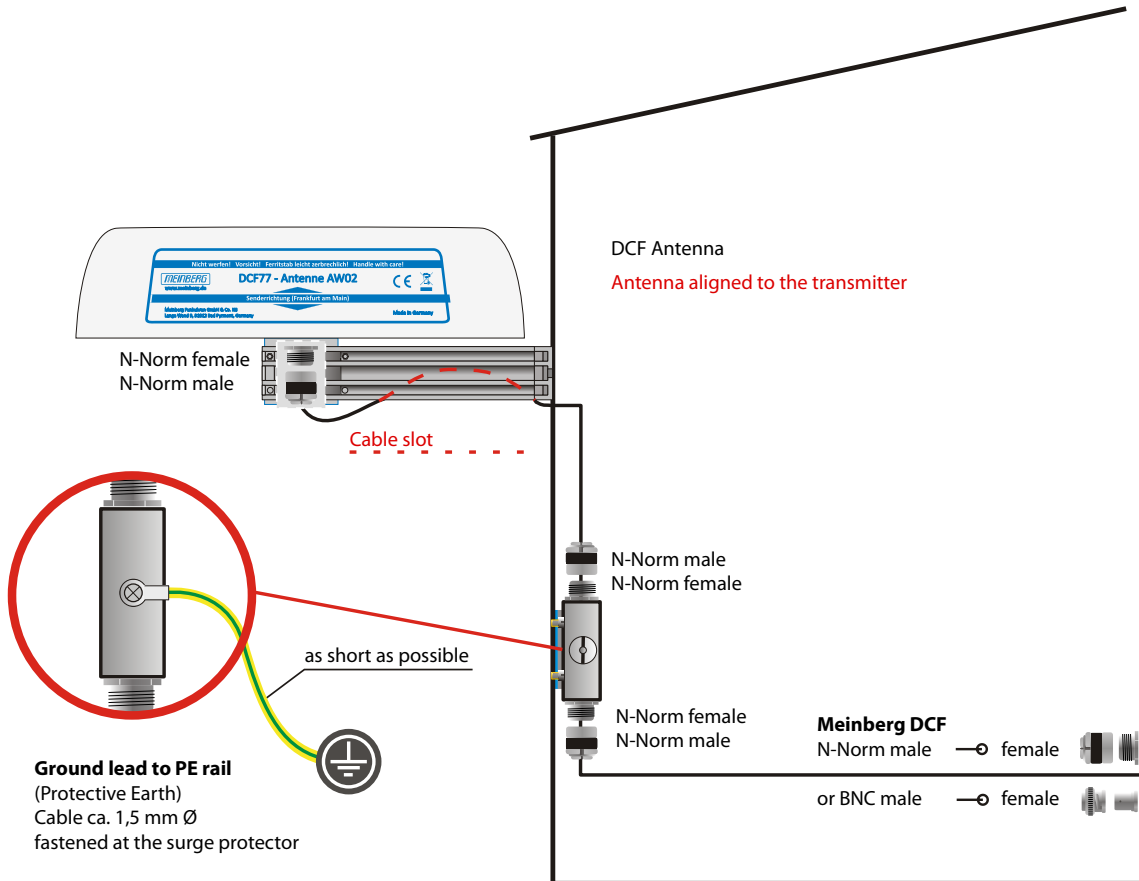


Figure: Longwave antenna mounted on a wall. The optional surge protector keeps high voltage strikes through the antenna cable away from the receiver.

The antenna has to be aligned horizontally in longitudinal direction to the transmitter, i.e. in direction to Mainflingen near Frankfurt / Main in case of DCF77, or in direction to the location of the MSF or WWVB receiver accordingly.

If the antenna is not aligned properly then signal reception is degraded, which can result in a limited time accuracy. The antenna should be installed with a minimum distance of 30 cm away from all metal objects and possibly any microcomputers and electrical devices (engines, electricity, etc.). A distance of several meters from TV and computer monitors should be considered as well.

The best method to align a longwave antenna is to turn the antenna slowly until the monitored signal level is minimized, and then turn the antenna by 90° to achieve maximum reception. However, a high signal level alone is not a guarantee for good reception since it can even be caused by electrical noise in the associated frequency range. For standard longwave receivers it is important that the modulation mark is blinking exactly once per second, without intermediate flickering.

DCF77/PZF receivers use correlation techniques to decode the phase modulation provided by DCF77, and with these types of receiver the maximum interference immunity can be found by looking at the autocorrelation parameter displayed in the display menu "PZF-STATE". The displayed value should be as close as possible to 100 % for best reception.

**WARNING!**

Do not mount the antenna without an effective fall arrester!

**Danger of death from falling!**

- Ensure that you work safely when installing antennas!
- Never work without an effective fall arrester!

**WARNING!**

Do not work on the antenna system during thunderstorms!

**Danger of death from electric shock!**

- Do not carry out any work on the antenna system or the antenna cable if there is a risk of lightning strike.
- Do not carry out any work on the antenna system if it is not possible to maintain the prescribed safe distance to exposed lines and electrical substations.



### 8.3.3 DCF77 / PZF Receiver

If both the antenna and the power supply have been connected the system is ready to operate. After power up it takes up to three minutes for the receiver to synchronize, if reception is good enough. A high "Correlation & Field" is an indicator for a good signal quality.

To check the field strength and the signal correlation value, select in the Front Panel "Reference Time → Info PZF → Correlation & Field".

The correlation "State" starts in a "raw" mode, when the receiver tries to find the initial correlation. When good correlation has been found the receiver checks it 20 times: this state is labeled "check" and the correlation value is increased from 1 to 20. If the correlation quality stays good the state changes to the "fine" mode. The signal strength should be 100 or higher.

If no correlation with the incoming signal is possible then the clock changes automatically to DCF77 AM reception mode and tries to decode the second marks.

For further detailed clock configuration, please refer to the Chapter [Clock](#)".

## 8.4 Cable Types

Antenna Type	Cable Type	Maximum Cable Length
Meinberg GPS Antenna	RG58	300 m / 1000 ft
Meinberg GPS Antenna	RG213	700 m / 2300 ft
Multi GNSS Antenna	Belden H155	70 m / 230 ft
Long Wave Antenna *	RG58	300 m / 1000 ft
Fiber Optic **	Fiber Optic	2000 m / 6500 ft

\* DCF77 (Germany, Middle Europe), MSF (GB), WWVB (US), JJY (Japan)

\*\* Fiber Optic - GOAL - GPS Optical Antenna Link; DOAL - DCF Optical Antenna Link

# 9 LTOS6 Management and Monitoring

## 9.1 Via Web GUI

### 9.1.1 Main Menu

**LANTIME - Main Menu**

**General Information**

LANTIME	M1000 IMS (GPS)	Serial Number	060811015170
Contact	Unconfigured ( <a href="#">Configure Now</a> )	Serial Number LANCPU	004711258370
Uptime	10 days, 20:19	Location	Unconfigured ( <a href="#">Configure Now</a> )

**Network Information**

Hostname	timeserver	Domain	
LAN IPv4 (VIF 1 - lan0:0)	172.28.7.7/16	IPv6 (VIF 1)	Not assigned
LAN IPv4 (VIF 2 - lan1:1)	Not assigned	IPv6 (VIF 2)	Not assigned
LAN IPv4 (VIF 3 - lan2:2)	Not assigned	IPv6 (VIF 3)	Not assigned
LAN IPv4 (VIF 4 - lan3:3)	Not assigned	IPv6 (VIF 4)	Not assigned
LAN IPv4 (VIF 5 - lan4:4)	Not assigned	IPv6 (VIF 5)	Not assigned
PTP IPv4 (Slot: ES11)	192.168.100.10/24	PTP IPv6 (Slot: ES11)	Not assigned

**Receiver Information**

MRS Status	Sync to GPS	Receiver information	sync; 51.9827 9.2261 166m; 10/10SVs; normal operation
------------	-------------	----------------------	---

**NTP Information**

NTP Status	Offs.-1us Stratum: 1	Date/Time	UTC 07:59:11 Mon, 10/16/2017
------------	----------------------	-----------	------------------------------

**PTP Information**

Port State (Slot: ES11)	UNINITIALIZED	PTP Mode (Slot: ES11)	Multicast Slave
-------------------------	---------------	-----------------------	-----------------

**Last messages**

```

2017-10-05 17:39:26 UTC: LANTIME -> Oscillator Adjusted [CLK: 1 ]
2017-10-05 11:44:44 UTC: LANTIME -> Oscillator Not Adjusted [CLK: 1 ]
2017-10-05 11:43:43 UTC: LANTIME -> Normal Operation
2017-10-05 11:43:38 UTC: LANTIME -> Network Link Up [LAN Interface: 0 ]
2017-10-05 11:43:24 UTC: LANTIME -> NTP Restart
2017-10-05 11:43:24 UTC: LANTIME -> NTP Sync To MRS
2017-10-05 11:43:24 UTC: LANTIME -> NTP Sync
2017-10-05 11:43:23 UTC: LANTIME -> NTP stratum changed from 16 to 1
2017-10-05 11:43:20 UTC: LANTIME -> NTP Not Sync
2017-10-05 11:43:07 UTC: LANTIME -> XMR Reference Disconnected [Reference Source: 7 (CLK1 STR in)]
2017-10-05 11:43:07 UTC: LANTIME -> XMR Reference Disconnected [Reference Source: 6 (CLK1 FRQ in)]
2017-10-05 11:43:07 UTC: LANTIME -> XMR Reference Disconnected [Reference Source: 5 (CLK1 PTP (IEEE1588))]

```

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

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

**Internet**  
 Website: <https://www.meinbergglobal.com>  
 Email: [info@meinberg.de](mailto:info@meinberg.de)

This chapter provides you with configuration options and status information of your LANTIME system accessed via Web GUI. The main page contains an overview of the most important configuration and status parameters for the system.

- Information about LANTIME model and software
- Network information
- Receiver status
- NTP status
- PTP status (option)
- Last messages
- Statistics (NTP/MRS Performance, NTP Access ...)
- Extended Statistics (MRS - external reference input signals)
- Documentation (Manuals), support information

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/lantime_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.

### 9.1.1.1 Introduction

To start a http or a secured https session with the Web Interface running on the CPU of your LANTIME system, you need to open your internet browser and type in the IP address of the interface you are using for this connection. Both http and https protocols are per default enabled at each assigned network interface. If you wish to use only one dedicated network interface for management and monitoring and the rest for other services you can find the corresponding configuration options in the Chapter "LTOS Configuration → Via Web → Network" in the submenu [Network Services](#).

If the connection with the LANTIME is established correctly you will be prompted to enter login data to start the web session. Per default the entering user-name/password are: root/timeserver. For security reasons you are advised to change the default credentials after the first login. The corresponding user administration settings can be found in the Chapter "LTOS6 Configuration → Via Web → System" in the submenu [User Management](#).

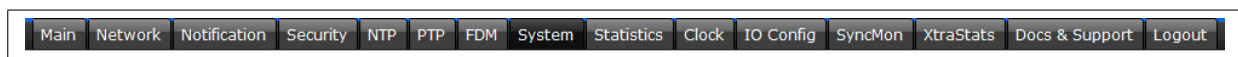
After entering the correct password, the main menu page of the web interface of a LANTIME system shows up.

The main page contains an overview of the most important configuration and status parameters of the system, including:

- general information (model name, serial number, uptime since last reboot)
- assigned network and PTP interfaces (both in IPv4 or IPv6 configuration)
- receiver status information (sync or not, for GNSS receivers some additional satellite data)
- SHS (Secure Hybrid System) status in redundant receiver configuration, which provides a plausibility mode where the incoming times of both time signals are continuously compared against each other. For more information about the SHS mode and the corresponding settings you can find in Chapter "LTOS6 Configuration → Web GUI → Security → [SHS Configuration](#)".

### 9.1.1.2 How to navigate through the Web Interface

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



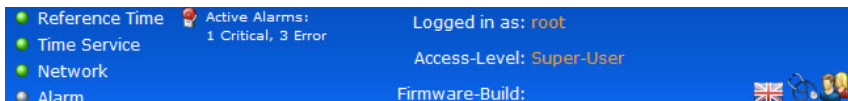
Scrolling down the main page you will find a section containing last log messages generated during the LANTIME operation. The messages in this field are limited to the last 50 and are chronologically ordered. The messages are stored in the file `/var/log/lantime_messages`, which is created after every start of the system (and is lost after a power off or reboot). To view all log messages in the log file you would have to use the CLI (Command Line Interface). For your reference, a list of available CLI commands for LANTIME management and monitoring is provided in the Chapter "LTOS6 Configuration → [Via CLI](#)".

### 9.1.1.3 Web Interface - Notifications and Alarms

At the top of the main page in the right corner you can find an image of the status LED lamps which are physically located at the front site of a LANTIME system, in models with an integrated front panel unit. When the system is in operation and everything runs as expected, the upper three status LEDs are turned to green and the Alarm indicator is switched off. If you experience after the powering up the system and after the startup has been completed that one or more LEDs are switched on red, please proceed to the Chapter on [Troubleshooting and Alarming](#).

**Please note:** startup of the system can take a several minutes, depending on the hardware configuration of your system.

Next to the status LEDs you will see displayed all active alarms currently present on a LANTIME with critical and error severity levels. With a mouse click over the alarms you will reach a table of notification events with red marked indicators at the events which triggered the alarms.



For further information how to eliminate a cause of each individual alarm, proceed to the Chapter on [Troubleshooting and Alarming](#).

Next to the alarm area in the main page there is a field with informational data about your login status and information to which access-level group you belong as a current user. There are three types of users: Super-User, Admin-User and Info-User. The exact definitions of the three different user types and their access-level rights you can find in Chapter "LTOS6 → Web GUI → System-> [User Management](#)".

At the top right corner of the main page you can see a few icons. The displayed flag indicates the language pack which is currently activated for the web interface display. For the moment you can choose between English and German languages packs.

Next to the language flag, there is an icon showing a doctor's stethoscope linked with a diagnostic file of the system, which includes all the necessary data for diagnostic and troubleshooting of the device. By clicking this icon a current diagnostic file will immediately start to download for you to save it to your local computer for a further use. The downloading can take up to 60 seconds, depending on the file size, which can be several MB. In the diagnostic file all the data about the system configuration and log messages are stored. The diagnostic file can be also an important tool for the Meinberg support team if you need some help with the configuration or you experience issues which you can not solve on your own. More about the diag file see Chapter "LTOS6 Configuration → via Web GUI → System → [Download Diagnostic File](#)".

The web interface is divided into several dialogue menus, where some of the dialogues (e.g. PTP; IO Config and TimeMon) depend on the hardware components which are integrated in the LANTIME system and only appear in systems with a corresponding configuration. The rest of the dialogues are common to all LANTIME and IMS systems.

You can move between the dialogues by clicking each individual name tag at the top of the menu line. When you click on the Logout tag, your Web session with the LANTIME device will be terminated immediately.

The two dialogues Main and XtraStats deliver you the status information about the LANTIME system after the last reboot. The rest of the dialogues provide configurations of features for the LANTIME operation and services. The dialogues with feature configurations are presented in a tree structure, where each submenu can be extended into a subtree by clicking at the "+" sign at the beginning of the submenu row. When you open the dialogue, the "+" will turn in "-" and when you click the "-" icon the currently open dialogue will close. You can have a few dialogues open at the same time in the currently selected menu (see the example on the next page).



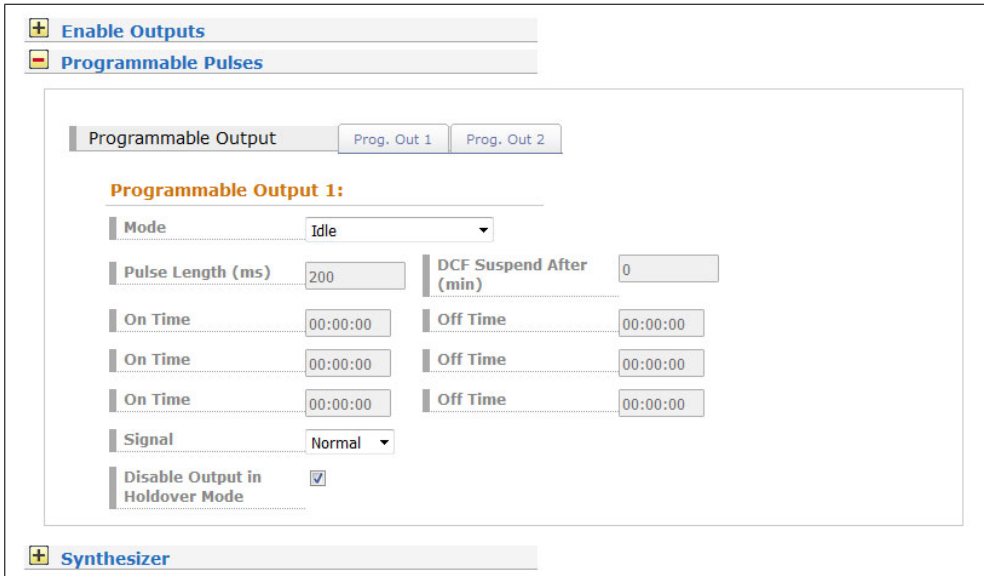


Figure: A tree structure of each menu. Opening a subtree by clicking a "+" and closing by "-" at the beginning of the submenu name

Generally, in any configuration menu you are located, when you fill in or edit one or more feature fields at the end you need to confirm the setting by clicking the "Save Settings" button at the bottom of the page. By doing so and if the setting has been carried out successfully, you will receive a dialogue in the Main Menu with a confirmation message written on a green field. At the same time when a new configuration has been applied a log message will appear in the list of last messages in the Main Menu saying: "Device Configuration Changed".

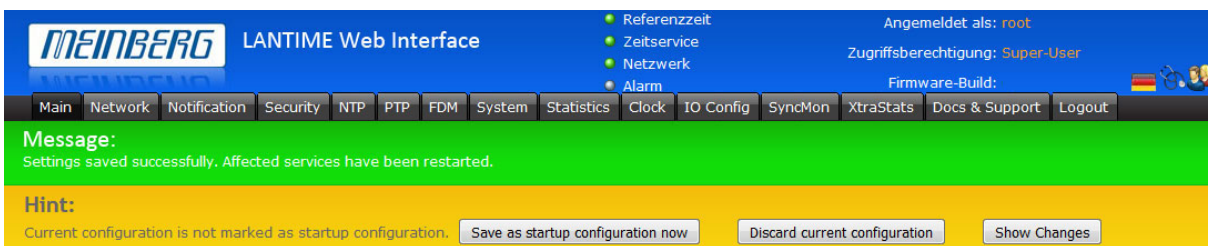


Figure: Settings saved successfully. Affected services have been restarted

A Saving startup configuration dialogue. Options for saving, discarding the current configuration and showing changes between the startup configuration and the current one.

Apart of the configuration message you will receive also an attention notice displayed on a yellow bar, saying: "Current configuration is not yet marked as a startup configuration". This means that you need to confirm the new configuration first by clicking on a "Save as startup configuration now" button if you want to keep it as a startup configuration by the next startup of the system. By clicking this button you will receive another confirmation message saying: "Activate current configuration really as startup configuration?" which you confirm by clicking the "OK" button. The new configuration has now become the startup configuration on your LANTIME system.

On the other hand, if you want to return to the last saved startup configuration then you select "Discard current configuration" button when the message on a yellow bar appears.

Each entry you fill in in the provided dialogues is checked for plausibility for that particular field. If you for example used wrong characters (e.g. letters in the IP Address configuration or any special characters which are not allowed) or you provided an invalid network configuration then you will receive a message displayed on a red bar saying a type of error and at which feature entry it occurred. The false entry will not be accepted by the system, neither the rest of any new settings you may have configured by that time, therefore you will have to redo the configuration steps again. See an example of a warning message if an error by entering a feature occurs.

**Message:**

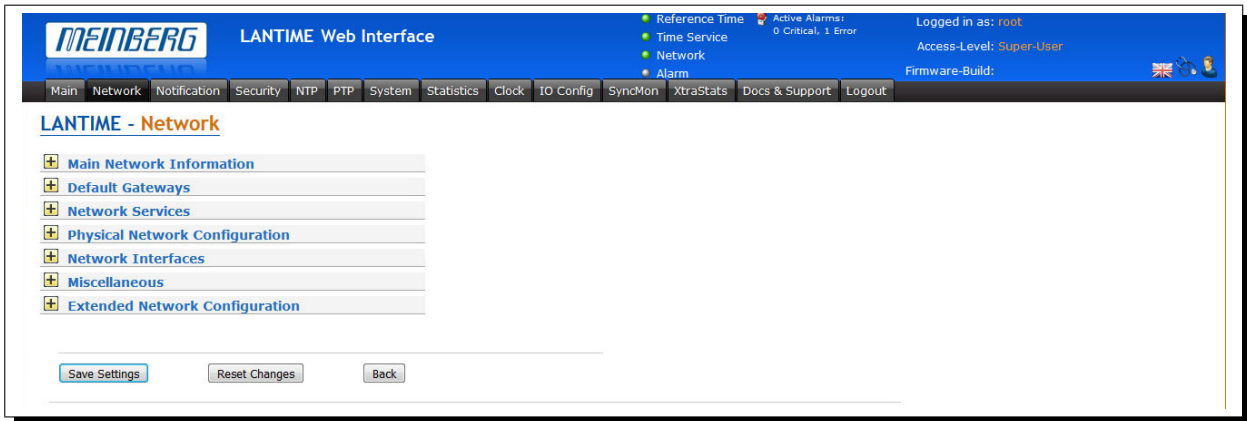
You want to change the time zone of the NTP service to local time. This is a protocol violation and the time server can't be used to synchronize standard NTP clients correctly, which expect UTC time.  
Please press save settings again to confirm the operation.

*Figure: A display of a warning message with a type of error and indication to which feature it belongs*

Allowed signs and special characters which you can use to fill in dialogue boxes you can find in the chapter "Before you Start → Text and Syntax Conventions".

For configuration of the system features now proceed to the dedicated menu which is described in a corresponding chapter.

## 9.1.2 Network



### 9.1.2.1 Main Network Information

**Main Network Information**

Hostname <input style="width: 90%;" type="text" value="timeserver"/>	Domain <input style="width: 90%;" type="text"/>	
Nameserver 1 <input style="width: 90%;" type="text"/>	Nameserver 2 <input style="width: 90%;" type="text"/>	

#### Hostname

The hostname of the LANTIME is a unique name of a computer in a network. Each IP address configured on the LANTIME is assigned to this hostname.

#### Domain

This field is used to configure the network domain name. A network domain name is a text-based label easier to memorize than the numerical addresses used in the Internet protocol (e.g. meinberg.de).

#### Nameserver1

IP Address of the primary DNS Server in the network.

The DNS server is used to resolve IP addresses as well as hostnames in a network.

#### Nameserver2

Here can a alternate Nameserver be defined

### 9.1.2.2 Default Gateways

In this menu you can configure default gateways to be used for IPv4 and IPv6. For a default gateway, a "default" entry is created in the main routing table of a LANTIME. If the LANTIME does not have a direct route or a routing rule to a destination IP, it will always attempt to reach the destination via the default gateway.

**IPv4 Gateway** Configuration of the default IPv4 gateway.

**IPv6 Gateway** Configuration of the default IPv6 gateway.

### 9.1.2.3 Network Services

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

In this submenu you can enable or disable various services for the existing virtual network interfaces. The +/- buttons can be used to select or deselect entire rows or columns in the matrix.

The following service states are possible:

- A service has been activated for at least one virtual interface and is active.
- Service has not been activated for any virtual interface and is therefore stopped.

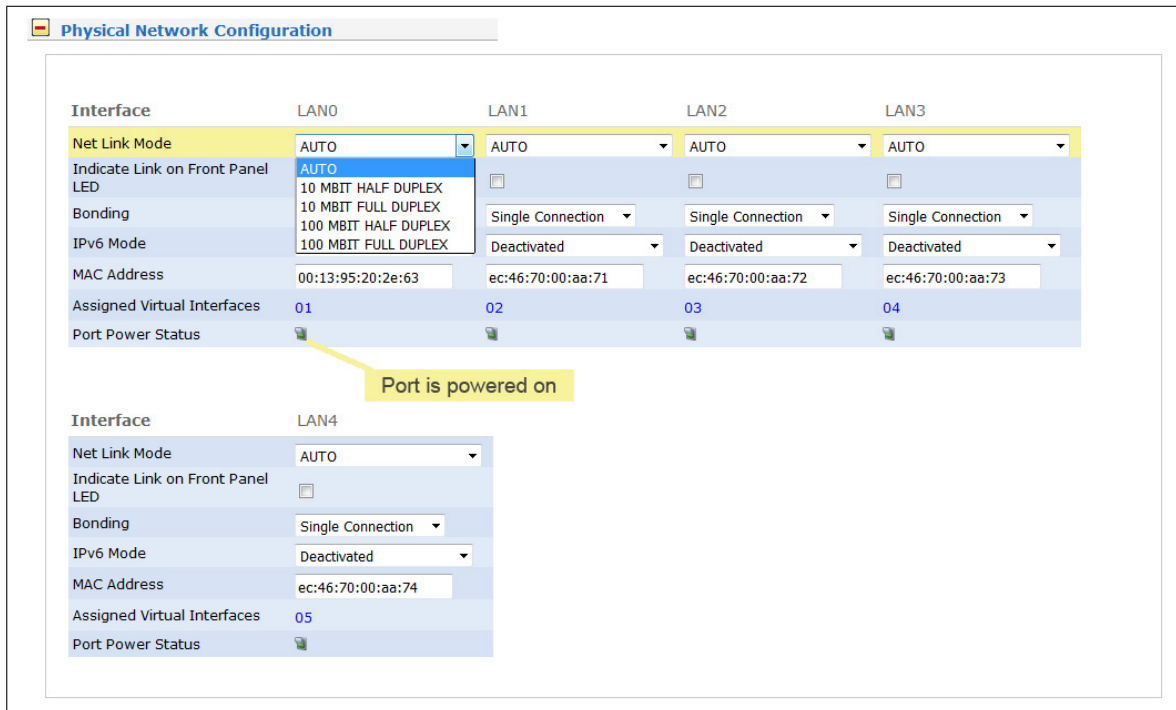
The following services are supported by the LANTIME:

**NTP:** Network Time Protocol, UDP Port 123  
**HTTP:** Hyper Transfer Protocol, TCP Port 80  
**HTTPS:** Hyper Transfer Protocol Secure, TCP Port 443  
**TELNET:** Teletype Network, TCP Port 23  
**SSH:** Secure Shell, TCP Port 22  
**SNMP:** Simple Network Management Protocol, UDP Port 161 / 162 (Traps)  
**FTP:** File Transfer Protocol, TCP Port 20  
**TIME:** Time Protocol, TCP/UDP Port 37  
**DAYTIME:** UDP Port 13  
**FPC:** Emulates the FrontPanel of a LANTIME and maps it in a browser.

**TCP Port 10000** Login to a command line of a Lantime via a webbrowser. TCP port 4200

**WEBSHELL:** Input in the web browser: [IP/HOSTNAME]:4200

### 9.1.2.4 Physical Network Configuration



#### Net Link Mode

Allows you to configure the network connection mode of the interface. You can choose among supported link modes of the respective physical interface.

The default value AUTO (Autonegotiation) can remain unchanged under normal circumstances. Autonegotiation refers to a method which allows two interconnected Ethernet devices to independently negotiate the maximum possible transmission speed and the duplex method and to configure them accordingly.

#### Indicate Link on Front Panel LED

Link status of the network port. As soon as one of the selected network ports has no link, this status will be indicated by a red "Network" LED on the front panel and the "Network Link Down" event will be reported. If a network link is available on all selected ports, the "Network" LED on the front panel will light up green.

#### Bonding

Here, 2 or more physical network ports can be grouped into a bond (group). The LANTIME supports the bonding modes "Active - Backup" and "LACP". The mode to be used can be selected in the submenu "Network → Miscellaneous → Bonding-Mode". For more information about how the two modes work, see the "Miscellaneous" submenu.

#### IPv6 Mode

Activation or deactivation of the IPv6 protocol.

#### MAC Address

Media Access Control, shows the MAC address of the given physical interface.

#### Assigned Virtual Interfaces

Indicates which virtual interfaces are assigned to the given physical interface.

#### Port Power Status

This feature is available in IMS systems, where several physical interfaces can be available. The port power status is an indicator if a particular physical interface is powered on or off.

### 9.1.2.5 Network Interfaces



In this menu the virtual interfaces of the LANTIME are managed. Up to 99 virtual interfaces can be assigned to the available physical ports. The name of the virtual interface consists of a consecutive number of a physical interface and the number of a virtual interface (starting with zero).

```
Physical Interface :: lan0
Number of the virtual interface :: 2
```

The example above shows a configuration in which a total of three virtual interfaces are assigned to the physical interface lan0, namely lan0:0, lan0:1 and lan0:2.

In the case of an active bond, the physical interface is replaced by the name of the bonding group, for example Bond0: 0.

#### Add interface

With this button a new virtual interface can be created. The new interface is assigned by default to the physical port lan0 and is added at the end of the row of the existing virtual interfaces. The assignment can be changed in the "Miscellaneous" tab.

#### Submenu IPv4:

In this submenu the IPv4 parameters can be configured or the current configuration given by the DHCP server can be displayed.

**TCP/IP address:** IPv4-Address of the given interface.

**Netmask:** Configuration of the subnetmask for the given interface.

**Gateway:** Configuration of an interface-specific gateway. This setting must be made only if the IP of the interface is NOT in the same subnet as the default gateway and the cross-network traffic in the subnet should be enabled via the gateway.

**Enable DHCP-Client:** With this setting a DHCP client can be activated for the automatic assignment of the network configuration by a DHCP server.

#### Submenu IPv6:

In this menu the IPv6 parameters can be configured or the configuration given by a DHCP server can be displayed.

**TCP/IP address:** Ipv6-Address of the given interface

**Enable DHCP-Client:** With this setting a DHCPv6 client can be activated for the automatic assignment of the network configuration by a DHCPv6 server.

#### Submenu Misc:

**Assigned Interface:** Determines which physical network is associated with the currently selected virtual interface.

**"Virtual Interface" Delete Button:** Deletes the currently selected virtual interface.

- MAC Address:** Displays the MAC address of the assigned physical network port
- Label:** Individual text-description of the interface (alias).
- Submenu VLAN:**
- Enable VLAN Option:** Activation of the tagged VLAN function for the selected virtual interface.
- VLAN-Tag (0-4094):** VLAN tags from 0-4094 can be entered here. The selected tag is inserted into the data area of an Ethernet packet.
- Priority:** PCP (Priority Code Point). Sets the priority of an Ethernet frame. Priorities can be set between a low priority, value 1 and a high priority, value 7.
- The Priority value 0 corresponds to the Best Effort.

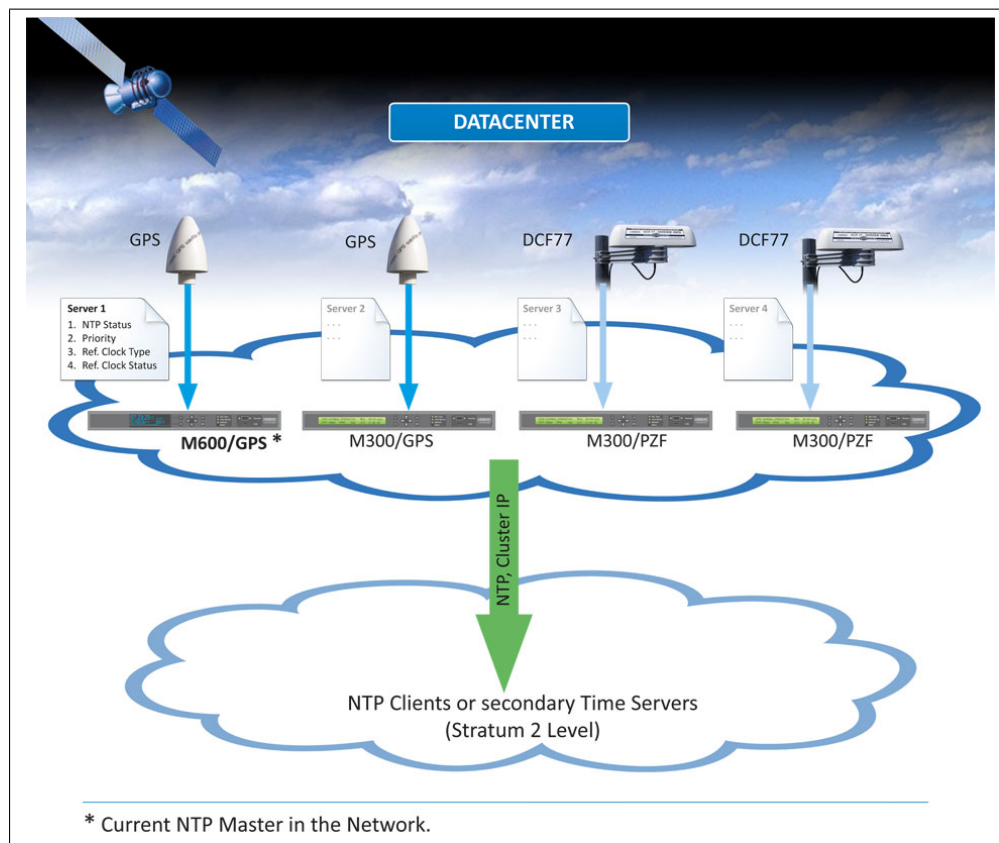
**Submenu Cluster:**

The Cluster mode is a method for providing redundant time synchronization by grouping (clustering) multiple LANTIME NTP servers. Within this group, the participating NTP servers continuously exchange status and quality information with each other. The status information is compared among each other and by a special algorithm a decision is made, which of the NTP servers should act as a current MASTER in the network. The rest of the group acts as SLAVE and stays passive as a backup. If the current master loses its synchronization source or any other failure occurs, another NTP server from the cluster takes over the master role. The current master responds to requests from NTP clients via a common cluster IP. Even if the master is replaced by another NTP server, this IP does not change.

The configuration of a NTP cluster is useful if at the side of NTP clients only one IP address for an external NTP server can be configured and redundancy is still required.

The current master is selected according to the following parameters in this order:

1. NTP status (sync, not sync);
2. Priority (configurable by the user, the lowest value has the highest priority, default = 0);
3. Ref-Clock Type - GNSS receivers such as GPS have the highest rating;
4. Ref-Clock Status (sync, not sync).





### 9.1.2.6 Cluster Configuration

The screenshot shows the 'Network Interfaces' configuration window. At the top, there is a tab for 'Interface 01 - lan0:0' with sub-tabs for 'IPv4', 'IPv6', 'Misc', 'VLAN', and 'Cluster'. The 'Cluster' tab is active, displaying the following settings:

- Enable Cluster Option:** A checkbox that is currently unchecked.
- Mode:** Radio buttons for 'Multicast' (selected) and 'Unicast'.
- TCP/IP address:** An empty text input field.
- Netmask:** An empty text input field.
- Priority:** A dropdown menu set to '0'.

**Enable Cluster Option:** The cluster function can be activated via this selection box.

**Mode:** The cluster members can share their status information either via multicast or unicast messages. For multicast, a cluster multicast address 239.192.0.1 is used by default. This setting can be changed in the menu "Network → Miscellaneous". In addition, the network port which is used for the cluster communication can be changed there. By default, port 7000 is used for the cluster messages.

**TCP/IP Address:** IP address of the NTP cluster interface. The same cluster IP needs to be configured on all cluster members. It is recommended to configure a cluster IP in the same subnet as the corresponding virtual interface.

**Netmask:** Netmask Configuration for the cluster interface.

**Priority:** The priority set here is taken into account when the MASTER is determined by the cluster algorithm. The lowest value has the highest priority.

Example configuration for a multicast cluster:

The screenshot shows the configuration page for 'Interface 01 - lan0:0' with the 'Cluster' tab selected. The 'Cluster' section is expanded, showing the following settings:

- Enable Cluster Option:
- Mode:  Multicast  Unicast
- TCP/IP address: 172.27.80.101
- Netmask: 255.255.0.0
- Priority: 0

Example configuration for an unicast cluster:

The screenshot shows the configuration page for 'Interface 01 - lan0:0' with the 'Cluster' tab selected. The 'Cluster' section is expanded, showing the following settings:

- Enable Cluster Option:
- Mode:  Multicast  Unicast
- Other IPv4-Member: 172.27.80.51, 172.27.80.52
- TCP/IP address: 172.27.80.101
- Netmask: 255.255.0.0
- Priority: 0

In the Unicast cluster, the IP addresses of the cluster members must be entered in the "Other IPv4 Member" field.

### 9.1.2.7 Miscellaneous

#### Cluster Port:

Configuration of a free network port for the cluster communication. Per default this port is set to 7000.

#### Cluster Multicast Address:

Configuration of the cluster multicast address. Via this address, LANTIME cluster members exchange their status messages if Multicast mode is selected.

#### DSCP NTP Classification:

DSCP = Differential Service Code Point. DSCP is generally a method for prioritizing the traffic via IP. On the LANTIME, this setting allows the NTP packets to be assigned to a certain traffic class. The information about the traffic class is inserted into a header of a IPv4 packet. Routers can evaluate this information and handle the NTP packets as prioritized.

#### Bonding-Mode:

In the menu "Network → Physical Network Configuration", two or more physical network ports can be grouped into a bond (group). The Bonding Mode is used to configure either the "ACTIVE BACKUP" or the "LACP" mode (Link Aggregation Control Protocol), which are supported on the LANTIME.

#### ACTIVE-BACKUP:

One physical interface in the bonding group acts as an "active slave". All network traffic of a LANTIME Bond runs through this interface. The other physical interfaces in the bonding group are passive. In case the current active interface loses the network connection, the passive interface seamlessly takes over. Even the MAC address of the network port remains unchanged.

LACP: LACP (802.3ad) allows a combination of multiple physical connections to a logical one. This results in a load sharing and, in addition, increases the safety in case of a failure compared to "Active Backup". It is important that other connected network devices also support LACP and the network ports are configured accordingly.

### 9.1.2.8 Extended Network Configuration

In the Extended Network Configuration, a bash script can be edited, which is executed automatically each time the LANTIME is rebooted or a network-related configuration changes.

### 9.1.2.9 PRP Configuration

PRP stands for Parallel Redundancy Protocol and is defined in the standard IEC 62439-3 since 2010. PRP is Layer-2 based and has been developed for computer networks which are in need of a reliable solution regarding high availability and operational functionality. A LANTIME with two or more interfaces, running firmware 6.22.001 or higher, has the ability to act as a DAN ("Dual Attached Node" - a device which is connected to both redundant networks).

#### Configuring the LANTIME

The LANTIMEs PRP configuration is done through the webinterface using the manual configuration. Open the manual network configuration of the LANTIME this way: "System → Services and Functions → Manual Configuration → Network Configuration"

Depending on the physical interfaces you want to configure for PRP, you have to search for the specific sections in the file. For this example, we will configure LAN1 ( → [PHYSICAL INTERFACE 1]) and LAN2 ( → [PHYSICAL INTERFACE 2]) to a particular PRP group. The configuration below is showing a default configuration of the physical interfaces of a LANTIME.

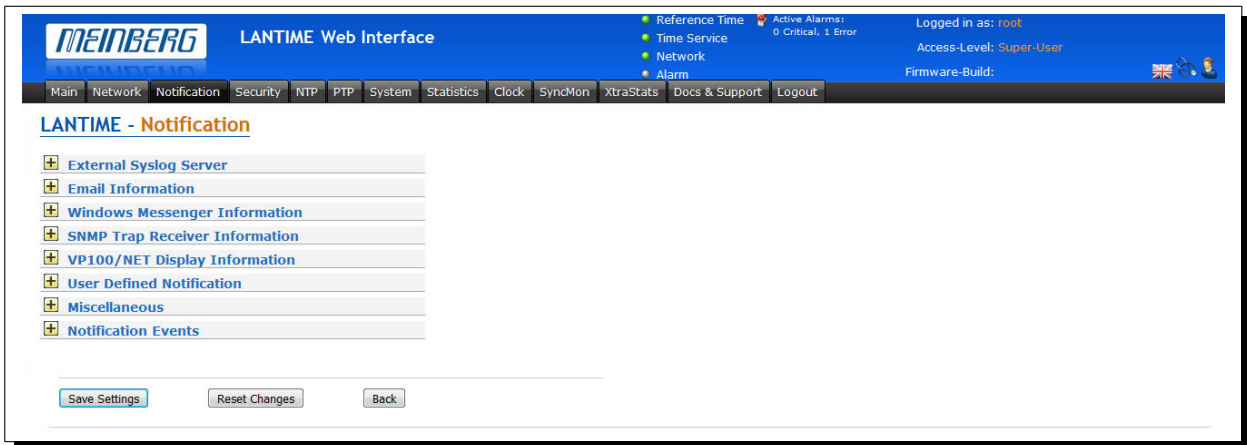
```
[PHYSICAL INTERFACE 1]
MAC-ADDRESS = ab:cd:ef:00:11:22
NET-LINK-MODE = AUTO
BONDING =
INDICATE-LINK = OFF
SUPPORTED-MODES = AUTO 10HD 10FD 100HD 100FD
IPV6-MODE = DEACTIVATED
IMS-SLOT-NUM = 0
POWER-OFF = NO
PRPGROUP = -

[PHYSICAL INTERFACE 2]
MAC-ADDRESS = ab:cd:ef:33:44:55
NET-LINK-MODE = AUTO
BONDING =
INDICATE-LINK = OFF
SUPPORTED-MODES = AUTO 10HD 10FD 100HD 100FD
IPV6-MODE = DEACTIVATED
IMS-SLOT-NUM = 0
POWER-OFF = NO
PRPGROUP = -
```

The PRPGROUP parameter is responsible for the PRP configuration of the LANTIME. By default, PRP is deactivated, which is indicated with a "-" as value. In order to activate PRP on LAN1 and LAN2, just change the value from "-" to a single digit. This value has to be configured on all physical interfaces, which shall run in the same PRP group. After editing the file, press "Save Settings". You will be forced to confirm a message, which gives you a hint that you have changed a configuration file manually.

Please reload the configuration by confirming with "OK". It is not allowed to configure a Bonding on an interface where PRP is already running. On the other hand do not configure PRP on an interface, which is assigned to a Bond.

## 9.1.3 Notification



### 9.1.3.1 External Syslog Server

All information which is written into SYSLOG (/var/log/messages) on the LANTIME, can also be forwarded to a remote server.

#### Syslog-Adress(s):

You can enter up to 2 external Syslog Servers via the webinterface. As standard, the reachability of the Syslog Server is checked via Ping/ICMP. If the registered Syslog Server cannot be reached, it will not be entered into the Syslog configuration file /etc/syslog-ng/syslog-ng.conf. In case ICMP is not allowed in the network, due to firewall regulations, you can switch off the pingcheck via the manual network configuration. To proceed navigate as described down below:

"System Page → Services and Functions → Manual Configuration → Network Configuration": Enter the value "NO" for the Parameter "SYSLOGPINGCHECK" and save the new settings:

**Warning:**  
Use the manual configuration only if you are a qualified administrator who is knowledgeable about the system.

**Edit Network Configuration Manually:**

```
[GENERAL CONFIGURATION]
HOSTNAME=timeserver
DOMAINNAME=
IPV4GATEWAY=172.28.0.1
IPV6GATEWAY=
DSCP_NTP=0
CLUSTER_REFRESH_MULTICAST_JOIN=NO
CLUSTER_REFRESH_INTERVAL=0
CLUSTER_MULTICAST_ADDRESS=239.192.0.1
CLUSTER_PORT=7000
BONDING-MODE=ACTIVE-BACKUP
SYSLOGLEVEL=emerg
SYSLOGPROTOCOL=UDP
SYSLOGPORT=0
SYSLOGPINGCHECK=NO
```

**Minimum Log Level:**

Log Level Configuration

**Transport-Protocol:**

Transport - Protocol Configuration:

UDP - connectionless transmission

TCP - connection oriented

**Port:**

Configuration of the network port which is to be used. As default, IANA has registered port 514 for syslog messages.

### 9.1.3.2 Email Information

The LANTIME is able to inform about certain system events via e-mail. In the menu "Email Information" you can make the necessary settings. In the submenu "Notifications" you can select the system events, for which the LANTIME has to send out a notification e-mail.

The screenshot shows the 'Email Information' configuration page. It includes the following elements:

- Recipient:** Text input field.
- Sender:** Text input field.
- Smarthost:** Text input field.
- Port:** Text input field with the value '25'.
- Enable Authentication:** A checkbox that is currently unchecked.
- User:** Text input field.
- Password:** Text input field.
- Additional Email Recipient:** Text input field with an 'Add' button next to it.
- Table:** A table with two columns: 'Additional Email Recipients' and 'Options'. A blue bar at the bottom of the table contains the text 'Currently no additional Email recipients configured'.

- Recipient:** E-mail of the desired recipient.
- Sender:** Address of the sender.
- Smarthost:** To send the e-mails you require a smarthost (relay-server). Please enter the server address here.
- Port:** Network port configuration. Default setting is 25, because the SMTP (Simple Mail Transfer Protocol) uses TCP Port 25 as standard.
- Activate Authentication:** Many mail servers require a valid authentication. (Checkbox) Please check mark the box to activate it.
- Username/ Password:** Please enter a valid access for the e-mail server.
- Additional E-mail Recipients:** Configuration of additional e-mail recipients.

### 9.1.3.3 SNMP Trap Receiver

The LANTIME is able to inform about certain system events with the help of SNMP traps. In the menu "SNMP Trap Receiver" you can configure up to 4 trap receiver. In the submenu "Notifications" you can select the system events, for which the LANTIME has to send an SNMP Trap.

**SNMP Trap Receiver Information**

SNMP Trap Receiver 1  Community

Version

SNMP Trap Receiver 2  Community

Version

SNMP Trap Receiver 3  Community

Version

SNMP Trap Receiver 4  Community

Version

Number of Retries  Timeout (seconds)

**SNMP Trap Receiver:** IP address or hostname of the SNMP trap receiver.

**Community:** SNMP Read Community of the Trap Receiver.

**Version:** SNMP version to use.

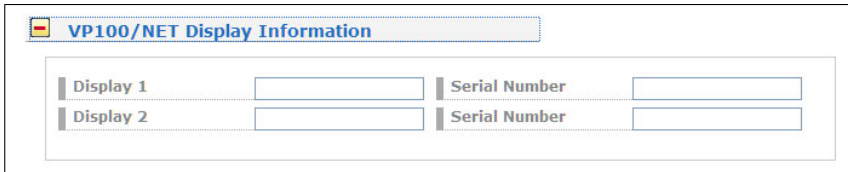
**Number of Retries:** Specifies the value a lantimes retries to send a Trap.

**Timeout:** Connection timeout value.



### 9.1.3.4 VP100/NET Display Information

The Meinberg VP100 / 20NET network display is used to display the time and date. This display has an integrated network card and a SNTP client. The time is taken from any NTP time server via the NTP protocol and thus the internal clock is adjusted. This display can also display any characters as scrolling text. All LANTIME alarm messages can be displayed as text messages on the display. In the submenu "Notifications", you can select the system events which are to be sent to the display by the LANTIME. A message appears three times in succession as a scrolling text on the display.



Display	IP Address	Serial Number
Display 1	<input type="text"/>	<input type="text"/>
Display 2	<input type="text"/>	<input type="text"/>

**Display:** IP Address of the network display.

**Serial number:** You have to enter the correct serial number of the display here.  
The serial number is displayed after pressing the red SET button four times.

### 9.1.3.5 Notifications

#### User-defined Notifications

A freely definable script which should be executed when certain system events occur, can be created via the "User-defined notification" menu item. This script can be viewed and edited via the button "Notification Edit". Upon delivery this script contains a few comments:

```

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

```

In the submenu "Notification Events", you can select the system events on which the script should be executed.

#### Miscellaneous

The screenshot shows a configuration window titled "Miscellaneous". Inside, there are two settings:

- Enable Heartbeat**: A checkbox that is currently checked.
- Heartbeat Interval (m)**: A dropdown menu with the value "1" selected.

The network heartbeat describes a function, with which the LANTIME cyclically sends an SNMP trap to the configured SNMP trap receivers to report itself as "alive" and "active".

The SNMP OID of the trap is: 1.3.6.1.4.1.5597.30.3.0.88 (mbgLtNgTrapHeartbeat).

**Activate Heartbeat:** The heartbeat can be activated via this checkbox

**Heartbeat-Intervall (m):** Heartbeat interval in minutes.

### 9.1.3.6 Notification Events

The "Notification Events" submenu provides an overview of all system events that may occur during LANTIME operation. The checkboxes can be used to configure external alarms for each event. The following information channels are available:

Event	Type	Status	Triggered	Triggers									
				EMAIL	WMAIL	SNMP	DISP	USER	ALED	RELAY IO3			
										REL1	REL2	REL3	
Normal Operation	Info			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP Not Sync	Error		Last: Mon Oct 23 13:49:59 2017	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP Sync	Info		01h 26m 48s ago	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP Stopped	Critical			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP Offset Limit exceeded	Error			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTP Offset Limit OK	Info			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
System Reboot	Action		Last: Mon Oct 23 13:49:36 2017	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLK1 Not Responding	Critical			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLK1 Not Sync	Error			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
CLK1 Sync	Info		01h 27m 08s ago	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IMS Error	Error			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IMS OK	Info		Last Event: Mon Oct 23 13:49:21 2017	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Trusted Source OK	Info		Last Event: Mon Oct 23 13:49:43 2017	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Trusted Source Error	Error			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Autorepeat Event: Never

Max. Number of Repetition: 0

**EMAIL:** Sends an e-mail based on the e-mail configuration (see chapter "E-mail Information")

**SNMP:** Sends an SNMP Trap to the configured SNMP Trap (see chapter "SNMP Trap Receivers")

**DISP:** Shows the notifications on the configured network displays (see chapter "VP100/NET Display Information")

**USER:** Activates the user-defined script (see chapter "Notifications")

**ALED:** When the event occurs, the alarm LED of the LANTIME will light up

**RELAY:** When the event occurs, the error relay at the LANTIME is set to ERROR



1) Information; 2) Alarm; 3) Last change

**Automatic Event Repeat:** An interval can be configured, with which notifications are sent again.

**Max. Number of Repetitions:** The number of repetitions can be limited by this parameter.

## 9.1.3.7 Overview for all Events

Event	Severity Levels (according to X.733)	Description
Normal Operation	Clearing event	Indicates normal operation of the LANTIME
NTP Not Sync	Warning or Critical	NTP Service is not sync -> NTP Messages
NTP Sync	Clearing event	NTP service is successfully synchronized
NTP Stopped	Critical	NTP service stopped -> NTP Messages
System Reboot	Info event	The system has restarted
CLK[NR] Not Responding	Warning or Critical	Receiver module is not responding -> Ref. Clock Messages
CLK[NR] Not Sync	Warning or Critical	Receiver module is not sync -> Ref. Clock Messages
CLK[NR] Sync	Info event	Receiver module is synchronous to its time source
Antenna Faulty	Critical	No antenna or sufficient signal was detected -> Ref. Clock Messages
Antenna Reconnect	Clearing event	Antenna / signal was detected by the LANTIME
Antenna Short Circuit	Critical	Short circuit at the antenna connection -> Ref. Clock Messages
Device Configuration Changed	Info event	Software configuration of the LANTIME has been changed
Leap Second Announced	Info event	A leapsecond was announced
SHS Time Limit OK	Info event	The set SHS time limit value has not been exceeded

Table: All Notification Events

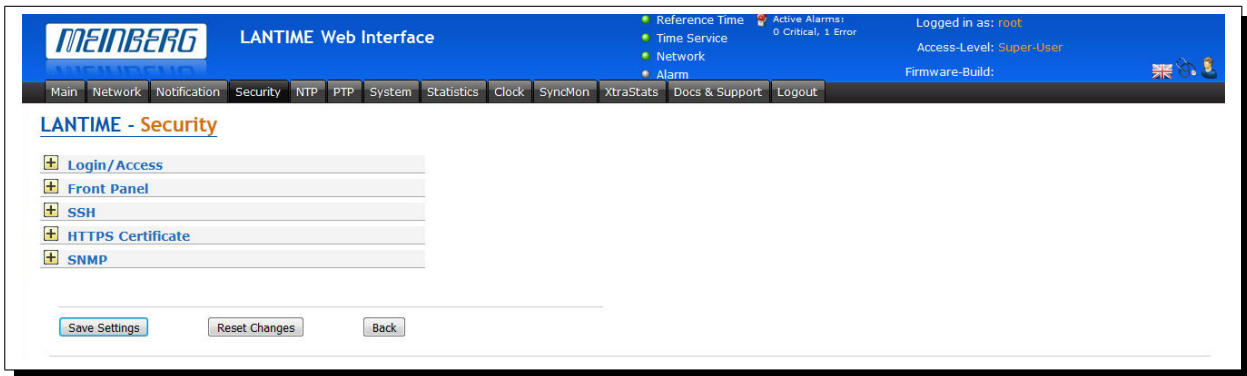
Event	Severity Levels (according to X.733)	Description
SHS Time Limit Warning	Warning or Critical	The set threshold for an SHS warning has been exceeded
SHS Time Limit Error	Critical	The set threshold for an SHS error has been exceeded -> <a href="#">SHS Configuration</a>
Power Supply Failure	Critical	Error detected on a power supply -> ??
Power Supply OK	Info event	Power supply ready for operation
Sync Monitor	Warning	Sync Monitor limits were exceeded
XMR Limit Exceeded	Warning	Set MRS limits have been exceeded -> <a href="#">Ref. Clock Messages</a>
XMR Reference Disconnected	Critical	A configured MRS time source is no longer available -> <a href="#">Ref. Clock Messages</a>
XMR Reference Detected	Info or Warning	A configured MRS time source is available
XMR Reference Changed	Info or Warning	The active MRS source has changed
Network Link Down	Critical	No network connection on one of the LAN ports -> <a href="#">Network Messages</a>
Network Link Up	Clearing event	Network connection detected on the LAN port
PTP Link Down	Critical	No network connection on the PTP network port
PTP Link Up	Clearing event	Network connection detected on the PTP network port
PTP State Changed	Info or Warning	The current PTP status has changed

Table: All Notification Events

Event	Severity Levels (according to X.733)	Description
PTP Error	Critical	A PTP error has been detected -> <a href="#">PTP Global Status</a>
Low System Resources	Warning or Critical	Low system resources detected
Sufficient System Resources	Clearing event	System resources restored
Fan Failure	Critical	An error has been detected on a fan -> <a href="#">Miscellaneous Messages</a>
Fan OK	Info event	No mistakes on installed fans
Certificate Expired	Info or warning	HTTPS certificate has expired -> <a href="#">HTTPS Certificate</a>
Oscillator Adjusted	Clearing event	Internal oscillator runs stably and is completely adjusted
Oscillator Not Adjusted	Info event	Internal oscillator is not adjusted -> <a href="#">Ref. Clock Messages</a>
Cluster Master Changed	Warning	The master of a LANTIME NTP cluster has changed -> <a href="#">Menu: Network</a>
Cluster Falseticker detected	Warning	An NTP falseticker was detected in the cluster compound
Cluster Falseticker cleared	Clearing event	Previously detected cluster falseticker is back in order
IMS Error	Critical	An error has been detected on an IMS module -> <a href="#">Miscellaneous Messages</a>
IMS OK	Clearing event	IMS module is error-free
NTP Offsetlimit exceeded	Warning or Critical	Maximum NTP offset value has been exceeded -> <a href="#">Sync Monitoring</a>
NTP Offsetlimit OK	Info event	Maximum NTP offset not exceeded -> <a href="#">Sync Monitoring</a>

Table: All Notification Events

## 9.1.4 Security

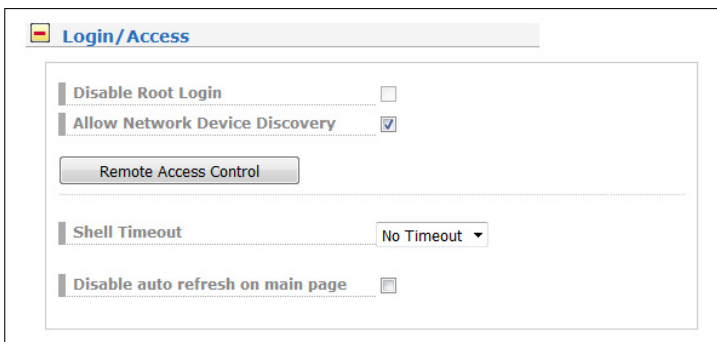


This page allows to configure access restrictions and snmp. It also provides the functionality to handle SSH keys and the HTTPS certificate.

If unsure of required values please contact the network security administrator and provide these parameters.

### Login/Access

The "Login" menu allows you to set general security settings for the login behavior of the LANTIME.



#### Disable Root Login:

This function can only be activated by an admin user or by a super user. If this function is active, the "root" user can no longer log on to the LANTIME.

#### Allow Network Device Discovery:

When this function is activated, the AVAHI service is started on the LANTIME, which is used to locate devices and services in a local network, using a multicast mode of communication. The automatic network discovery is per default activated.

**Remote Access Control:**

In this configuration file, you can configure an access control for the LANTIME web interface, based on the IP protocol. In this file you can enter the IP addresses, which should be allowed to access the web interface. Once the first entry has been made, access to all other clients is automatically prohibited. Individual client IPs or entire subnets can be configured.

**Example for IPv4:**

```
Host: 172.16.1.1
Subnet: 172.27.*.*
```

**Example for IPv6:**

```
Host: 2001:610::12/29
Subnet: 2001:610::* /29
```

**Shell Timeout:**

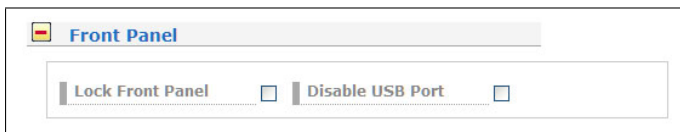
Defines a timeout in seconds. After expiration of this period without any user interaction, the current session on the command line will be terminated for the logged-in user.

**Disable auto refresh on main page:**

Prevents automatic reloading of the web interface in 60 seconds, as long as a user is in the main LANTIME web interface.

**Front Panel:**

Contains general security settings for the front panel of the LANTIME.

**Lock Front Panel:**

When the function is activated, the front panel of a LANTIME is disabled.

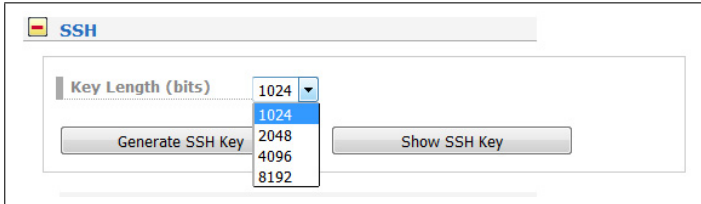
**Disable USB Port:**

After activating the feature, the USB port of a LANTIME at the front panel is deactivated and connected USB sticks can not be detected.



### 9.1.4.1 SSH - Secure Shell

Via "Secure Shell Login" (SSH) it is possible to establish a secured connection to the LANTIME. All data is encrypted during the transmission over Ethernet. To use this service, SSH must be enabled on each interface in the network settings (read also the configuration chapter 9.1.2.3 "Web GUI → Network → Network Services").

**Key Length (Bits):**

Determines the key length for a new key to be generated.

**Generate SSH Key:**

Generates a key pair, consisting of a public and private key, in configurable length.

**Show SSH Key:**

You can use this button to display the public SSH keys of a LANTIME.

### 9.1.4.2 HTTPS Certificate

HTTPS is a 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 a 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 is changed.

**Note:** Per default there is a self-signed certificate installed on the LANTIME which is not signed by a Certificate Authority (CA). Therefore some web browsers will state that the connection is not secure. If you want to install a certificate which was signed by a trusted Certificate Authority the "Upload SSL Certificate" button can be used. More details on this in the following instructions.

**Generate SSL Certificate:**

Allows to create a new self-signed SSL certificate.

**Show SSL Certificate:**

Review the currently installed SSL certificate.

**Download SSL Certificate:**

Allows to download the currently installed SSL certificate.

**Generate Certificate Request:**

Allows to generate a Certificate Signing Request (CSR) which can be sent to a Certificate Authority in order to apply for a signed certificate.

**Upload SSL Certificate:**

Allows to upload a certificate which was signed by a trusted Certificate Authority. 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.

### 9.1.4.3 Uploading certified Multi-Level / chained Certificates

Steps below require an SSH access to your time server.

In addition to SSL certificates, also multi-level / chained certificates are supported. In this case, the private key with its corresponding certificate and the certificate chain are divided into two files, which are both in the 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 and the certificate enclosed between BEGIN and END CERTIFICATE.

The CA-file on the other hand contains just the certificate chain, where each single intermediate certificate is enclosed between BEGIN and END CERTIFICATE line as shown above.

The PEM file that contains the private key and the LANTIME's web server certificate should be copied manually to `/etc/https.pem` and the intermediate CA(s) 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, otherwise the web server cannot start automatically.

#### 9.1.4.4 SNMP

The Simple Network Management Protocol (SNMP) is used in network management systems to monitor status of devices. SNMP works by querying "Objects". An object is simply something that we can gather information about a network device. The so called management information base (MIB) is a file which contains all objects that can be managed through SNMP.

The Meinberg SNMP MIB Files can be downloaded on the "System" page → Services and Functions → Download SNMP MIB". The files named "MBG-SNMP-ROOT-MIB.mib" and "MBG-LANTIME-NG-MIB.mib" need to be used to monitor a LANTIME V6 system.

(see also configuration chapter 9.1.8.2 "Web GUI → System → Services and Functions")

By default the SNMP service is not activated on a LANTIME V6 system. The service can be activated on each interface at the "Network page → Network Services".

(see also configuration chapter 9.1.2.3 "Web GUI → Network → Network Services")

The different SNMP configuration parameters are described below:

#### Activated Protocol Versions:

Configuration of the SNMP protocol version. The following options can be selected: "V1/V2 only", "V3 only", "V1/V2/V3".

## V1/V2 Parameter

### Read Community:

The read community is only used for SNMP versions V1 and V2. It is like a user id or password that allows access to the LANTIME SNMP objects. The SNMP Monitoring system sends the read community string along with all SNMP requests. If the community string is correct, the LANTIME responds with the requested information. If the community string is incorrect, the LANTIME simply discards the request and does not respond.

### Write Community:

The write community is only used for SNMP versions V1 and V2. It is like a user id or password that allows access to the LANTIME SNMP objects. The SNMP Monitoring system sends the write community string along with all SNMP-SET commands. If the community string is correct, the SNMP-SET command is executed. If the community string is incorrect, the SNMP-SET command is not executed.

## V3 Parameter

### Security Name:

SNMP V3 User name

### Security Level:

Messages can be sent unauthenticated, authenticated, or authenticated and encrypted by setting the Security Level to use:

noAuthnoPriv – unauthenticated and unencrypted

authNoPriv – authenticated and unencrypted

authPriv – authenticated and encrypted

### Engine ID:

Within an administrative domain, a SNMP V3 Engine ID is a unique identifier of an SNMP engine. A string with a maximum of 27 characters can be entered here. The string is used to generate the hex engineID by using the text format scheme described in RFC3411. If for example the string "hello" is configured as engineID, the generated hex engineID would be 800015dd0468656c6c6f

- 15dd is the hexadecimal representation of the Meinberg enterprise ID 5597
- 04 is an indicator that the text format scheme is used to generate the engine ID
- 68656c6c6f is the hexadecimal representation of the string "hello"

V3 Parameter	
Security Name	root
Security Level	noAuthNoPriv ▼
Engine-ID	hello
Rights	Readonly Access ▼

**Rights:**

Configuration of the access level (Read access or Read/Write access).

**Authentication Protocol:**

The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).

**Authentication-Passphrase:**

User passphrase that must be at least 8 characters in length.

**Privacy Protocol:**

The protocols used for Encryption are DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

**Privacy Passphrase:**

A passphrase which is used when encrypting packets. It must be at least 8 characters in length.

### 9.1.4.5 SHS Configuration

SHS is the abbreviation for Secure Hybrid System and is available on LANTIME systems with two reference clocks. When the SHS mode is enabled only the currently active clock is used for passing the timing signal on to the NTP service, the other clock is indicated as "no select" and used only for measuring and comparing a time difference between both receivers.

In this respect SHS is different from a redundant mode. In redundant mode a switching unit switches between one or the other clock, depending on its availability and sync status and the active clock passes the timing signal on the NTP service.

SHS mode takes care for a secure operation and it steps into action when a time difference between both receivers exceeds a configurable time limit.

When this happens the alarms will be triggered and send out via configured notification channels (e.g. SNMP trap, email, syslog message). Besides, the NTP should be stopped in this case too to support the secure operation of the timing service, therefore you have to select "Stop NTP Service on Time Limit Error" at this step.

On the other hand, in IMS Systems with two reference clocks the timing signal coming from the clocks is continuously measured with a RSC card (Redundant Switch Control unit) and compared against each other. The measurements are forwarded to the SHS mode if this is enabled. Similar as in LANTIME systems with SHS, the alarms can be triggered when a difference of the two signals exceeds the configured time limit settings and the NTP service should be configured to stop.

The screenshot shows the 'SHS Configuration' window with the following settings:

- SHS-Mode:** Disabled (dropdown menu)
- Time Limit Warning Level (ms):** 0 (input field)
- Time Limit Critical Level (ms):** 0 (input field)
- Stop NTP Service on Time Limit Error:**  (checkbox)

#### SHS-Mode

The SHS mode can be selectively enabled or disabled via this selection box. If the SHS mode is disabled, no time comparison takes place and the times of both receivers are transferred directly to the NTP service. The NTP service then decides autonomously which time is used for synchronization (redundant mode).

#### Time Limit Warning Level

If the calculated time difference between the two reference clocks exceeds the configured value, the LANTIME generates a "SHS Time Limit Warning" alarm. This alarm can be sent via e-mail or SNMP Trap, if it is configured correspondingly in the Notification settings.

(see also configuration chapter "Web GUI → Notification → [Email Information](#)")

In LANTIME IMS systems with a built-in RSC, the parameter is configured in nanoseconds. For systems without an RSC in milliseconds.

#### Time Limit Error Level (ms)

If the calculated time difference between the two reference clocks exceeds the configured value, the LANTIME generates a "SHS Time Limit Warning" alarm. This alarm can be sent via e-mail or SNMP Trap, if it is configured correspondingly in the Notification settings.

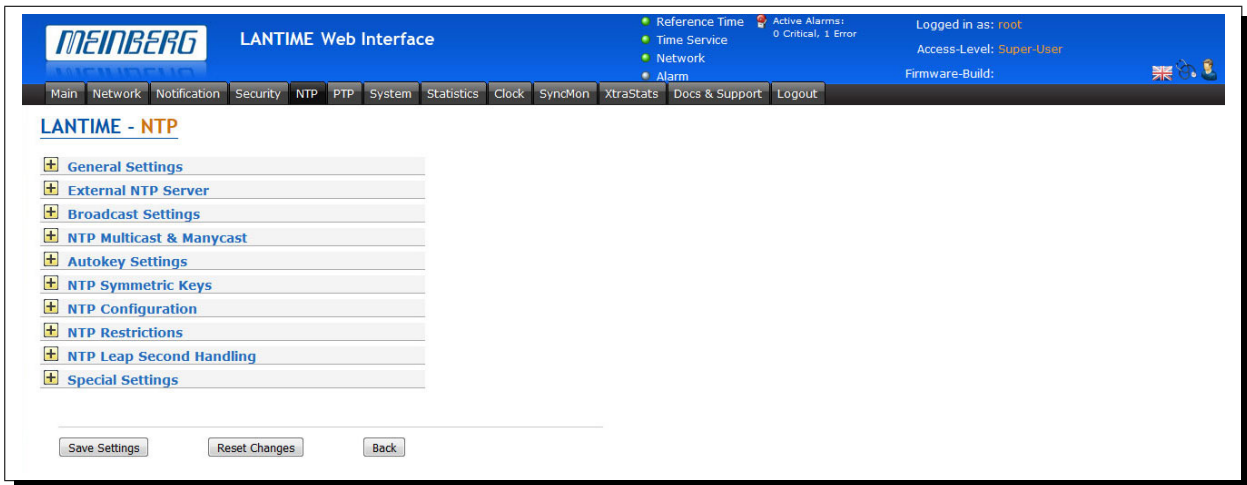
In LANTIME IMS systems with a built-in RSC, the parameter is configured in nanoseconds. For systems without an RSC in milliseconds.

### **Stop NTP Service on Time Limit Error**

Here you can decide if the NTP service is to be terminated at the Critical "TimeLimitError". In this case, requesting NTP clients would no longer receive a response from the time server.

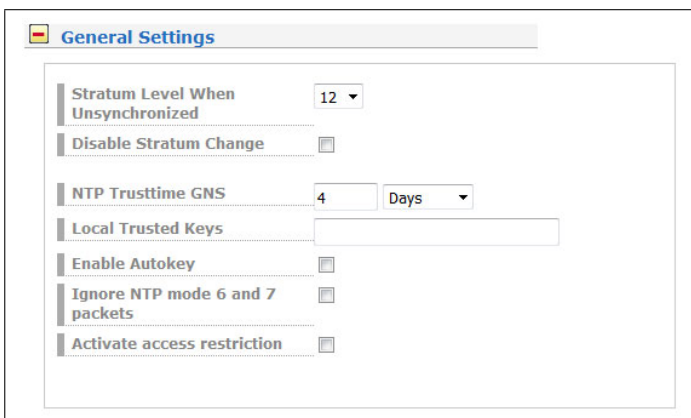


## 9.1.5 NTP



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

### 9.1.5.1 General Settings



#### Stratum Level when Unsynchronized

The stratum value for NTP refers to a distance away from a reference source and not the accuracy. For example, a time server with an internal reference such as GPS or DCF77, internally has a Stratum 0 and is considered from an external network as Stratum 1. The setting "Stratum Level when Unsynchronized" is used to configure the stratum value, by which the server presents itself in the network, when a reference time source is not available. This value does not take an effect until the configured NTP Trusttime for the internal reference clock has expired and no further time sources such as external NTP servers are available.

### Disable Stratum Changes

By activating this operation mode, the server always presents itself (even if asynchronous) as a Stratum 1 server in the network. The "Stratum Level When Unsynchronized" setting will become ineffective.

#### Examples:

- a) A LANTIME, which is synchronized by its internal reference clock such as GPS or DCF77, acts as a Stratum 1 NTP server. If the "Disable Stratum Change" function is activated, the NTP server will act as Stratum 1 server, if the reference clock goes asynchronous and no other time sources are available.
- b) A LANTIME, which is only synchronized by an external NTP server with Stratum 3, acts in a network as Stratum 4 NTP server. If the "Disable Stratum Change" function is activated, the NTP server will still act as Stratum 4 NTP server, even if the connection to the external NTP server is lost.
- c) If NTP of the LANTIME with activated "Disable Stratum Change" function, changes from its internal reference clock to an external NTP server with Stratum 2, the Stratum of the LANTIME will change from 1 to 3.

### NTP Trusttime

This setting defines for how long NTP should "trust" the internal reference clock of a server after this has become asynchronous. The status of an asynchronous reference clock is also called "free running". The accuracy of a "free running" reference clock depends on the type of the integrated oscillator. The trust time should therefore be set dependent on the accuracy of the "free running" reference clock.

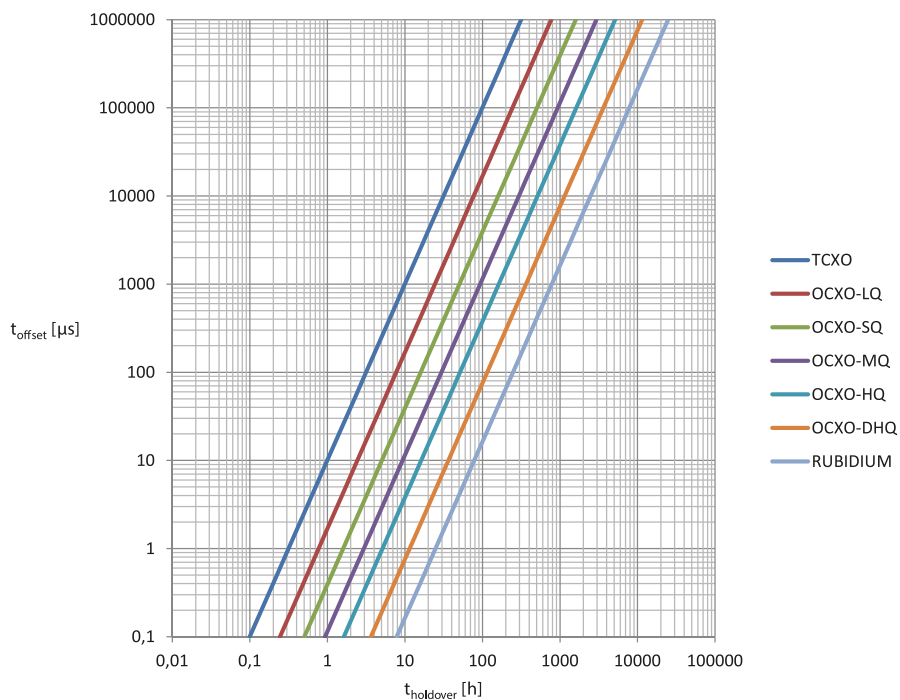


Figure: relation between holdover time (x) and offset (y) by using of built-in Meinberg oscillators

### How do I configure the correct Trusttime in my application environment?

As an example, we now assume that our receiver has a built-in TCXO oscillator. The Trusttime should run out from an offset of 1ms. The graphic shows that this offset is reached after 10 hours of holdover time. Therefore a Trusttime of 10 hours should be configured.

Procedure: First you should find out which oscillator is used. Go to the web interface menu "Monitoring and Management → Clock → Receiver Information → Oscillator Type". Then you can define an offset, from which the NTP should lose its stratum or the trust time.

You can find a list of oscillators available for Meinberg reference clocks here:  
<https://www.meinbergglobal.com/english/specs/gpsopt.htm>

### Local Trusted Keys

In this field, you can enter the IDs of the symmetric keys which shall be used for the authentication. If you have more than one key, the IDs need to be entered with a space to separate them from one another. You can configure the symmetric keys in the submenu "NTP Symmetric Keys" on the NTP page. See "NTP Symmetric Keys" sub chapter for more information.

### Ignore NTP Mode 6 and 7 Packets

This setting cause that internal information, like Access statistics, cannot be queried by other NTP able devices in the network, via the NTP service of the server. The setting does not have any effect on the time synchronization between NTP clients and the server.

By activating this setting the following lines will be written into the NTP configuration of the Server:

```
restrict default noquery
restrict -6 default noquery
restrict 127.0.0.1
restrict -6 ::1
```

### Activate access restriction

By activating this setting the following lines will be written into the NTP configuration of the Server:

```
restrict default noserve
restrict -6 default noserve
restrict 127.0.0.1
restrict -6 ::1
```

These settings cause that the server no longer responds to NTP requests. In the submenu "NTP Restrictions" you can configure a "white list" of client IP addresses or even entire subnets whose requests are allowed to be answered by the server.

### 9.1.5.2 External NTP Server

Via the configuration page you can enter up to 7 external NTP server as backup for the internal reference clock.

#### Server Address:

IP oder Hostname of an external Server.

#### Symmetric Keys:

In this optional field, you can enter the ID of a symmetric key, which is to be used for authentication with the external server.

To carry out with the authentication, we must pay attention to the following:

- a) The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.
- b) Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".
- c) The same key with the same ID must be configured on the external server.

#### Minpoll and Maxpoll:

With these settings, you can set the minimum and maximum polling interval (query cycle) for a given external server. NTP starts with the minimum polling interval and changes step by step to the maximum of the polling interval.

#### Use Iburst:

The iburst activation accelerates the initial synchronization with an external server.

**Particularity LANTIME/MRS:**

With an MRS, the external NTP servers are not written into the NTP configuration of the server. They are queried internally every 32 seconds with the help of an "ntpdate" command. The determined time offset to the internal reference is filtered and sent to the MRS unit.

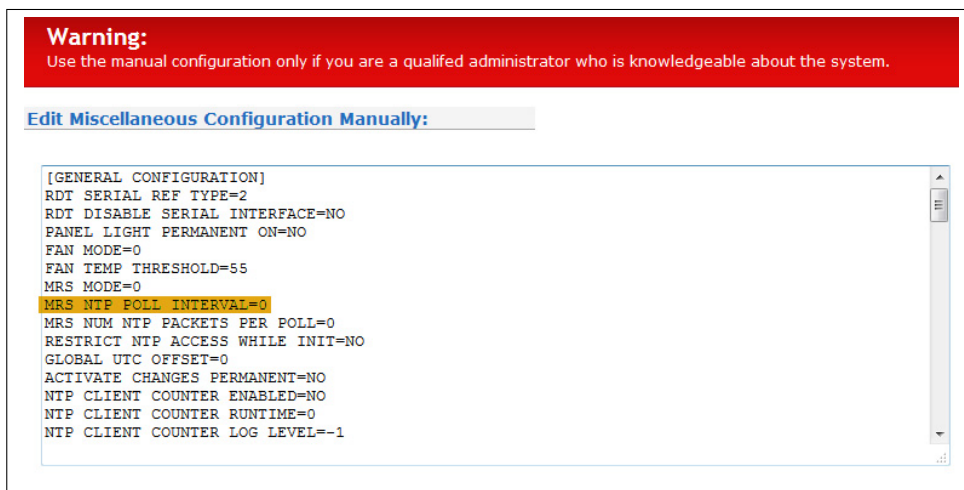
Due to this particularity, the configuration possibilities for external NTP server are different:

Server Address 1	192.168.101.11	Symmetric Key	2	Use Autokey	<input checked="" type="checkbox"/>
Minpoll	Auto	Seconds	Maxpoll	Auto	Seconds
				Use iburst	<input type="checkbox"/>
Server Address 2	192.168.101.13	Symmetric Key		Use Autokey	<input checked="" type="checkbox"/>
Minpoll	Auto	Seconds	Maxpoll	Auto	Seconds
				Use iburst	<input type="checkbox"/>
Server Address 3	192.168.101.13	Symmetric Key		Use Autokey	<input checked="" type="checkbox"/>
Minpoll	Auto	Seconds	Maxpoll	Auto	Seconds
				Use iburst	<input type="checkbox"/>

The parameters Minpoll, Maxpoll and Iburst cannot be configured on a LANTIME/MRS. Regarding the authentication only a symmetric key which is used for all configured external servers, can be configured. It is not possible to use different keys for individual servers.

For a LANTIME/MRS you can adjust the default polling interval of 32 seconds via the manual configuration of the server. To proceed follow this menu navigation:

Web Interface - "System Page → Services and Functions → Manual Configuration → Standard Configuration → Miscellaneous Configuration"



You can use the parameter "MRS NTP POLL INTERVAL" to adjust the polling interval of the external server. As per default this value is set to 0, which means that external are queried every 32 seconds. Values can be set between 1 and 10 and are used as a power of 2. For example if this value is set to 6, this is equal to  $2^6 = 64$  seconds for a polling interval.

Use the parameter „MRS NUM NTP PACKETS PER POLL“ to set the number of NTP queries sent per polling interval. Per default this value is set to 0, which means that 4 packets are sent in a given polling interval. Set a value between 1 and 8, which corresponds to the actual number of packets.

### 9.1.5.3 Broadcast Settings

If the NTP time should be distributed in Broadcast mode in a local network, you can enter a valid broadcast address into this menu. Please note: starting with NTP4 version, the broadcast mode must always be used with authentication.

#### Broadcast Address:

A valid broadcast address of a local network, to which the LANTIME is connected must be entered here.

#### Broadcast Interval:

The interval at which the server sends the NTP packets to the configured broadcast address.

#### Symmetric Keys:

In this field you can enter the ID of a symmetric key, which is to be used for authentication with the NTP clients.

The following must be respected, to make the authentication work:

- a) The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.
- b) Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".
- c) The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client, which is configured as a broadcast client with authentication:

```
keys /etc/ntp.key # Path to the NTP Key File
trustedkey 1 # The Key ID, which is used for the authentication
broadcastclient # This client works as a broadcast client
```

### 9.1.5.4 NTP Multicast and Manycast

The screenshot shows the configuration page for NTP Multicast & Manycast. It contains two main sections:

- NTP Multicast:**
  - Enable Multicast:
  - Multicast Address:
  - Broadcast Interval: Auto (Seconds)
  - Symmetric Key:  Use Autokey:
  - TTL: 127
- NTP Manycast:**
  - Enable Manycast:
  - Manycast Address:
  - Symmetric Key:  Use Autokey:

### 9.1.5.5 NTP Multicast

NTP Multicast offers the possibility to distribute the time by multicast in the network. The Internet Assigned Numbers Authority (IANA) has exclusively allocated the multicast IP address 224.0.1.1 for NTP. Therefore, it is recommended to use this address as a multicast address. However, also other addresses of the multicast address space can be set.

The multicast address space is as follows:

```
Ipv4: 224.0.0.0 -> 239.255.255.255
Ipv6: Every FF00::/8 Address
```

**Multicast Address:** A correct multicast address must be entered here.

**Broadcast Interval:** The interval at which the server sends the NTP packets to the configured broadcast address.

**TTL:** The configured TimeToLive (TTL) value determines how many hops NTP packets can pass in the network. Each network hop reduces this value by 1. When the value reaches zero, the network packet is dropped.

**Symmetric Keys:** For NTP Multicast, an authentication is recommended, but not mandatory. However, if the authentication is configured on the server side, it is also necessary to do so on the client side.

In the field "Symmetric Keys" you can therefore enter the ID of a symmetric key, which is to be used for authentication with the NTP clients.

The following must be respected, to make the authentication work:

- The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.
- Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".
- The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client, which is configured as a multicast client with authentication:

```
keys /etc/ntp.key           # Path to the NPT Key file
trustedkey 1                # The Key ID, which is used for the authentication
multicastclient 224.0.1.1 key 1 # The Client listens on the Multicast Address 224.0.1.1 and
                                # uses the key with ID 1 for authentication
```

### 9.1.5.6 NTP Multicast

NTP Multicast describes the possibility that one or more NTP servers are behind a multicast address. However, contrary to the multicast method, the servers do not send NTP packets periodically to this multicast IP. The Multicast feature is much more a method to automatically reconfigure the NTP service of a requesting client. The NTP service of the client selects up to 3 servers automatically, which seem to be "best" for him. The NTP service then reconfigures itself independently, and establishes a unicast communication with these servers. As with multicasting, it is recommended to use authentication methods.

**Enable Multicast:** It activates the Multicast-Feature

**Multicast Address:** Address field for entering the multicast address (multicast address space)

The Multicast Address Range is as follows:

```
Ipv4: 224.0.0.0 -> 239.255.255.255
Ipv6: Every FF00::/8 Address
```

**Symmetric Keys:** For NTP Multicast, a key method for authentication is recommended, but not mandatory. However, if the authentication method is configured on the server side, it is necessary to do so on the client side.

In the field "Symmetric Keys" you can therefore enter the ID of a symmetric key, which is to be used for authentication with the NTP clients.

The following must be respected, to make the authentication work:

- The NTP key file of the server must contain the ID. You can edit the key file in the submenu "NTP → NTP Symmetric Keys" on the NTP page.
- Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".
- The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client, which is configured as a multicast client with authentication:



```
keys /etc/ntp.key           # Path to the NPT Key file
trustedkey 1                # The Key ID, which is used for the authentication
manycastclient 224.0.1.2 key 1 # The Client listens on the Multicast Address 224.0.1.2 and
                             # uses the key with ID 1 for authentication
```

### 9.1.5.7 NTP Symmetric Keys



Since NTP version 3, NTP has been providing an authentication method using symmetric keys. The "NTP MD5 Edit key" button can be used to edit the NTP key file of the server. Upon delivery of the server, the file contains a sample key. The "Automatically Generate MD5 Keys" button allows MD5 keys to be generated automatically.

The following is an representative excerpt from an NTP key file:

```
1    M    f294fa0                # MD5 key
2    MD5  BtdW/<gj2*2M;!'-qAIN    # MD5 key
3    SHA1 094c533b614d9e4bcb6e18a97a7b0e4d459025bd # SHA1 key
```

The first column contains a unique key ID (value range 1 - 65535). The second column contains the key type ("M" or "MD5" for an MD5 key, or "SHA1" for a SHA1 key). The third column contains the key string, which may be between 1 and 32 characters long.

## How do I set up authentication between a LANTIME and my NTP clients?

1. Add the keys which are to be used to the key file of the server. The following is a representative excerpt from the key file of a server:

```
1    M    f294fa0                # MD5 key
2    MD5  BtdW/<gj2*2M;!'-qAIN    # MD5 key
3    SHA1 094c533b614d9e4bcb6e18a97a7b0e4d459025bd # SHA1 key
```

2. Enter the IDs of these keys into the "Trusted Keys" field under "NTP → General Settings", for example:



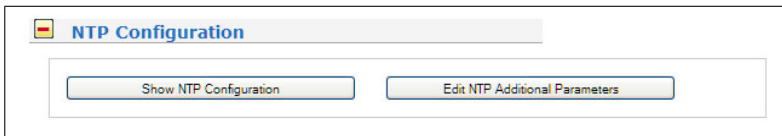
3. The following is a sample excerpt from the NTP configuration of a Linux client which uses the key with the ID 2 for authentication with the server 192.168.100.1 and the key with the ID 3 for authentication with the server 192.168.100.2:

```
keys /etc/ntp.keys # path to keys file
trustedkey 2 3 # IDs of keys to be trusted

server 192.168.100.1 iburst minpoll 6 maxpoll 6 key 2
server 192.168.100.2 iburst minpoll 6 maxpoll 6 key 3
```

In this case, the key file of the client must contain the keys with the IDs 2 and 3, which must be identical to the keys of the server.

### 9.1.5.8 NTP Configuration



The current NTP configuration file is displayed via the "Show current NTP configuration" button. This file is automatically generated by the system at every restart or change of the NTP configuration and cannot be edited directly.

If additional settings are required for NTP (Authentication, Restriction ...), which are not covered with the existing settings on the NTP page, an additional configuration file must be used. This file can be edited and managed using the "Edit Additional NTP Parameters" button. Every time the 'ntp.conf' is created this additional file is automatically attached to it.

### 9.1.5.9 NTP Restrictions



The "NTP Restrictions" page can be used to restrict NTP access to specific IP addresses.

For example, to allow access for all addresses from the subnet 192.168.100.x, enter 192.168.100.0 under IP Address and 255.255.255.0 under Netmask. Access can also be allowed for individual IP addresses.

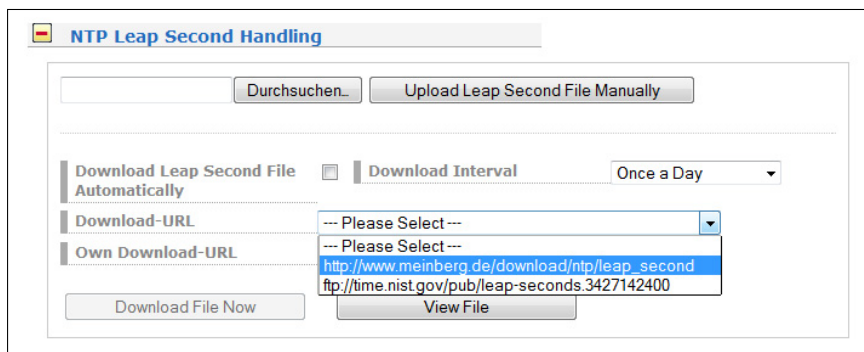
In order to enable the restricted access, the "Activate Access Restriction" option must be activated under "NTP" page, under → "General settings". Client IP addresses, which are not covered in the allowed IP address ranges, will no more receive NTP responses from the LANTIME.

### 9.1.5.10 NTP Leap Second Handling

The time base for mostly all the world's local time zones is called Coordinated Universal Time, UTC, which is derived from a several atomic clocks which are distributed in different countries all over the world. The rotation of the earth is not constant and varies over time, while the mean earth rotation speed is decreasing slowly. This is the reason why so called leap seconds are inserted into the UTC time scale, which compensate the UTC time with the real earth rotation. A leap second is always inserted at 23:59:59 (UTC), either on 31.12. or 30.06. (Other dates are theoretically possible, but practically have not been used yet).

Some protocols or methods for transferring the time information, e.g. GPS, NTP, PTP, DCF77 and IRIG can pre-announce leap seconds to give a receiver the opportunity to prepare for a leap second in advance. The GPS satellite system distributes the leap second announcement six months before the leap second event. Meinberg LANTIMEs with GPS receivers receive this announcement automatically via the GPS signal. In the log file of the LANTIME, the entry "Leap Second Announced" is generated when the date of the leap second is received.

Other synchronization methods do not offer this announcement possibility, which can lead to a one second time jump. Therefore, it is necessary to keep the NTP leap second file up-to-date on these systems, so that a leap second is correctly inserted at the midnight (UTC).

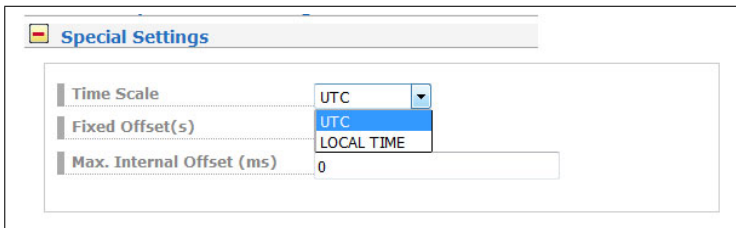


In the menu "NTP Leap Second Handling", you can view the currently stored leap second file, you can manually upload the file or configure an automatic download from the following source pages:

#### Available Download Sources for Leap Second Files:

1. NIST Leap Second File:  
<ftp://time.nist.gov/pub/> (directory listing)  
<ftp://time.nist.gov/pub/leap-seconds.list> (current leap second file)
2. IERS (Earth Rotation and reference systems Service) Leap Second File:  
<https://hpiers.obspm.fr/iers/bul/bulc/ntp/> (directory listing)  
<https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list> (current leapseconds file)
3. Meinberg Leap Second File (Copy of the IERS Leap Second File):  
<https://www.meinberg.de/download/ntp/leap-seconds.list>  
[https://www.meinberg.de/download/ntp/leap\\_second](https://www.meinberg.de/download/ntp/leap_second)

### 9.1.5.11 Special Settings



#### Time Scale

This setting configures the time zone of the NTP. The default setting is "UTC", since NTP is based on UTC by default and standard NTP clients expect UTC time.

The setting "LOCAL TIME" should only be selected, if the time server is used to synchronize specific clients that require local time. If you select "LOCAL TIME" here, the exact time zone must be configured in the menu "System → Display".

**Attention:** The use of "LOCAL TIME" is a violation of the NTP standard and causes standard NTP clients to accept faulty time and to make a time jump accordingly.

#### Fixed Offset (s)

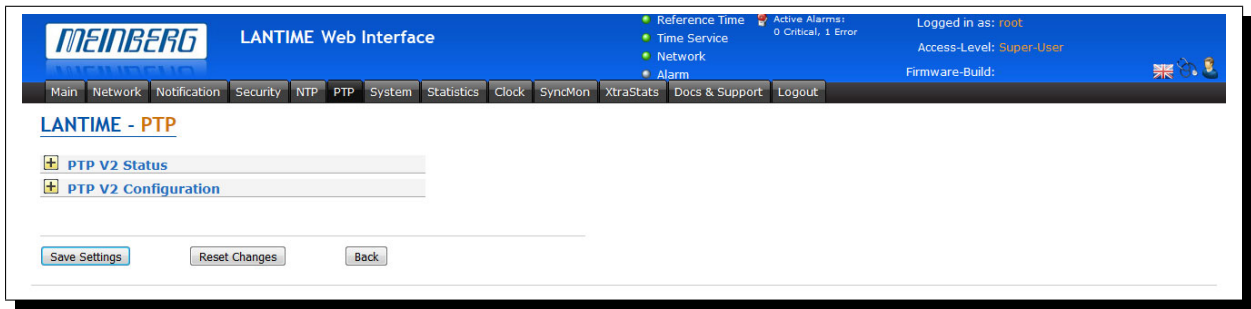
This value is used to manipulate the output time of the NTP service. The configured value in seconds is added to the current time and provides a possibility to spoof the NTP time if wanted.

Attention: The use of a "Fixed Offset" is a violation of the NTP standard and causes standard NTP clients to accept faulty time and to make a time jump accordingly.

#### Max. Internal Offset (s)

This value in milliseconds specifies a minimum accuracy the NTP service must reach, before the server starts to serve time to the clients. E.g. entering a value of 1ms means that the service will wait until the internal clock has reached 1ms accuracy or better.

## 9.1.6 PTP



All parameters for proper PTP functionality can be configured in a clear and user friendly Web GUI. The set of parameters which can be configured in the Web GUI corresponds to the PTP card version currently installed in the system. Some features are available with TSU-GbE cards and above only and these are marked as optional (\*) in this manual.

When you log in to the Web GUI, please follow to the PTP dialog. In the main menu the following sub-menus are listed:

- PTPv2 Status
- PTPv2 Configuration

If more than one PTP unit (PTP ports) is built into the system, then the status and configuration for each port can be edited separately and will be listed on this page.

### 9.1.6.1 PTP Status Information

The PTPv2 status dialogue shows all current status information of the selected PTP card according to its settings configured in the configuration submenu.

### 9.1.6.2 PTP Network Status

In the Network tab you can check if network settings of the PTP card are valid.

The screenshot displays the 'PTP V2 Status' dialog box. At the top, there is a tab for 'Interface 01 (Slot: IO2)' which is currently selected. Below the tab, there are four sub-tabs: 'Network', 'Global', 'SyncE', and 'Info'. The 'Network' tab is highlighted with an orange border. Under the 'Network' tab, the following settings are visible:

Network:	
Net Link Mode	1000 MBIT FULL DUPLEX
TCP/IP Address	172.27.19.58
Netmask	255.255.0.0
Local MAC Address	EC:46:70:00:60:C1
UUID	EC:46:70:FF:FE:00:60:C1

Below the network settings, there are three more interface tabs: 'Interface 02 (Slot: IO3)', 'Interface 03 (Slot: IO5)', and 'Interface 04 (Slot: IO6)'. Each of these tabs has its own set of sub-tabs: 'Network', 'Global', 'SyncE', and 'Info'.

#### Local MAC Address of the PTP unit

If the PTP card operates currently as a Grandmaster (GM) its local MAC Address is shown in the status of PTP slaves which are currently synchronized to this GM.

#### UUID

The UUID is the unique identifier of the PTP port which is based on the MAC address of the PTP port.

### 9.1.6.3 PTP Global Status

In the Global submenu the current operation mode of the selected PTP port (interface) is shown. The appearance of this page depends on the mode of the PTP card operation. Different states of a PTP port are possible. For example, if the unit is configured as a PTP master clock, then this page shows "Master" state. In MRS (Multi Reference Source) devices, the PTP mode "Slave" may be displayed here.

**PTP V2 Status**

Interface 01 (Slot: MRI1) | Network | **Global** | SyncE | Info

**Global:**

PTP Mode	Multicast Slave	Domain Number	0
Port State	stopped	Port Link up	No
Grandmaster MAC	00:00:00:00:00:00	Delay Asymmetry	-0.0ns
Clock accuracy	Unknown	Clock class	0
PTP Seconds	534949	Time Source	not defined
UTC Offset	0s	Leapsecond	Not Announced

TSU Time: ARB:07.01.70 04:35:49.971261;

Interface 02 (Slot: IO3) | Network | Global | SyncE | Info

Interface 03 (Slot: IO4) | Network | Global | SyncE | Info

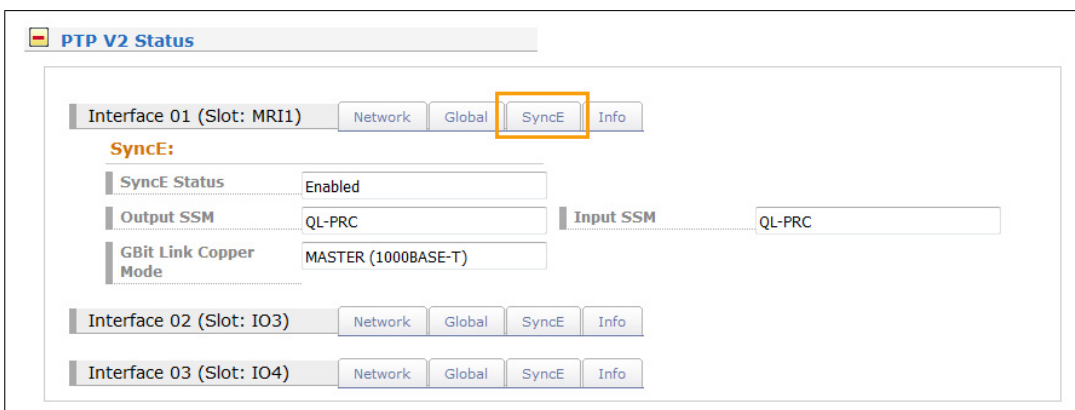
#### Port States

<b>Uninitialized</b>	The PTP module is booting up, the software daemon has not yet started, the IP address is not yet assigned.
<b>Initializing</b>	In this state the port initializes its data sets, hardware, and communication facilities.
<b>Faulty</b>	Not defined in LANTIME systems.
<b>Stopped</b>	The PTP service has been stopped or it has not started due to a missing link on the PTP port or a not-synchronized master clock after a startup.
<b>Disabled</b>	Not defined in LANTIME systems.
<b>Listening</b>	The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.
<b>preMaster</b>	A short transitional state while the port is becoming a master.
<b>Master</b>	The port is a current master.
<b>Passive</b>	The port is in passive mode, meaning there is another master clock active in the PTP domain. The port can enter master state when it wins the BMCA (Best Master Clock Algorithm) due to a failure/service degradation of the current master.
<b>Uncalibrated</b>	The port wants to become a slave in the PTP domain and has already detected a suitable grandmaster. The TSU is waiting to calculate the path delay to a Grandmaster.



<b>Slave</b>	The port has successfully subscribed to a master and receives all expected messages. It also successfully measured the path delay using delay request messages.
<b>Grandmaster MAC</b>	The MAC Address of the current Grandmaster.
<b>Clock Accuracy</b>	The clock accuracy of the active grandmaster. This value is used in the Best Master Clock Algorithm to select the best master.
<b>PTP Seconds</b>	Current value of the raw PTP seconds value (seconds since 1970).
<b>UTC Offset</b>	This value represent the current Offset to the PTP time based on TAI to calculate UTC.
<b>Domain Number</b>	A PTP domain is a logical group of PTP devices within a physical network which is defined by the same domain number. Slave devices that should sync to a certain master in the network must be configured with a unique domain number which is the same as for the master.
<b>Port Link up</b>	Status 0: the port is down, check the link LED and the connection to the link partner. If faulty, the network card should be replaced.  Status 1: the port is in normal operation.
<b>Delay Asymmetry</b>	If a static asymmetry offset in the network is known, this value may be entered (in ns) to compensate it before the PTP start.
<b>Clock Class</b>	PTP Clock class of the currently selected PTP grandmaster. This value is used in the Best Master Clock Algorithm.
<b>Time Source</b>	The type of a time source as used by the Grandmaster (informative only).
<b>Leap Second</b>	Leap second announcement flag, set up to 24 hours prior the leap second event, depending on the GM implementation.
<b>TSU Time</b>	Displayed time of day in the selected PTP timescale.

#### 9.1.6.4 SyncE Status



You can check if SyncE functionality is activated on the card or not (if supported by the PTP module).

### 9.1.6.5 PTP Configuration Menu

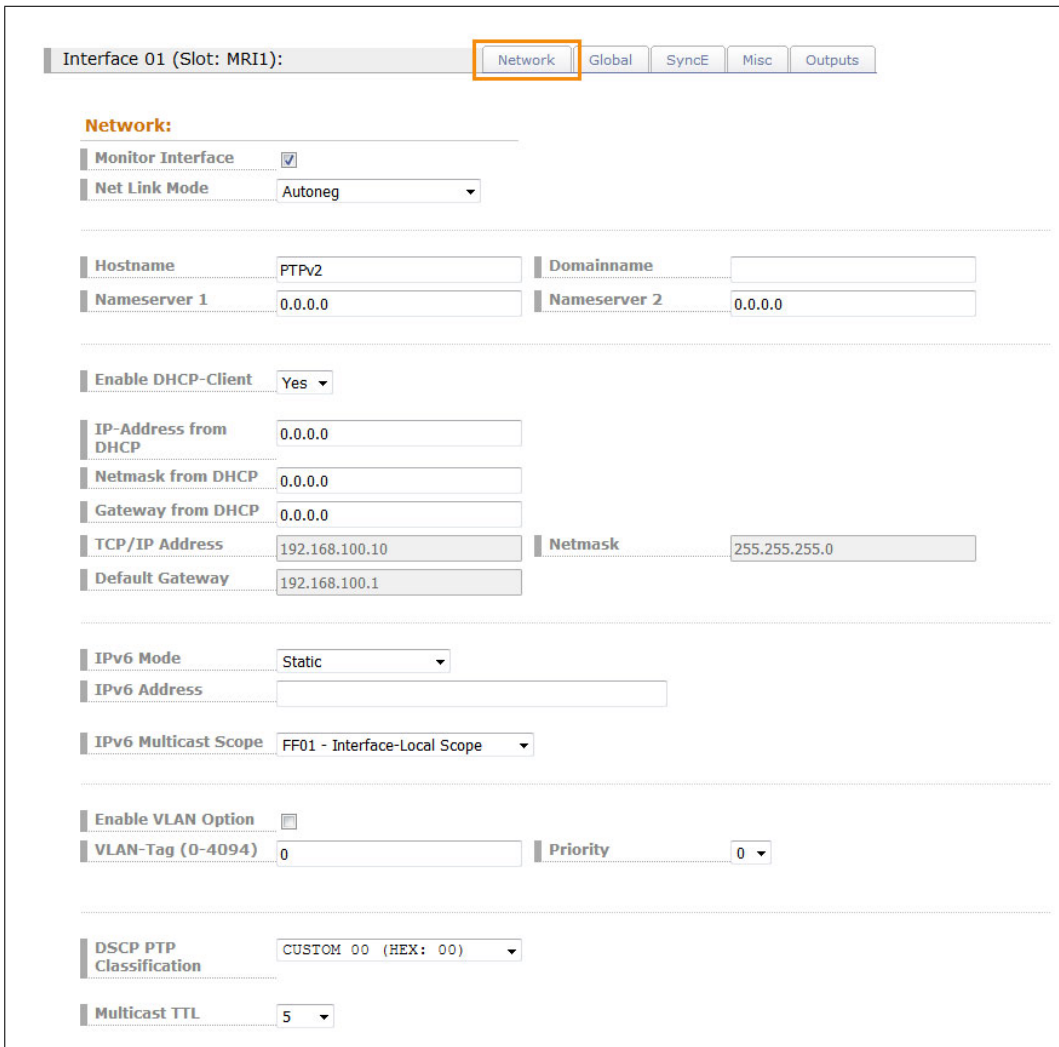
All parameters for proper operation of each PTP port (interface) which are built into the system should be configured separately according to its function in the PTP network. Whenever a change should be applied, it needs to be saved by confirming the “Save Settings” button at the bottom of the page.



The configuration parameters are grouped in the submenus as follows. Submenus marked with \* are available in TSU-GbE (and higher version) cards only.

- Network
- Global
- SyncE\*
- Misc\*
- Outputs\*

### 9.1.6.6 PTP Network Configuration



Interface 01 (Slot: MRI1): **Network** Global SyncE Misc Outputs

**Network:**

Monitor Interface

Net Link Mode Autoneg

---

Hostname PTPv2 Domainname

Nameserver 1 0.0.0.0 Nameserver 2 0.0.0.0

---

Enable DHCP-Client Yes

IP-Address from DHCP 0.0.0.0

Netmask from DHCP 0.0.0.0

Gateway from DHCP 0.0.0.0

TCP/IP Address 192.168.100.10 Netmask 255.255.255.0

Default Gateway 192.168.100.1

---

IPv6 Mode Static

IPv6 Address

IPv6 Multicast Scope FF01 - Interface-Local Scope

---

Enable VLAN Option

VLAN-Tag (0-4094) 0 Priority 0

---

DSCP PTP Classification CUSTOM 00 (HEX: 00)

Multicast TTL 5

#### Network Configuration

##### Monitor Interface

Monitoring of network port's link status.

As soon as the selected PTP network connection no longer detects a link, this state triggers a "PTP Link Down" event. This event is displayed in the menu "Notification → Notification Events".

If the PTP module is not required and is therefore not connected to the network, the checkbox "Monitor Interface " can be unchecked. No error event will be triggered then.

##### NET Link Mode

Selectable values are:

- Autonegotiation
- 100 MBIT HALF DUPLEX
- 100 MBIT FULL DUPLEX
- 1000 MBIT HALF DUPLEX
- 1000 MBIT FULL DUPLEX

##### Hostname

Hostname, a unique alphanumeric label, which distinguishes the selected PTP port from others in the network can be entered here.

##### Domainname

Domainname for the selected PTP can be assigned.

<b>Nameserver1</b>	Nameserver1 can be entered if it is used in a network.
<b>Nameserver2</b>	Nameserver2 can be entered if it is used in a network.
<b>Enable DHCP-Client</b>	Activation / deactivation of DHCP service. If a DHCP Client is activated the field for static IP configuration is deactivated. The opposite is the case when DHCP Client is deactivated.
<b>IP-Address from DHCP</b>	If DHCP service is found in the network, a valid IP for a PTP port will be assigned automatically and displayed here.
<b>Netmask from DHCP</b>	If DHCP service is found in the network, a valid Netmask for a PTP port will be assigned automatically.
<b>Gateway from DHCP</b>	If DHCP service is found in the network, a valid Gateway for a PTP port will be assigned automatically.
<b>TCP / IP Address</b>	If the DHCP Client is deactivated, this field can be edited to assign a valid static IP address for the selected PTP interface.
<b>Netmask</b>	If the DHCP Client is deactivated, this field can be edited to assign a netmask for the selected PTP interface.
<b>Default Gateway</b>	If the DHCP Client is deactivated, this field can be edited to assign a default gateway for the selected PTP interface.
<b>IPv6 Mode</b>	IPv6 addressing via DHCPv6 / Static assignment / Router Advertisement are available.
<b>IPv6 Address</b>	Ipv6 Address assigned to the selected PTP port. If Static option is activated for Ipv6 Mode, then a valid static IP address can be configured in this field.
<b>IPv6 Multicast Scope</b>	The prefix of IPv6 multicast addresses specifies their scope. A specific scope in case of multicast mode can be selected here.
<b>Enable VLAN Option</b>	Activation / deactivation of Virtual LAN (IEEE 802.1Q) service on the PTP interface.
<b>VLAN-Tag (1-4094)</b>	A 12-bit value specifying a VLAN ID to which a PTP port belongs.
<b>Priority</b>	Values 0 (default, lowest priority) to 7 (highest priority) which can be used to prioritize network traffic for different types of data.
<b>Disable SSH Service</b>	If checked then SSH Access for this PTP port is deactivated.
<b>DCSP PTP Classification</b>	Differentiated Services Code Point. This is a QoS parameter within the IP header of the Classification PTP packet to prioritize the traffic.
<b>Multicast TTL</b>	Time-To-Live. By default, the PTP multicast traffic is not routed and this value is defined as "1" by the PTP standard. However a user defined configuration of the TTLvalue can be entered here to change the default value.

### 9.1.6.7 PTP Global Configuration

The screenshot shows the 'PTP V2 Configuration' window for 'Interface 01 (Slot: MRI2)'. The 'Global' tab is selected. Under 'Global:', the 'Operating Mode' is set to 'PTP V2'. Other settings include 'Select Profile' (Custom), 'PTP Mode' (Multicast Slave), 'Unicast Master Address 1' (172.29.9.210), 'Unicast Master Address 2' (0.0.0.0), 'Delay Mechanism' (E2E), 'Network Protocol' (UDP/IPv4 (L3)), 'Priority1' (128), 'Priority2' (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), 'Announce Receipt Timeout' (3), and 'Alternate Time Offset Indicator' (No). A 'Profile Specific Configuration' section at the bottom lists various standards like IEEE C37.238-2011, IEC 61850-9-3, etc.

#### Operating Mode

##### PTP or NTP

If supported, it is possible to run an NTP service in server mode with hardware timestamp support. In this step, choose between PTP and NTP mode. It is not possible to run both modes simultaneously on one TSU card.

##### PTPv2 or PTPv1 (HPS100 - license PL-C/D/E)

The card can operate in PTPv1 mode to serve as a communication interface between PTPv1 and PTPv2 network elements.

##### Monitor (HPS100 - license PL-D/E)

This close-up shows the 'Global:' section with 'Operating Mode' set to 'Monitor'. The radio buttons for 'PTP V2', 'PTP V1', and 'NTP' are unselected, while 'Monitor' is selected and highlighted with an orange box.

To monitor PTP network elements and generate statistics, a HPS100 can operate in monitor mode. Only if this mode is activated, it is possible to monitor PTP-nodes in the network via the HPS100.

**Select Profile**

User can choose among preselected sets of PTP parameters defined in profiles usually used in different industries. If the default setting "Custom" is selected, the user can select any parameter combination available in the global configuration section as long as the PTP standard allows it. Depending on the selected profile, there might be profile specific parameters available which can be found in the "Profile Specific Parameters" section below the standard PTP parameters sections.

**There are twelve different presets currently supported on PTP cards:**

---

In Unicast Master / Slave Mode:

---

**Telecom ITU-T G.8265.1**

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot: "Layer 3 (UDP/IPv4,v6)"

**Telecom ITU-T G.8275.2**

- Ann Msg Rate: 8/sec
  - Sync Msg Rate: 128/sec
  - Del Req Rate: 128/sec
  - Priority 1: 128
  - Priority 2: 128
  - Delay Mech: "E2E"
  - Network Prot: "Layer 3 (UDP/IPv4,v6)"
-

In Unicast or Multicast Master / Slave Mode:

---

### Default E2E IEEE 1588-2008

Default Profile with End-To-End Delay Mechanism as defined by the IEEE 1588-2008 standard, available in Multicast and Unicast mode.

- Ann Msg Rate: 2/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot: "Layer 3 (UDP/IPv4,v6)"

### SMPTE ST 2059-2

- Ann Msg Rate: 4/sec
- Sync Msg Rate: 8/sec
- Del Req Rate: 8/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E" or "P2P"
- Network Prot: "Layer 3 (UDP/IPv4,v6) or Layer 2 (IEEE 802.3)"

### AES67 Media Profile

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 8/sec
- Del Req Rate: 8/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E" or "P2P"
- Network Prot: "Layer 3 (UDP/IPv4)"

---

In Multicast Master / Slave Mode:

---

**Default P2P IEEE 1588-2008**

Default Profile with P2P delay mechanism as defined by the IEEE 1588-2008 standard, available in Multicast mode.

- Ann Msg Rate: 2/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot: "Layer 3 (UDP/IPv4,v6) or Layer 2 (IEEE 802.3)"

**Telecom ITU-T G.8275.1**

- Ann Msg Rate: 8/sec
- Sync Msg Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot: "Layer 2 (IEEE 802.3)"

**Power IEEE C37.238-2011**

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot: "Layer 2 (IEEE 802.3)"
- VLAN (802.1Q): enabled (VLAN ID:0, Prio:4)
- Power Profile: TLVs enabled



**Power IEEE C37.238-2017**

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P or E2E"
- Network Prot: "Layer 3 (UDP/IPv4,v6) or Layer 2 (IEEE 802.3)"
- VLAN (802,1Q): enabled (VLAN ID:0, Prio:4)
- Power Profile: TLVs enabled

**Utility IEC 61850-9-3**

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 1/sec
- Del Req Rate: 1/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"
- Network Prot: "Layer 2 (IEEE 802.3)"
- Power Profile: TLVs enabled

**IEEE 802.1AS**

- Ann Msg Rate: 1/sec
- Sync Msg Rate: 8/sec
- Del Req Rate: 1/sec
- Priority 1: 248
- Priority 2: 248
- Delay Mech: "P2P"
- Network Prot: "Layer 2 (IEEE 802.3)"

**DOCSIS 3.1**

- Ann Msg Rate: 8/sec
- Sync Msg Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot: "Layer 2 (IEEE 802.3)"

**PTP Mode:**

A PTP port can operate in one mode only: master or slave. When the mode is selected the user can choose between multicast or unicast-only protocol. In the newest firmware a combined unicast multicast master mode of operation is also supported.

**Hybrid Mode:**

In this mode PTP messages Sync, FollowUp and Announce are sent in Multicast whereas the DelayRequest and DelayResponse Messages are sent in Unicast.

**Delay Mechanism:**

Two options possible:

E2E (End-to-end) where delay measurement messages are sent directly from a slave to the master (two end nodes).

P2P (Peer-to-peer): each device (a peer) in the network exchanges peer-to-peer delay measurement messages. This way each node can keep a track of the delays between itself and its immediately connected neighbour. P2P mechanism can be used in 1588 PTP-capable networks only.

**Network Protocol:**

Two options for network protocol are possible:

ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet frames including MAC addresses of a slave and master.

UDP-UDP/IPv4/IPv6 (Layer 3): User Data Protocol one of the main protocols used for the Internet.

**Priority 1:**

The attribute is used in the execution of the best master clock algorithm (BMCA). Lower values take precedence. Configurable range: 0..255. The operation of the BMCA selects clocks from a set with a lower value of priority1 over clocks from a set with a greater value of priority1.

**Priority 2:**

The attribute is used in the execution of the BMCA. Lower values take precedence.

Configurable range: 0..255.

In the event that the operation of the BMCA fails to order the clocks based on the values of priority1, clockClass, clockAccuracy and scaledOffsetLogVariance, the priority2 attribute allows the creation of up to 256 priorities to be evaluated before the tiebreaker. The tiebreaker is based on the clockIdentity. The values clockClass, clockAccuracy and scaledOffsetLogVariance depend on the internal state of the grandmaster and cannot be configured.

**Msg. Intervals:**

Specify the settings for PTP message rates.

**Announce Interval:**

Specifies the rate for sending announce messages between masters in order to select the current Grand Master. Available settings are: 16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s with a default value 2 seconds.

**Sync Interval:**

Specifies the rate for sending sync messages from a master to slave.

Available settings are: 128/s, 64/s ... 64s, 128s, with a default value 1 second.

**Delay Request Interval**

Specifies the rate how often delay request messages are sent from a slave to the master. Delay request messages intervals 128/s, 64/s ... 64s, 128s, with a default value 2 seconds.

**Announce Receipt Timeout:**

Specifies the rate for announce receipt timeout messages which is generally 2-10 times the Announce Interval rate, with a default value of 3. In this time the BMCA procedure should select the current Grand Master.

**Interval Duration [s]:**

Requested duration until timeout / renewal.

**Domain Number:**

A PTP domain is a logical group of PTP devices within a physical network which is defined by the same domain number. Slave devices that should sync to a certain master in the network must be configured with a unique domain number which is the same as for the master.

**Timescale:**

Two options are possible:

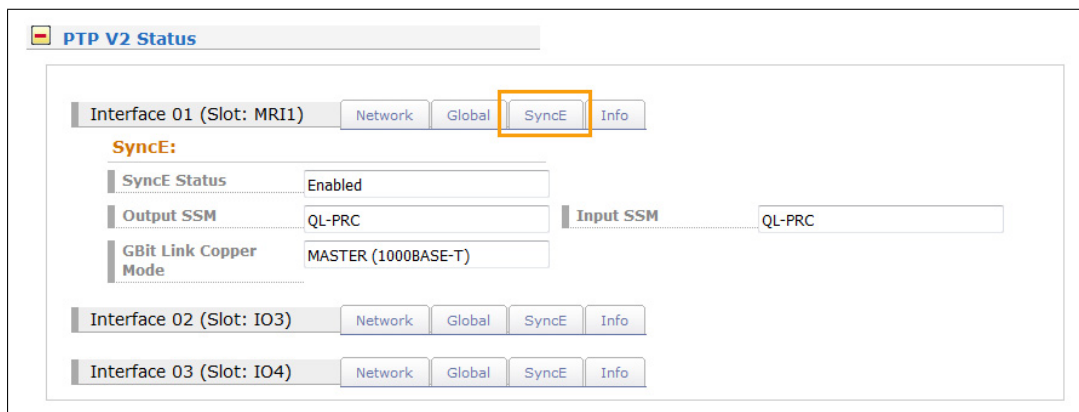
**PTP:** As per default TAI timescale is used in PTP timing. TAI is a linear timescale without discontinuities such as inserted leap seconds in the UTC timescale. A time unit is based on SI second. The TAI timescale started with 1 January 1970 00:00:00.

**ARB as arbitrary:** In normal operation, the epoch is set by an administrative procedure.

**Alternate Time Offset Indicator Extension:**

The Alternate Time Offset Indicator (ATOI) TLV extension is used to transmit local time information, such as local time zone offset and summer time changeover, from master to slave devices. This TLV has a current offset data field and can therefore provide the data required to convert TAI- or UTC-based time information to local time.

### 9.1.6.8 Option SyncE Configuration



This submenu allows all relevant settings for the Synchronous Ethernet functionality. SyncE is an ITU-T standard for computer networking that facilitates the transference of clock signals over the Ethernet physical layer.

#### Note:

The SyncE signal can only be used as a reference input signal, when a TSU-GbE card operates in an MRI Slot (see menu - "Configuration Receiver → MRS Settings").

#### Enable SyncE

Activation / Deactivation if SyncE signal on a PTP port. SyncE runs on the PHY network layer therefore it does not disturb PTP on Layer 2 or Layer 3. They both can run in parallel on the same port.

#### Quality Level Selection

If enabled, the Quality Level is transported once per second within the ESMC (Ethernet Synchronization Message channel) and are determined automatically depending on the clock status in master mode or used as they are received as an input in slave mode. If this mode is disabled, then the settings chosen below in Fixed Input SSM and Fixed Output SSM are used permanently as static values.

#### SDH Network Option

The selected values for the Quality levels depend on the SDH network options which reflect to Option 1 (for SDH, E1 based systems) or Option 2 (for SONET, T1 based systems).

**Fixed Input SSM** Fixed Quality level of the SyncE input signal.

**Fixed Output SSM** Fixed Quality level of the SyncE output signal.

#### Gbit Link Copper Mode

If the copper port is used for SyncE in Gbit mode then the Clock Master or Clock Slave needs to be defined. This is not necessary if optical connections via SFP are used as this is determined automatically there.

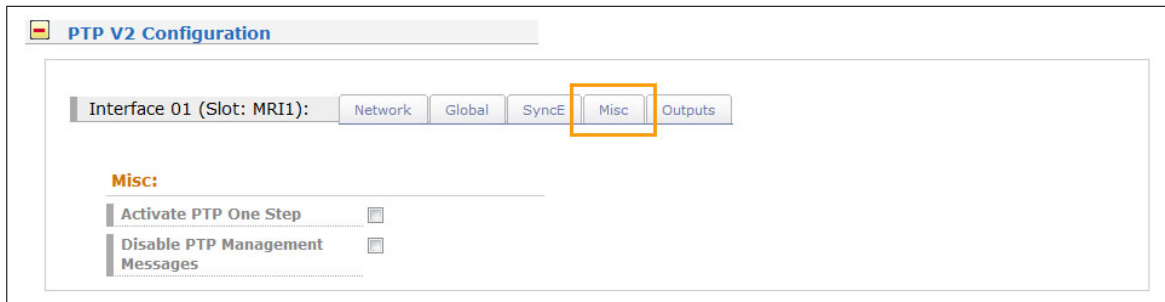
#### Mode

User can select if the copper port should be forced to act as the clock master or clock slave depending on the role (Master/Slave) that this SyncE port should have. Misconfiguration can lead to link loss, so the user needs to take care about the proper configuration of the link partners.

#### Port

The port can operate in a SyncE clock master or clock slave mode. A configuration is only necessary for the copper port but not for Fibre Optic connections.

### 9.1.6.9 Option Misc. Configuration



#### Activate PTP One Step:

Per default Two Step approach is active.

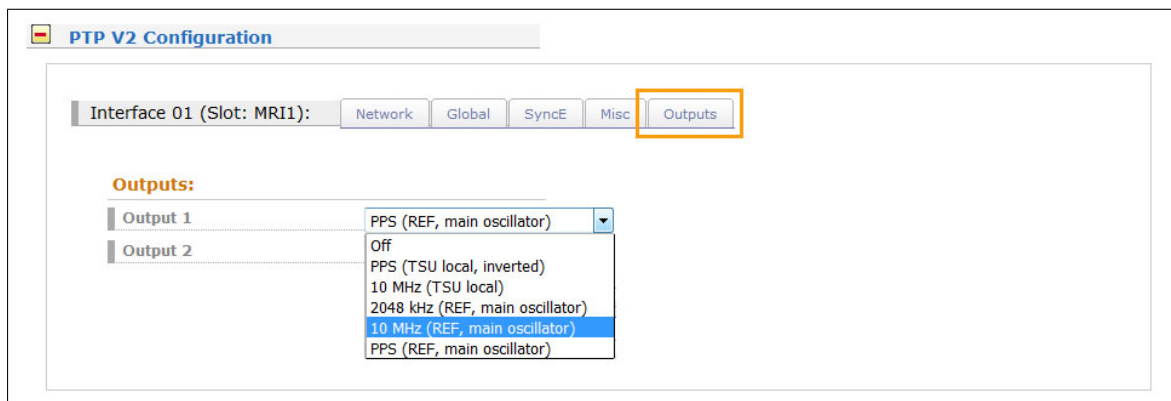
Two Step approach: The PTP protocol requires the master to periodically send SYNC messages to slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by sending this time stamp in a separate packet (a so-called FOLLOW-UP message).

One Step operation enabled: the SYNC messages itself is time stamped on- the- fly just before it leaves the network port. Therefore, not FOLLOW-UP message is needed.

#### Disable PTP

A protocol within PTP use to query and update the PTP data sets maintained by master clocks. These messages are also used to customize a PTP system and for initialization and fault management. Management messages are used between management nodes and clocks. This feature is enabled per default.

### 9.1.6.10 Option: Output Configuration



TSU-GbE card comprises one Gigabit Ethernet SFP/RJ45 Combo Port for network synchronization and two female BNC output interfaces with a list of available signals as follows:

- PPS (generated locally on the TSU, inverted)
- 10 Mhz (generated locally on the TSU)
- 2.048 MHz (taken from active internal clock module)
- 10 MHz (taken from active internal clock module)
- PPS (taken from active internal clock module)

Per default no output signal is active on both outputs.

## 9.1.7 FDM - Frequency Deviation Monitoring

**LANTIME Web Interface**

Reference Time, Time Service, Network, Alarm, Active Alarms: 0 Critical, 1 Error, Logged in as: root, Access-Level: Super-User, Firmware-Build:

Main | Network | Notification | Security | NTP | PTP | **FDM** | System | Statistics | Clock | IO Config | SyncMon | XtraStats | Docs & Support | Logout

### LANTIME - FDM Configuration

FDM Status

FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot IO4]:

Interface 01: General | Analog Outputs | Receiver

**General:**

Current Frequency	50.020	Hz
Time Deviation	25.4306	Seconds
Frequency Deviation	0.020	Hz
Reference Time	2017.10.16 08:54:55	
Power Line Time	2017.10.16 08:55:20.431	
Last Synchronisation	2017.10.16 08:54:55	

---

Line Frequency	50 Hz
Flags	Synced, Power Line Time Locked,

+ FDM Configuration

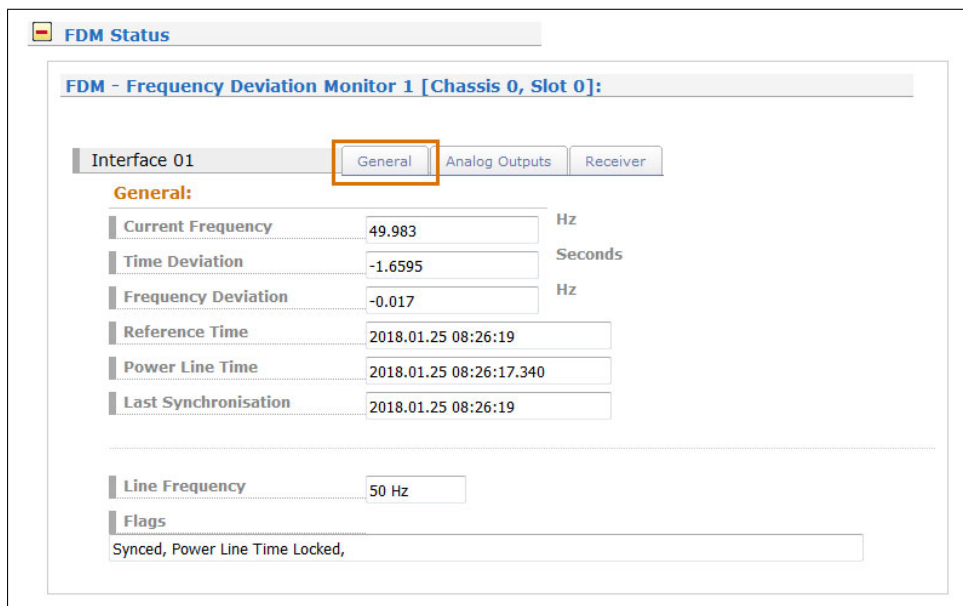
+ FDM Information

Save Settings | Reset Changes | Back

A preconnected reference is necessary to provide a serial time string, a PPS (pulse per second) signal and 10MHz frequency. The accuracy of the measurements is derived from these signals.

The module calculates the frequency as well as the time, based on the mains frequency. The time deviation (TD) is the difference of this calculated time (PLT) to the reference time (REF). This time deviation as well as the frequency itself is sent out via serial interface or is being converted to an analog voltage output provided by a DAC.

## 9.1.7.1 FDM Status



**FDM Status**

**FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot 0]:**

Interface 01 **General** Analog Outputs Receiver

**General:**

Current Frequency	49.983	Hz
Time Deviation	-1.6595	Seconds
Frequency Deviation	-0.017	Hz
Reference Time	2018.01.25 08:26:19	
Power Line Time	2018.01.25 08:26:17.340	
Last Synchronisation	2018.01.25 08:26:19	

---

Line Frequency	50 Hz
----------------	-------

**Flags**

Synced, Power Line Time Locked,

This menu shows the following values:

**Current Frequency:** the current frequency of the monitored power network

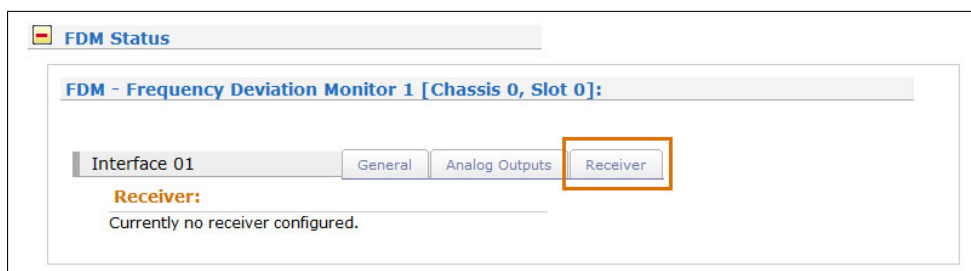
**Reference Time:** REF - the time of the reference clock (i.e. GPS)

**Power Line Time:** PLT - the time of the monitored power line

**Line Frequency:** mains frequency (50Hz or 60Hz)

**Flags:** transmitted Flags by FDM (Error Bits)

## Receiver State



**FDM Status**

**FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot 0]:**

Interface 01 General Analog Outputs **Receiver**

**Receiver:**

Currently no receiver configured.

The "Receiver" tab displays all connected and configured receivers.



### 9.1.7.2 FDM Configuration

#### Automatic Monitoring of Powerline Frequency

It is possible to define an upper and lower limit for the powerline frequency and receive alarm messages (email, syslog, SNMP traps) when a LANTIME device detects that the frequency measurement value is outside the acceptable range.

The screenshot shows the 'FDM Configuration' window for 'Interface 01'. The 'General' tab is active. The configuration parameters are as follows:

Parameter	Value	Unit
Line Frequency	50 Hz	
Min Frequency	49900	mHz
Max Frequency	50100	mHz
Max Negative Time Deviation	1000000	ms
Max Positive Time Deviation	1000000	ms
Timezone	(UTC) - UTC	
Activate Logging	<input checked="" type="checkbox"/>	
Restart FDM	Execute now	

With the FDM configuration menu the following parameters can be set:

<b>Line Frequency:</b>	configure frequency of the observed power line
<b>Min Frequency:</b>	an error occurs if the frequency reaches the min constraint
<b>Max Frequency:</b>	an error occurs if the frequency reaches the max constraint
<b>Max Negative Time Deviation:</b>	an error occurs if the frequency reaches the max negative constraint
<b>Max Positive Time Deviation:</b>	an error occurs if the frequency reaches the max positive constraint
<b>Timezone:</b>	used local timezone for reference time and powerline time
<b>Activate Logging:</b>	activate logging for FDM in XtraStats
<b>Reset FDM</b>	to restart the device

## Configuration of serial ports

The screenshot shows the 'FDM Configuration' window for 'Interface 01' on 'Chassis 0, Slot 0'. The 'Serial Port' tab is selected. Under the 'Serial Port' section, there are two configuration blocks for 'COM 1' and 'COM 2'. Each block contains the following settings:

- Baud Rate:** 19200
- Framing:** 8N1
- String Type:** FDM Standard
- Mode:** per second

**Baud Rate** for the transmission of serial time telegrams  
600, 1200, 2400, 4800, 9600, 19200

**Framing** 7N2,7E1,7E2,8N1,8N2,8E1,7O2,8O1

**String Type** type of generated serial time telegram  
FDM Standard, FDM Short, FDM Areva, FDM TPC,  
Fingrid, FDM Standard 2, FDM 3 and FDM Computime

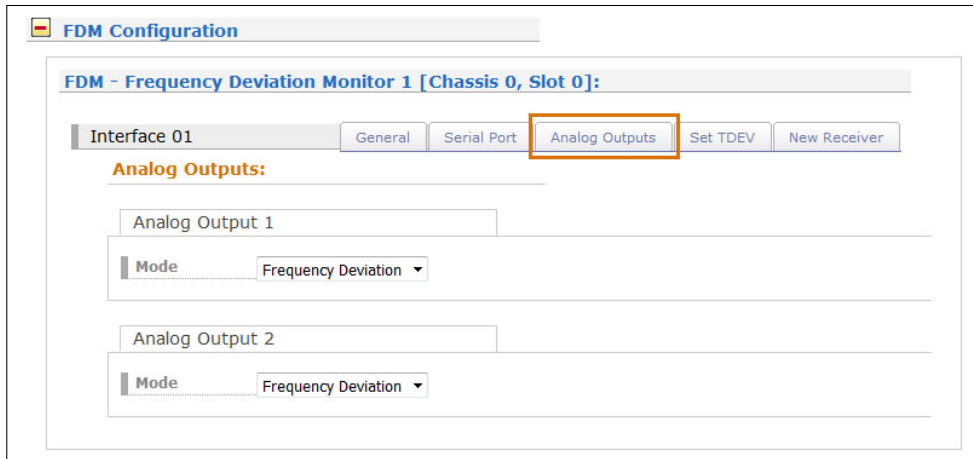
The standard FDM telegram format contains the following values:  
mains frequency (FF.xxx Hz)  
frequency deviation (+-FF.xxx Hz)  
reference time (HH:MM:SS)  
power line time (HH:MM:SS.mmm)  
time deviation (+-MM:SS.mmm)

**Mode** per second, per minute and on request

## Analog Outputs

The FDM180 provides two analog outputs (A0/A1) via the 16-pin X1 connector. These outputs have a voltage range of  $-2.5V \dots + 2.5V$ , divided into 65,536 steps (16-bit resolution).

Either the frequency deviation or the difference time of each analog output can be selected as display-value.



### Mode:

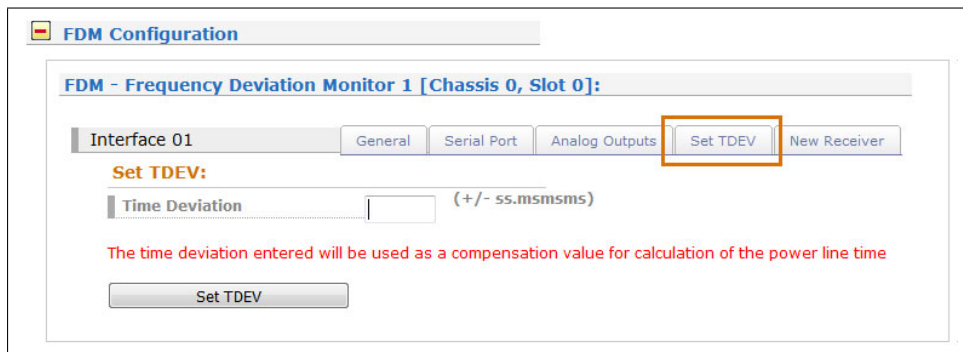
**Time Deviation:** Depends on the defined constraints for Min Time Deviation and Max Time Deviation

Example: min:-100s and max:+100s if the time deviation reach -100s the analog output is at  $-2.5 V$  and if +100s then at  $+2.5 V$  with a resolution of 16bit DAC

**Frequency Deviation:** Depends on the defined constraints for Min Frequency Deviation and Max Frequency Deviation

Example: min: 45Hz and max: 55Hz @ 50Hz line frequency if the frequency deviation reach 45Hz the analog output is at  $-2.5 V$  and if 55Hz then at  $+2.5V$  with a resolution of 16bit DAC

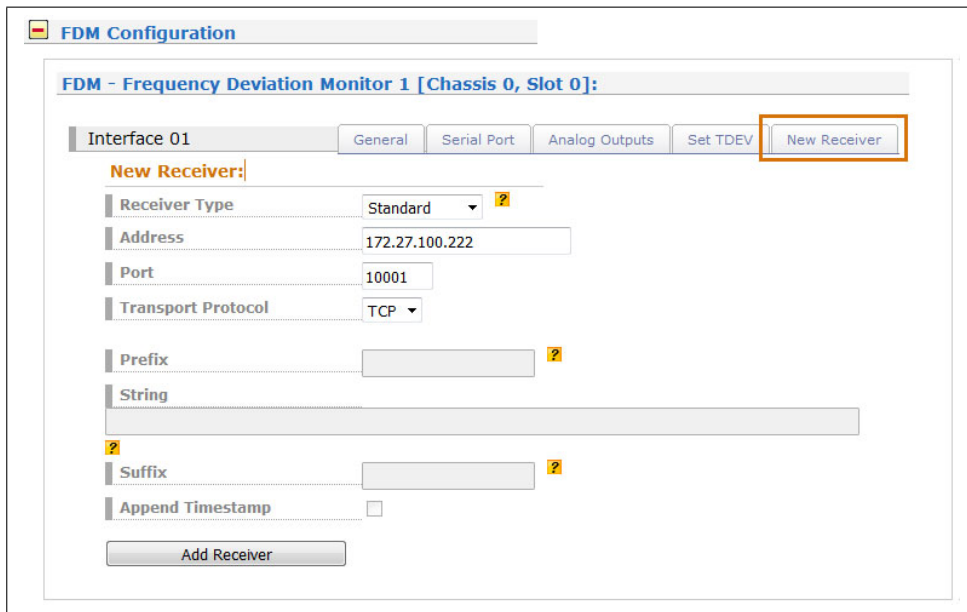
## Submenu Set TDEV



The screenshot displays the 'FDM Configuration' window for 'FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot 0]'. The 'Interface 01' tab is active, and the 'Set TDEV' button is highlighted with an orange box. Below the tabs, the 'Set TDEV:' section contains a 'Time Deviation' input field with a unit of '(+/- ss.msmsms)'. A red note states: 'The time deviation entered will be used as a compensation value for calculation of the power line time'. A 'Set TDEV' button is located at the bottom of this section.

**Time Deviation** set a value to preconfigure the time deviation 0 for reset (example: if you already had one FDM and get another one and want that both FDM have the same time deviation value).

Submenu New Receiver



In this section, the user can add a new receiver for FDM telegrams. Any number of receivers (network displays and/or PCs for analysis and display of status messages or frequencies), which are connected to the same network, can be configured here.

**Receiver Type** Type of telegram for the network transmission

Standard: Standard FDM time telegram

Sent once per second

i.e. "F:50.016 FD:+00.016 REF:15:17:57 PLT:15:17:57.056 TD:+00.056"

Extended: Extended FDM time telegram with intermediate measurements and sequence ID

Sent once per second

i.e. "F:50.006 F:50.004 F:50.013 F:50.012 F:50.010 F:50.010 F:50.006 F:50.012 F:50.020"

or "F:50.013 FD:+00.013 REF:15:19:10 PLT:15:19:10.071 TD:+00.071 SEQ:0000000004"

Intermediate: Truncated FDM time telegram with intermediate measurements

Sent once per 100ms

M1:49.997 SEQ:0000000053

M2:49.996 SEQ:0000000054

M3:50.000 SEQ:0000000055

M4:49.999 SEQ:0000000056

M5:49.996 SEQ:0000000057

M6:49.996 SEQ:0000000058

M7:49.997 SEQ:0000000059

M8:49.995 SEQ:0000000060

M9:49.996 SEQ:0000000061

M9:49.996 SEQ:0000000062

Custom: Customized FDM time telegram, which consists of prefix, string and suffix

Sent once per second

**Address:** Address or host name of the message recipient (display or computer)

**Port:** Used TCP/UDP port for telegram transmission

**Transport Protocol:** Used protocol for telegram transmission (TCP/UDP)

Only if receiver type "Custom" is selected

**Prefix:** Prefix of customized strings, control characters can be specified by their hex value (ASCII), for example:  
 "\x01" for SOH (Start of Header) or "\x02" for SOT (Start of Text)

**String:** Customized time telegram, which can be composed of arbitrary text and the following variables (identified by the prefix '%'):

PLFRQ	Power Line Frequency (i.e. 50.023)
FRQDEV	Frequency Deviation (i.e. +00.023)
REFTIME	Referenc Time (i.e. 15:17:23)
POWERLNTIME	Power Line Time (i.e.. 15:17:22.550)
PLTDEV	Power Line Time Deviation (i.e. -00.450)
IDX	Intermediate Measurement Index (i.e. 1)
IMMFRQ1	Intermediate Measurement Frequency with Index 1 (i.e. 50.034)
IMMFRQ2	Intermediate Measurement Frequency with Index 2 (i.e. 50.034)
...	
SEQID	Sequence ID (i.e. 0000000061)
SYSTIME	System Time (i.e. 15:17:23)
SYNCSTATE	Synchronization Status (' ' = synchronized, '*' = unsynchronized)
SYNCTEXT	Synchronization Text („OK“ = synchronized, „NO“ = unsynchronized)
TIMESTAMP	Current Timestamp (i.e. 2016-03-15 16:03:10.042)
TIMESTRING	Time string to set the display time (i.e. S16:04:37;15.03.16S)

An auto-toggle feature allows to define a sequence of formats by setting up comma-separated format strings. Additionally, the duration of a format string can be defined using the FORMATSTR@DURATION format.

The following example will show the Powerline Frequency for 20 seconds, then the Reference Time for 30 seconds, then the Frequency Deviation for 10 seconds. Afterwards, it will start over with the PLF display:

```
PLF %PLFRQ Hz@20,REF %REFTIME@30,FDV %FRQDEV@10
```

**Suffix:** Suffix of customized strings, control characters can be specified by their hex value (ASCII), for example:  
 "\x0A" for LF (Line Feed) or "\x0D" for CR (Carriage Return)

#### Append

**Timestamps:** Indicates, whether a timestamp shall be appended to the message

### 9.1.7.3 FDM Information

FDM Information

**FDM - Frequency Deviation Monitor 1 [Chassis 0, Slot 0]:**

Common Information

Name	Value
Model:	FDM180M (89)
Serial Number:	011811000170
Software Revision:	v1.14 (Standard)
Supported Features:	IMS data
Serial Ports:	2 (8)
Number of Programmable Pulse Outputs:	0
Number of Supported Time Capture Inputs:	0

<b>Temperature Sensor 1</b>	<b>Temperature Sensor 2</b>
Current: 43.75°C	Current: 39.50°C

Overview: Information about the used FDM module, model name, serial number, software revision, used serial ports and display of the temperature sensors (degrees Celsius).

#### 9.1.7.4 Serial FDM Telegrams

#### 9.1.7.5 Standard FDM String

The STANDARD string is a sequence of 62 ASCII characters containing the frequency F, the frequency deviation FD, the REF time, the power line time PLT and the time deviation TD, each item separated by a space character. The string is sent out at the beginning of every new REF time second and ends with the characters Carriage-Return (Hex code 0Dh) and Line-Feed (Hex code 0Ah). The letters displayed in italics are replaced by the calculated values whereas the other characters are part of the string:

*F:49.984*\_FD:-00.016\_REF:15:03:30\_PLT:15:03:30.378\_TD:+00.378<CR><LF>

The meaning of the several values is described below:

<i>F:49.984</i>	The measured power line frequency with a resolution of 1 mHz
<i>FD:-00.016</i>	The frequency deviation between calculated and nominal frequency, with sign character (+/-), resolution: 1 mHz, maximum: +-09.999 Hz
<i>REF:15:03:30</i>	The reference time from the preconnected clock (hours:minutes:seconds)
<i>PLT:15:03:30.378</i>	The power line time, based on the mains frequency, (hours:minutes:seconds.milliseconds) Time jumps, like changeover in daylight saving or leap seconds will not be executed by the PL time!
<i>TD:+00.378</i>	The time deviation between REF time and PL time, with sign character (+/-), resolution: 1ms, maximum: +-99.999s

#### 9.1.7.6 FDM Standard 2 Telegramm:

Like FDM standard, but it sends every 500 ms instead of 1 per second.

#### 9.1.7.7 Short FDM String

The SHORT string is a sequence of 23 ASCII characters containing simply information about frequency deviation FD and time deviation TD, separated by a space character. The string is sent out at the beginning of every new REF time second and ends with the characters Carriage-Return (Hex code 0Dh) and Line-Feed (Hex code 0Ah). The letters displayed in italics are replaced by the calculated values whereas the other characters are part of the string:

*FD:-00.016*\_TD:+00.378<CR><LF>

The meaning of the several values is described below:

<i>FD:-00.016</i>	The frequency deviation between calculated and nominal frequency, with sign character (+/-), resolution: 1 mHz
<i>TD:+00.378</i>	The time deviation between REF time and PL time,, with sign character (+/-), resolution: 1 ms



### 9.1.7.8 FDM Areva String

The Areva string is a sequence of 71 ASCII characters containing the frequency F, the frequency deviation FD, the time deviation TD, the power line time PLT and the reference time REF (preceded by the 3 digit day-of-the-year), each item separated by the characters Carriage-Return (Hex code 0Dh) and Line-Feed (Hex code 0Ah). Each of the five data items is preceded by a fixed 3 digit address (020 ... 024). The string starts with the STX character (start-of-text, Hex code 02h) and ends with a terminating ETX character (end-of-text, Hex code 03h) on time with the change of the REF time seconds. The letters displayed in italics are replaced by the calculated values whereas the other characters are part of the string:

```
<STX> 02049.984<CR><LF>
021-0.016<CR><LF>
022+00.378<CR><LF>
02315_03_30.378<CR><LF>
024068_15_03_30_<CR><LF>
<ETX>
```

The meaning of the several values is described below:

49.984	The measured power line frequency with a resolution of 1 mHz
-0.016	The frequency deviation between alculated and nominal frequency, with sign character (+/-), resolution:1 mHz
+00.378	The time deviation between REF time and PL time, with sign character (+/-), resolution: 1 ms
15_03_30.378	The power line time, based on the mains frequency, (hours_minutes_seconds.milliseconds) Time jumps, like changeover in daylight saving or leap seconds, will not be executed by the PL time!
068_15_03_30	The reference time from the preconnected clock, (day-of-the-year_hours_minutes_seconds)

### 9.1.7.9 TPC FDM String

The TPC string is a sequence of 29 ASCII characters containing the REF time (with day-of-the-year), the time deviation TD and the frequency deviation FD. The string starts with the SOH character (start-of-header, ASCII code 01h) on time with the beginning of every new REF time second and ends with the characters Carriage-Return (ASCII code 0Dh) and Line-Feed (ASCII code 0Ah). The letters displayed in italics are replaced by the calculated values whereas the other characters are part of the string:

**<SOH>288:10:11:29 -00.03F+50.01<CR><LF>**

The meaning of the several values is described below:

<b>288:10:11:29</b>	the reference time from the upstream radio clock, (day of year:hours:minutes:seconds)
<b>" " or "?"</b>	if reference time is synchron then " " otherwise "?"
<b>-00.03</b>	the mains frequency deviation from the setpoint, resolution 1 mHz
<b>F+50.01</b>	The power line frequency, 10 mHz resolution

### 9.1.7.10 Computime Extended FDM String

The extended Computime string is a sequence of 42 ASCII characters containing the REF time (with date and day-of-the-week), the time deviation TD and the frequency F. The string is send out at the beginning of every new REF time second and ends with the characters Carriage-Return (Hex code 0Dh) and Line-Feed (Hex code 0Ah). The letters displayed in italics are replaced by the calculated values whereas the other characters are part of the string:

**T:10:03:09:02:15:03:30D:+000.378F:49.984<CR><LF>**

The meaning of the several values is described below:

<b>T:10:03:09:02</b>	The date of the reference time from the preconnected clock, (year:month:day:day-of-the-week / Monday = 01, Sunday = 07)
<b>15:03:30</b>	The reference time from the preconnected clock, (hours:minutes:seconds)
<b>D:+000.378</b>	The time deviation between REF time and PL time, with sign character (+/-), resolution: 1ms, maximum: +-99.999s (the first digit is always 0!)
<b>F:49.984</b>	The measured power line frequency with a resolution of 1 mHz

### 9.1.7.11 FDM Fingrid String

The fingrid telegram consists of a sequence of 34 characters and contains the reference time, the time deviation and the frequency deviation. It ends with the characters carriage return (hex code 0Dh) and line feed (hex code 0Ah).

**079:08:13:55.000 T+6.780F+0.012<CR><LF>**

**079:08:13:55.000** reference time from the preconnected clock,  
(yeardays:hours:minutes:seconds:milliseconds)

**T+6.780** the time deviation between REF time and PL time,  
with sign character (+/-), resolution: 1 ms

**F+0.012** The frequency deviation between calculated and nominal frequency,  
with sign character (+/-), resolution: 1 mHz

Configure the fingrid telegram for the corresponding serial interface and use the mode "On request only (?)".  
Send T or ? to get the respond string exactly with the change of the next second within 1 s.

#### Example for the request of the Fingrid time telegram:

Date: 20 March 2017  
Time: 08:13:55 (UTC)  
Time Deviation: +6.780 s  
Frequency Deviation: +0.012 Hz

to FDM ← T or ? (at 08:13:54.xxx)  
from FDM → **079:08:13:55.000 T+6.780F+0.012<CR><LF>**

To correct the time deviation TD, please use the specified format. If the time deviation TD is accepted,  
the FDM confirms the command and applies the value within the next 2 seconds.

#### Example of setting TD to 6.780 seconds:

to FDM ← **F27 B3 PS +6.780<CR><LF>**  
from FDM → **F27<CR><LF>**

### 9.1.7.12 FDM III String

Configure FDM III string in serial parameters (for corresponding serial port) as output string type.

#### Example of FDM III String:

Date: 09 March 2017  
Time: 12:17:55 (UTC)  
Time Deviation: -1.573s  
Frequency Deviation: +0.095Hz

**068:12:17:55?T-01.537F+0.123SF+60.095ST12:17:53.463<CR><LF>**

**068:12:17:55** Reference time from the preconnected clock,  
(yeardays:hours:minutes:seconds)

**?** Local FDM status (" " sync or "?" not sync)

**T-01.537** The time deviation between REF time and PL time,

	with sign character (+/-), resolution: 1 ms
<b>F+0.123</b>	The frequency deviation between calculated and nominal frequency, with sign character (+/-), resolution: 1 mHz
<b>SF+60.095</b>	The measured power line frequency with a resolution of 1 mHz
<b>ST12:17:53.463</b>	The power line time, based on the mains frequency, (hours:minutes:seconds.milliseconds)

### 9.1.7.13 Error-Bits

The FDM module registers errors and overflows and sets or deletes eight error bits then. In this way, the user can find out if an "Overflow" occurs for example. These error bits document various error causes that occurred during operation.

The displayed value has the format: *X8 X7 X6 X5 X4 X3 X2 X1*

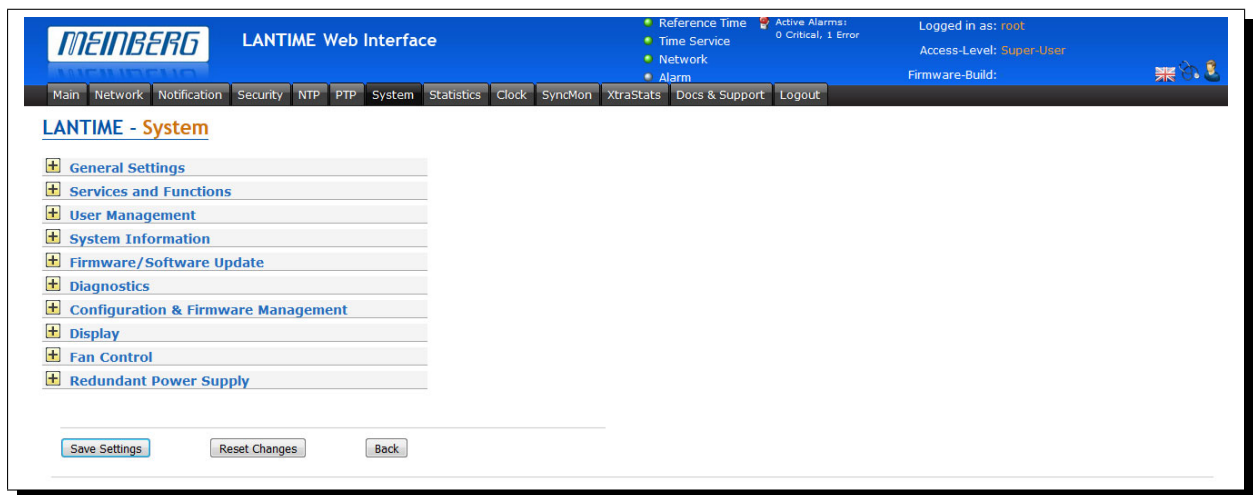
- X8:** A2 Overflow, analog output 2 has reached its final value
- X7:** A1 Overflow, analog output 1 has reached its final value
- X6:** Time Deviation Overflow, the time difference is greater than +- 99.999s
- X5:** Frequency Overflow, the frequency deviation is greater than the configured max./min values
- X4:** REF Free, no sec-impulse from the reference
- X3:** Power Line Time Free, no power line frequency (power line time remains at the last value)
- X2:** No Time String, no serial time telegram received
- X1:** No Power Line Time Init, the power line time has not (yet) been initialized

The error bits can be read out serially on request by an "E" (ASCII code 45h) via the interfaces COM 0/1.

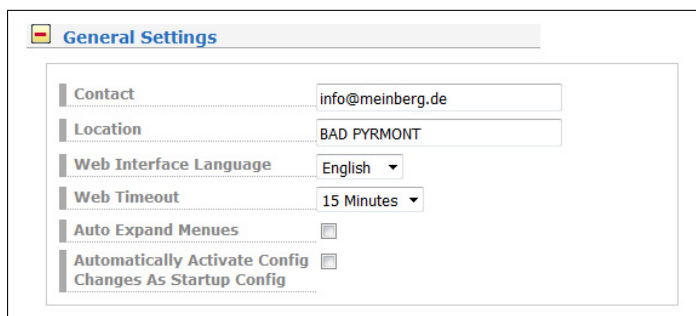
The format of the response string is:

ERROR:X8X7X6X5X4X3X2X1<CR><LF>

## 9.1.8 System



### 9.1.8.1 General Settings



#### Contact:

An input field for storing the contact information. The information is also displayed on the main page of the web interface and can be queried via SNMP.

#### Location:

An input field for storing the device location. The information is also displayed on the main page of the web interface and can be queried via SNMP.

#### Web Interface Language:

Language setting of the web interface.

#### Web Timeout:

The parameter Web Timeout defines how many minutes of inactivity can pass before a user is automatically logged out of the Web interface.

#### Auto Expand Menus:

If this feature is enabled all sub-menus will be expanded in each configuration dialogue.

#### Automatically Activate Config Changes As Startup Config:

If this option is enabled, each configuration change is immediately added to the startup configuration of the LANTIME (the startup configuration is the configuration that is used when the LANTIME is booted). If the option is not activated, the following note is displayed in the header of the Web interface after each configuration change:

**Hint:**

Current configuration is not marked as startup configuration.

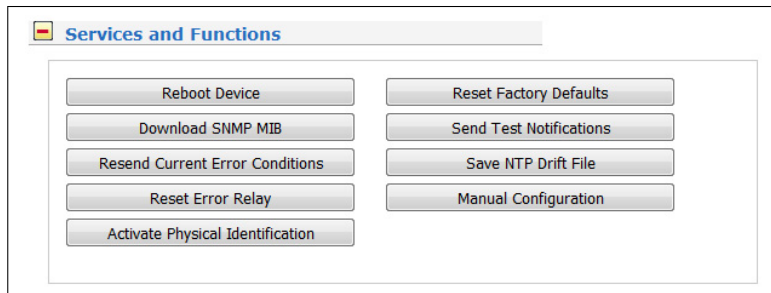
Save as startup configuration now

Discard current configuration

Show Changes

Each configuration change can then be saved as start configuration by confirming with "Save as startup configuration now" button.

### 9.1.8.2 Services and Functions



#### Reboot Device:

Initiates a restart of the LANTIME operating system. The built-in reference clock and output signals generated by the clock remain unaffected.

#### Download SNMP MIB:

Download the Meinberg SNMP MIB files. The archive file contains all Meinberg SNMP MIB files. To monitor a LANTIME time server with a V6 firmware via SNMP, only the MBG-SNMP-ROOT-MIB.mib and MBG-LANTIME-NG-MIB.mib files from the archive file are required.

#### Resend Current Error Conditions:

The button can be used to send the user the LANTIME error logs via e-mail or SNMP Trap. In order to use this function, the error events must be activated on the "Notification" page under "Notification Events" for the desired channel (eg e-mail or SNMP). An e-mail receiver or SNMP trap receiver must also be configured.

#### Reset Error Relay:

With this button the error relay can be set to an error-free position.

#### Activate Physical Identification:

This function can be used to find a LANTIME device. After the button is activated, the LANTIME starts to beep once per second and the alarm LED at the front panel flashes red. The function is terminated by pressing the "F2" button on the front panel.

#### Reset Factory Defaults:

Resets the LANTIME to factory defaults. (Attention: The network settings are retained during the reset via the web interface. If the network settings need to be reset as well, the reset must be initiated via the front panel.) During the reset, LANTIME restarts. After restarting the LANTIME can be reconfigured with the default user "root" and password "timeserver".

#### Send Test Notifications:

Sending a test notification to the configured e-mail recipients and / or SNMP trap receivers.

#### Save NTP Drift File:

The NTP service determines the offsets of the system clock at runtime and stores them in the so-called NTP drift file. This file is used by the NTP service to automatically adjust the system clock, even if no time source is currently available at short notice.

The "Save NTP Drift File" function saves the current NTP drift file /etc/ntp.drift on the internal Compact Flash card at /mnt/flash/data/ntp.drift. When the LANTIME is restarted, the value from the stored drift file can be read out by the NTP service, which accelerates the initial time adjusting process.

#### Manual Configuration:

The "Manual Configuration" button allows a direct access to the configuration files of the LANTIME. This feature should only be used by experienced administrators.

#### 9.1.8.3 Manual Configuration

**Warning:**  
Use the manual configuration only if you are a qualified administrator who is knowledgeable about the system.

**Manual Configuration**

**Standard Configuration**

- Notification Settings
- Miscellaneous Configuration

**Network Configuration**

- Network Configuration

**NTP Configuration**

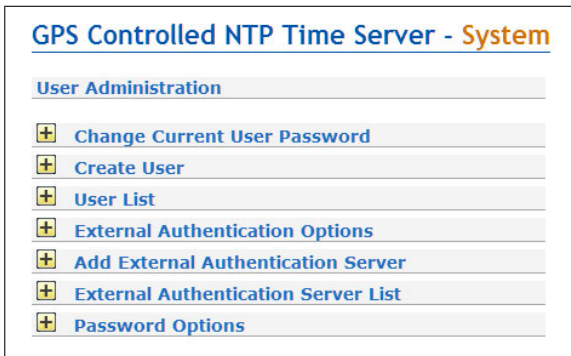
- NTP Configuration
- NTP Broadcast Configuration

- Notification Settings
- Miscellaneous Configuration
- Network Configuration
- NTP Configuration
- NTP Broadcast Configuration

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.).



#### 9.1.8.4 User Management



The screenshot displays two forms in a web interface. The first form, titled "Change Current User Password", contains two input fields: "New Password" and "Confirm Password", followed by a "Change Password" button. The second form, titled "Create User", contains four input fields: "User Name", "Password", "Confirm Password", and "Group Membership". The "Group Membership" field is a dropdown menu currently set to "Super-User", followed by a "Create User" button.

##### Change Current User Password

Here you can change the password of the currently authenticated user.

##### Create User

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.

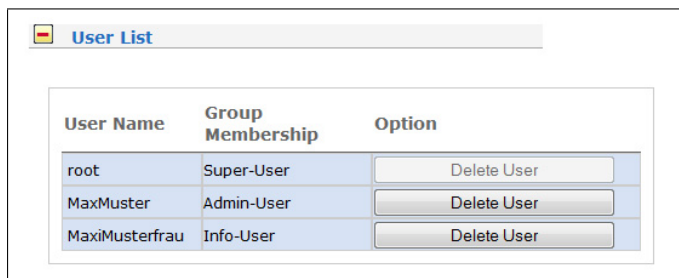
The table below illustrates the user-rights of each access level in detail.

	Super User	Admin User	Info User
Full access to the Command Line	✓		
Change device configuration through the WebUI	✓	✓	
Editing of the additional configuration files, which are available through the WebUI*	✓		
Perform Firmware Update	✓	✓	
Create a diagnostic file	✓	✓	
Create a new super user account	✓		
Review all webinterface configuration values	✓	✓	✓

\*Additional Network Configuration, Additional NTP Configuration, User defined notifications

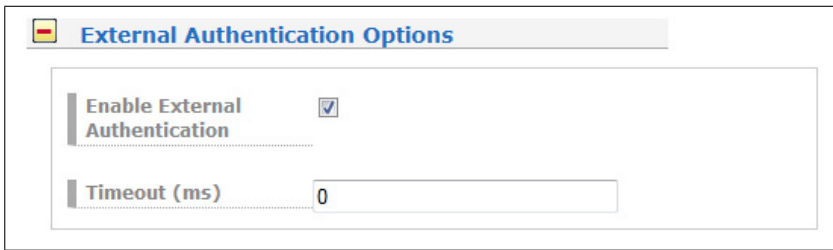
### User List

This submenu gives you an overview of all configured LANTIME users. By clicking "Delete User" a single user can be deleted.



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

### 9.1.8.5 External Authentication Options



The screenshot shows a configuration window titled "External Authentication Options". It contains two main settings:

- Enable External Authentication:** A checkbox that is currently checked.
- Timeout (ms):** A text input field containing the value "0".

The LANTIME supports Radius and TACACS as external authentication methods.

#### Enable External Authentication:

Through this checkbox you can either enable or disable the external authentication feature of the LANTIME.

#### Timeout (ms):

Period of time how long to wait for an "access accept" packet from an authentication server.

You can choose between several Authentication Methods:

#### RADIUS:

Radius stands for Remote Authentication Dial In User Service and provides centralized authentication for LAN-TIME devices. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport protocol.

The LANTIME RADIUS authentication requires that each account that should be able to login to the LANTIME has a Vendor Specific Attribute (VSA) called MBG-Management-Privilege-Level configured. This VSA has to be added to the RADIUS configuration of an external authentication server. Here some additional Information on the attribute:

```
Name = MBG-Management-Privilege-Level
Datatype = Integer
Vendor-Code = 5597
Vendor assigned attribute number = 1
Value range = 100, 200, 300
```

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

**TACACS:**

Terminal Access Controller Acc-Control System is a remote authentication protocol that gives the LANTIME the possibility to communicate with a TACACS authentication server.

The LANTIME TACACS authentication requires that each account that should be able to login to the LANTIME has configured an attribute called "priv-lvl". This attribute needs to be configured on the TACACS Server.

For a Super-User account the attribute has to be "100", for an Admin account "200" and for an Info User account "300". In the following an example of a tac\_plus server configuration file:

```
# This is the shared secret that clients have to use to access Tacacs+
key = meinberg

# User Groups

group = lantime_super_user {
    service = lantime_mgmt {
        priv-lvl = 100
    }
}

group = lantime_admin_user {
    service = lantime_mgmt {
        priv-lvl = 200
    }
}

group = lantime_info_user {
    service = lantime_mgmt {
        priv-lvl = 300
    }
}

# User

# LANTIME Super User
user = tacacs_su {
    member = lantime_super_user
    pap = cleartext „tacacs_su“ # User Password
}

# LANTIME Admin User
user = tacacs_au {
    member = lantime_admin_user
    pap = cleartext „tacacs_au“ # User Password
}

# LANTIME Info User
user = tacacs_iu {
    member = lantime_info_user
    pap = cleartext „tacacs_iu“ # User Password
}
```

## Add External Authentication Server

Through this form you can add an external authentication server to the LANTIME configuration. The external authentication has to be enabled first in the "External Authentication Options" menu.

### Authentication Method:

Configuration of the authentication method to use, either Radius or TACACS+. Detailed information on both methods can be found in the menu "External Authentication Options".

### Authentication Server:

The IP or Host of the selected Authentication Server (IPv4 and IPv6 are supported).

### Shared Secret:

A shared secret is used for a basic authentication between a LANTIME and the authentication server. The shared secret of the external authentication server has to be entered in this field. A list of allowed signs which can be used for the shared secret you can find in the chapter "Before you Start → Text and Syntax Conventions")

### Port:

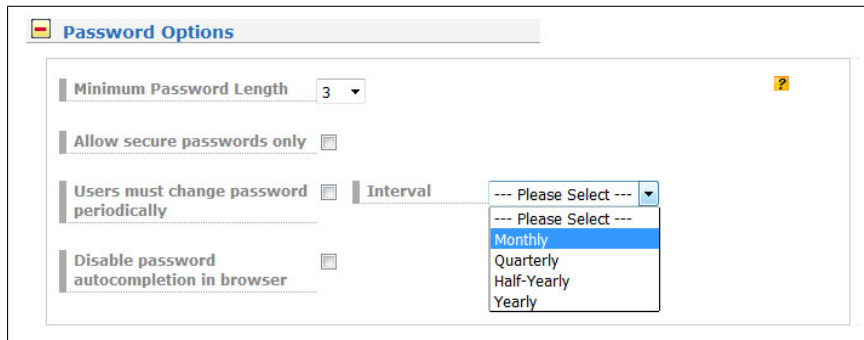
Depending on the authentication method, the default port is already configured here. If needed, the port can be changed.

## External Authentication Server List

Authentication Server	Port	Authentication Method	Option
192.168.101.1	49	TACACS+	Delete Server
192.168.101.1	1812	Radius	Delete Server

This table gives you a quick overview of the configured authentication servers. Each server can be removed by either a Super- or Admin-User by clicking the "Delete Server" button.

### 9.1.8.6 Password Options



This sub menu provides some general password settings.

#### Minimum Password Length:

This parameter sets 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. Former created passwords are not affected. The maximum length of a password is 64 characters.

#### Allow secure passwords only:

If this option is activated, only secure passwords will be allowed. A secure password needs at least:

- one lower character [a-z]
- one upper character [A-Z]
- one digit [0-9]
- one special character

A list of allowed signs which can be used as special characters you can find in the chapter "Before you Start → Text and Syntax Conventions")

#### Users must change password periodically:

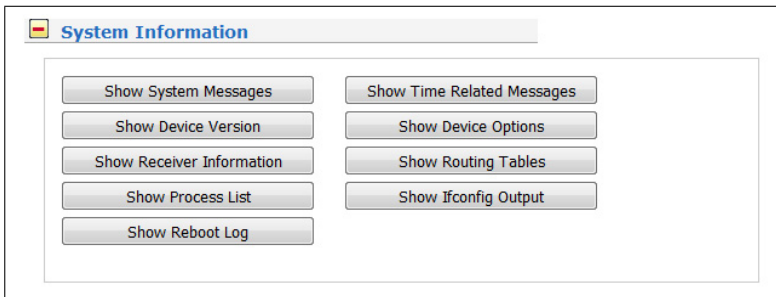
Users will be forced to change passwords at regular intervals. If a password is expired the user can not log in to the unit before changing his current password. Possible intervals:

- Monthly
- Quarterly
- Half-Yearly
- Yearly

#### Disable password autocompletion in browser:

After this feature is enabled, your browser will not autocomplete the credentials of a LANTIME.

### 9.1.8.7 System Information



The "System Information" menu offers the possibility to view important log files and setups of the LANTIME.

<b>Show System Messages:</b>	Displaying the LANTIME SYSLOG file stored in <code>/var/log/messages</code>
<b>Show Device Version:</b>	Displaying the additional device information (model, firmware, serial number, built-in hardware components, etc.)
<b>Show Receiver Information:</b>	Displaying the additional status information on the built-in reference clock.
<b>Show Process List:</b>	Displaying of all currently running processes.
<b>Show Reboot Log:</b>	Displaying the reboot logs stored in <code>/mnt/flash/data/reboot.log</code> . The log file contains information about past system reboots.
<b>Show Time Related Messages:</b>	Displaying the file <code>/var/log/lantime_messages</code> .
<b>Show Device Options:</b>	Displaying additional system parameters.
<b>Show Routing Tables:</b>	Displaying the network routing table.
<b>Show Ifconfig Output:</b>	Displaying information for all network interfaces (output of the command "ifconfig -a")

### 9.1.8.8 Firmware/Software Update



The screenshot shows a web interface for firmware/software updates. It features a title bar 'Firmware/Software Update'. Below the title bar, there is a text input field labeled 'Insert download URL'. Below that, there is a section 'or select a file' with a 'Browse...' button. To the right of the 'Browse...' button, the text 'Keine Datei ausgewählt.' is displayed. To the right of that text is a 'Start Update' button. At the bottom left of the form area is a 'Show Logfile' button.

If you need to update the software of your LANTIME, you need a specific update file. You can download the latest LANTIME firmware version from our website: <https://www.meinbergglobal.com/english/sw/firmware.htm>

The update file can be uploaded to the LANTIME by first choosing the file on your local computer with the "Browse" button and then press "Start Update". Afterwards you are prompted to confirm the start of the update process.

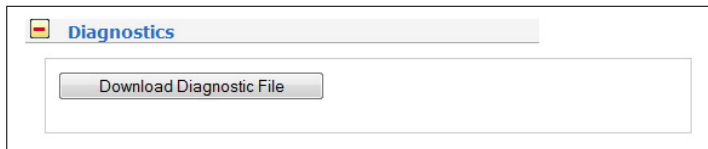
#### LANTIME - Updates for Reference Clocks and HPS Modules

Please be advised that "*Refclock Updates*" and "*HPS100 Firmware Updates*" can only be installed on systems with the LANTIME operating system LTOS Version 6.24.013 or higher. The latest Firmware Update packages are available at the following link: <https://www.meinbergglobal.com/english/sw/refclock-updates.htm>

**Note:** No new firmware revision number will be displayed under Firmware Management after a module update is installed. Refclock and HPS100 updates are enabled immediately after a reboot.



### 9.1.8.9 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 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 user to download the diagnostic file, because it is very helpful to identify the current state of the LANTIME and to find possible errors.

## 9.1.8.10 Configuration and Firmware Management

Configuration & Firmware Management

**Configuration Management**

Save Current Configuration As:

Upload Configuration:

Keine Datei ausgewählt.

Available Configurations	Options		
initial_config	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>
postconvert	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>
preconvert	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>
preupdate	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>
startup	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>	<input type="button" value="Download"/>

**Firmware Management**

Running Firmware
6.20.203-testing

Scheduled Firmware
6.20.203-testing

Available Firmware Files	Version	Type	Options	
OSV (Original Shipped Version)	6.18.014		<input type="button" value="Activate"/>	<input type="button" value="Delete"/>
fw_6.20.202-testing	6.20.202	testing	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>
fw_6.20.203-testing	6.20.203	testing	<input type="button" value="Activate"/>	<input type="button" value="Delete"/>

With this menu you can save different configuration files for backup on the flash memory of the LANTIME. By using the "Activate" button a stored configuration can be loaded, the "Delete" button can be used to delete a configuration file and the "Download" button in order to download a file.

Additionally more than one Firmware version can be archived on the LANTIME. If an updated version is not corresponding correctly in the environment, then it is possible to reactivate one of the established versions again on the LANTIME.

#### LANTIME - Updates for reference clocks and HPS modules (LTOS > 6.24.013)

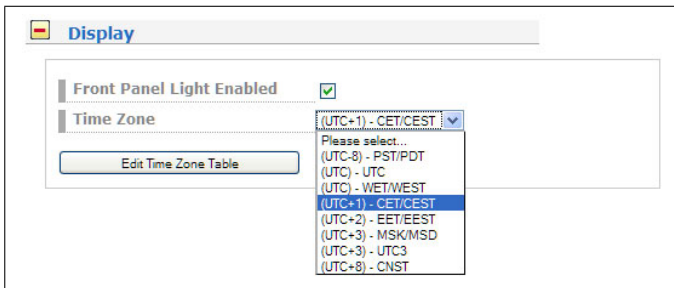
**Note:** No new firmware revision number will be displayed under Firmware Management after a module update is installed. Refclock and HPS100 updates are enabled immediately after a reboot.

LANTIME Firmware 6.24

Date: December 1, 2022

165

### 9.1.8.11 Display



#### Front Panel Light Enabled:

Through this checkbox the front panel display light can be switched on permanently.

#### Time Zone:

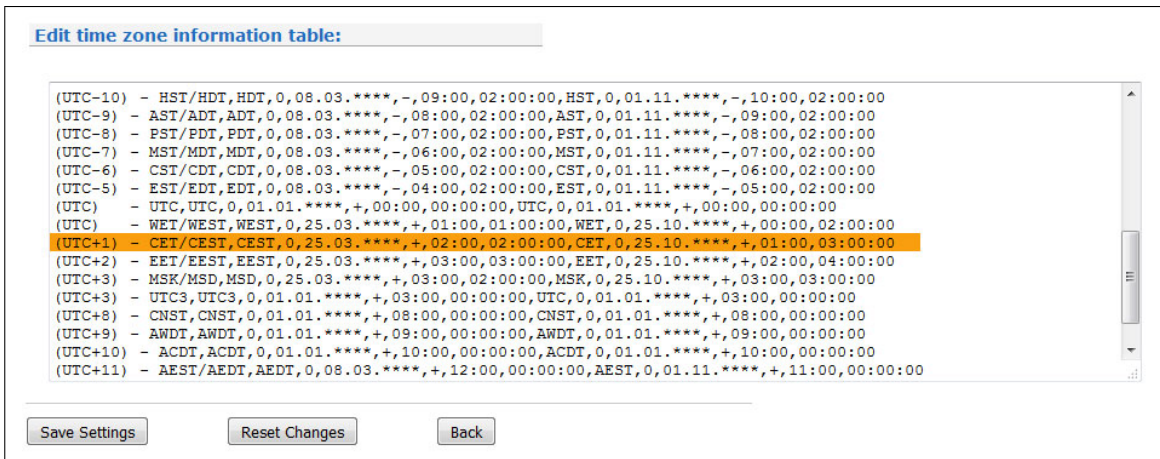
Time Zone setting for the front panel display of the LANTIME and the time which is shown in the "Date/Time" section of the Main page in the web interface. Note: This setting does not affect the time which is provided by the LANTIME through NTP, PTP, serial time strings or IRIG.

#### Exception:

In the case NTP is configured to provide local time instead of UTC you need to configure the exact local time zone here in the display time zone setting. This setting is then used for NTP as well.

#### Edit Time Zone Table:

The button "Edit Time Zone Table" can be used to add new timezone definitions.



#### Example:

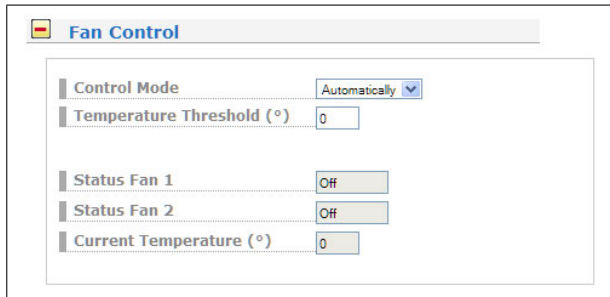
```
(UTC+1) - CET/CEST,CEST,0,25.03.****,+,02:00,02:00:00,CET,0,25.10.****,+,01:00,03:00:00
```

The string above is the time zone definition for middle Europe. If you require a new time zone setting, this needs to be configured in the same format. The string contains different information, each information is separated by a comma. A detailed description of different string parts shown by an example of the time zone setting for middle Europe is as follows:

1. Field: Display name of the time zone. This name is shown in the list of available time zones → (UTC+1) - CET/CEST
2. Field: Abbreviation of time zone with daylight saving (max 4 letter) → CEST
3. Field: Day of week of changeover to daylight saving time → 0 (Sunday)
4. Field: Date of changeover to daylight saving time (dd.mm.\*\*\*\*) → 25.03.\*\*\*\* (Changeover will take place at the first Sunday starting from 25.03.)
5. Field: Sign (+ or -) Add or subtract offset from UTC → +
6. Field: UTC Offset daylight saving (hh:mm) → 02:00
7. Field: Time of changeover → 02:00
8. Field: Abbreviation of standard time zone → CET
9. Field: Day of week of changeover to standard time → 0 (Sunday)
10. Field: Date of changeover to standard time (dd.mm.\*\*\*\*) → 25.10.\*\*\*\* (Changeover to standard time will take place at the first Sunday starting from 25.10.)
11. Field: Sign (+ or -) Add or subtract offset from UTC → +
12. Field: UTC offset (hh:mm) → 01:00
13. Field: Time of changeover → 03:00

### 9.1.8.12 Fan Control

These parameters are only available on LANTIME IMS devices with a built-in fan module.



- Control Mode:** Setting of the operating mode. The following options are available:
- Automatically:** With this mode, the fans switch on automatically as soon as the current system temperature exceeds the configured temperature threshold.
- On: In this mode the fans run permanently.  
Off: In this mode the fans are permanently turned off .
- Temperature Threshold (C°):** Specification of the system temperature threshold in degrees Celsius. The configured temperature value is taken into account for control of fans when the fan mode "Automatically" is selected.
- Status Fan 1:** Status display of the 1st fan.  
**Status Fan 2:** Status display of the 2nd fan.
- Current Temperature (C°):** Displaying the current temperature in degrees Celsius.

### 9.1.8.13 Redundant Power Supply

If your LANTIME is an IMS system, all available power supplies and power consumer are displayed and evaluated in this submenu.

#### Power Consumption Info

Shows available power results from the number of used power supply units. In the example below, we have three power supplies, each with 50 watts of power - which adds up to 100 watts + 50 watts as a redundancy reserve - a total of 150 watts when all power supplies are connected with power.

■ **Redundant Power Supply**

Status PWR 1	OK
Status PWR 2	OK
Status PWR 3	OK

Power Consumption Info

Number Power Supplies:	3/3
Available Power:	100.0W
Current Power:	51.5W
Redundancy:	Available
Overloading:	No
Number Consumer:	14

Consumer Load

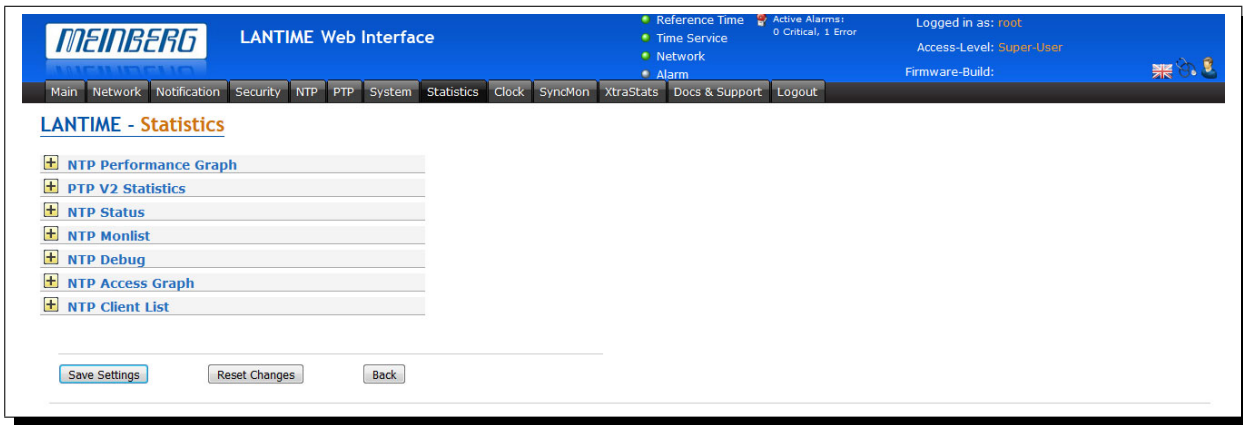
Backplane:	0.7W
Power Supplies:	4.5W
Display:	1.2W
FCU:	0.3W
GPS180 with OCXO-HQ:	6.8W
RSC180:	2.9W
GPS180:	5.0W
ELX800:	7.0W
ESI180:	1.1W
PTPv2 TSU:	5.0W
PTPv2 TSU:	5.0W
PIO180:	2.0W
PTPv2 TSU:	5.0W
PTPv2 TSU:	5.0W

As long as a value below 50W is displayed in the "Current Power" row, one power supply is sufficient to power up the system. With a value exceeding 50W, a total of three power supplies are required to ensure redundancy.

#### Consumer Load

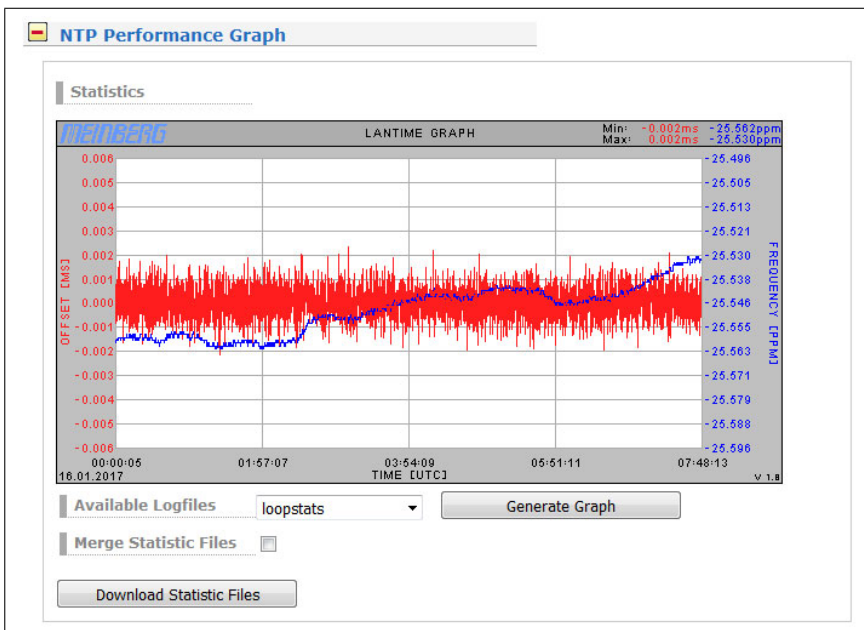
This table lists all consumers of the system. The backplane, the CPU, the power supplies, the receivers and all other modules used. The sum of all consumers gives the value that is displayed as Current Power.

## 9.1.9 Statistics



### 9.1.9.1 NTP Performance Graph

In the submenu NTP performance graph, the NTP statistics (loopstats) are displayed in the form of a graph.



The red lines and the primary Y-axis represent the offset between the system time and the NTP reference time source (in ms). The blue line and the secondary Y-axis, on the other hand, illustrate the frequency adjustment of the oscillator which is built on the CPU by the ntpd (in PPM), to adjust the system time to the reference time source.

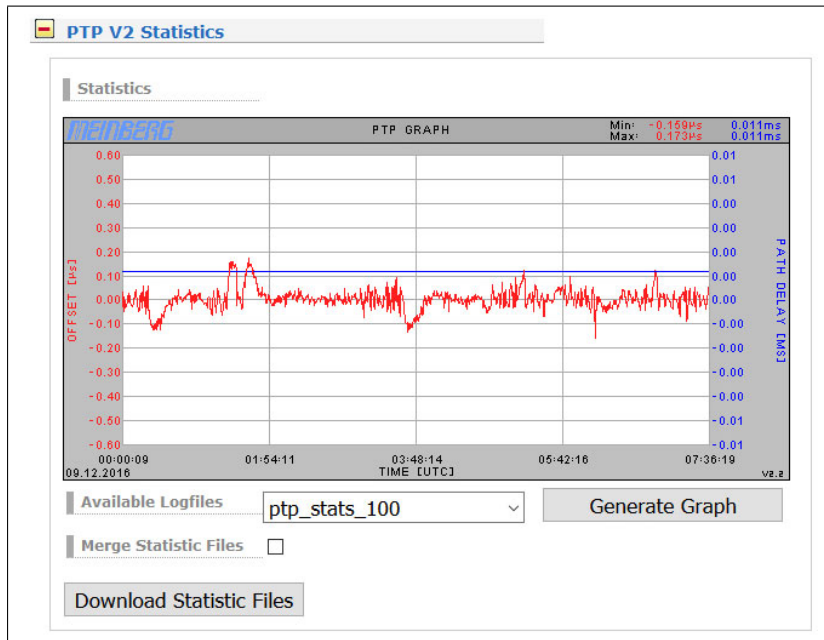
The minimum and maximum measured value of the frequency deviation and offsets can be read in the upper right corner.

#### Available Log Files:

You can select the available log data via the dropdown menu. The ntpd creates a new loopstats file for each day.

**Merge Statistic Files:**

After activating the checkbox and clicking on "Generate Graph", all available log files are merged and displayed as one graph.

**9.1.9.2 PTP V2 Statistics**

This graphic is only available if the LANTIME is equipped with a PTP module, which is configured as PTP SLAVE.

The red line shows the time offset between the time of the built-in reference clock and the incoming PTP signal (in micro s). The blue line shows the path delay determined by the PTP module.



### 9.1.9.3 NTP Status

This menu displays the output of the NTP command "ntpq -p". The command lists all reference time sources (peers) that are available to the NTP service. The following example shows the "ntpq -p" output from a LAN-TIME with a built-in GPS reference clock and 2 configured external NTP time servers:

Remote IP	Remote Host	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
o127.127.8.0	GENERIC(0)	.GPS.	0	l	6	8	377	0.000	-0.001	0.004
+131.188.3.221	ntp1.rze.uni-e	.DCFp.	1	u	13	16	377	23.274	0.205	0.166
+178.63.102.198	public.trexler.	215.184.123.138	2	u	4	16	377	19.234	0.347	0.061

**Remote IP:**

IP address of the NTP peer or 127.127.x.x if it is a hardware time reference, e.g. a radio clock or a GPS receiver.

A legend of codes standing next to each IP address of NTP peers is the following:

- '\*' This server is selected for synchronization.
- 'o' The system synchronization is derived from a pulse-per-second (PPS) signal, either indirectly via the PPS reference clock driver or directly via a kernel interface.
- '+' The peer is a candidate for synchronization.
- '-' The server is not suitable for synchronization.
- 'x' The server is detected as a falseticker and not suitable for synchronization.
- '#' The server is a survivor, but not among the first six servers.
- ' ' The peer is discarded as unreachable or synchronized to this server (sync loop).

**Remote Host:**

Resolved DNS name

**RefID:**

The time reference of the NTP peer.

**Stratum:**

Stratum value of the NTP peer.

**Type:**

Type of the NTP Peer:

- l: local reference clock
- b: broadcast or multicast
- u: unicast
- s: symmetric peer
- a: manycast

**When:**

Value in seconds. Indicates when the NTP peer was last queried.

**Poll:**

Period in seconds. Specifies the interval at which the NTP peer is queried.

**Reach:**

Octal value. Indicates the status of the last 8 queries. The value "377" means that the last 8 queries were successful.

**Delay:**

Value in ms. Displays the runtime of the NTP packet.

**Offset:**

The NTP software compares its own system time at regular intervals with its reference time sources. This process is called "polling". After each polling operation, the packet trip time is determined, calculated, and the current time difference ("offset") is calculated and displayed in milliseconds.

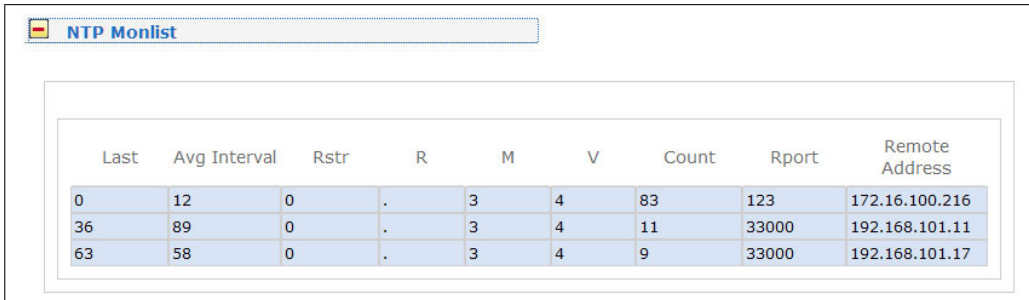
**Jitter:**

The packet trip time changes more or less depending on the characteristics of the network during the "polling" of external NTP sources at each time comparison, and the calculated time offset also varies. For this reason, the results of successive time comparisons are filtered by calculating weighted mean values for packet run time and time offset. The deviations of the individual values from these mean values are referred to as "jitter", and the higher the jitter value, the less accurate is the calculated time offset. On the other hand, a steadily increasing mean time offset indicates that the system time drifts away from the reference time. The value is displayed in milliseconds.

### 9.1.9.4 NTP Monlist

The submenu "NTP Monlist" lists all NTP clients which have queried the LANTIME time via NTP. The list is created and displayed using the NTP Query Tool. The following ntpq command is issued: ntpq -c mrulist

More information about the NTP Query Tool can be found in the NTP documentation at <http://doc.ntp.org/current-stable/ntpq.html>



The screenshot shows a window titled "NTP Monlist" containing a table with the following data:

Last	Avg Interval	Rstr	R	M	V	Count	Rport	Remote Address
0	12	0	.	3	4	83	123	172.16.100.216
36	89	0	.	3	4	11	33000	192.168.101.11
63	58	0	.	3	4	9	33000	192.168.101.17

**Last:**

Time in seconds. Specifies when the client requested the time from the LANTIME.

**Avg Interval:**

Interval: Average time in seconds between two NTP requests.

**Rstr:**

Shows if there are active Restrict Flags for this remote IP.

**R:**

Indicates whether the "Rate Control" is active or not.

**M:**

NTP package identification

- 0 → reserved
- 1 → symmetric active
- 2 → symmetric passive
- 3 → client
- 4 → server
- 5 → broadcast
- 6 → NTP control message
- 7 → reserved

**V:**

NTP Version

**Count:**

Number of packets received from the remote address

**Rport:**

"Source Port" of the last received packet

**Remote Address:**

IP Address of the requesting device

### 9.1.9.5 NTP Debug

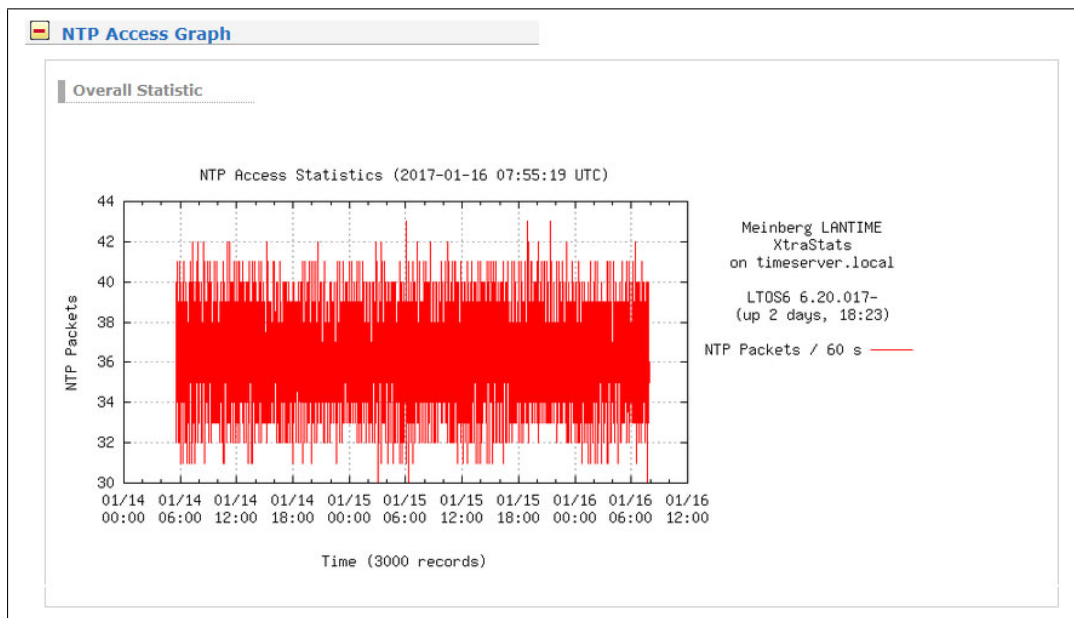
The NTP Debug submenu displays NTP debug information queried by the LANTIME using the NTP Query Tool (ntpq). The "ntpq" is executed with the following parameters:

- „clockvar“
- „associations“
- „readvar“

More information about the query tool can be found in the NTP documentation at <http://doc.ntp.org/current-stable/ntpq.html>

### 9.1.9.6 NTP Access Statistics

The LANTIME automatically counts all incoming network packets on UDP Port 123 of all available network interfaces. This statistic is graphically shown in the subchapter "NTP Access Graph". The red line indicates a value of received NTP Packets within one minute.



### 9.1.9.7 NTP Client List

In addition to the native NTP logging functions, the LANTIME offers the possibility to maintain a list of all NTP clients. The function is switched off by default, and can be activated if desired.

**NTP Client List**

Activate Logging  
 Duration of Recording: Continuously  
 Log Level: IPv4 only  
 Available Logfiles: ntp\_client\_counter\_20161209 Show

Date of Recording: 2016/12/09  
 Started at=2016-12-09 07:49:44 (UTC)  
 Total duration=00d, 00h, 00m, 35s  
 Logfile duration=00d, 00h, 00m, 35s  
 Today's clients=2  
 Total clients=2  
 Today's requests=5  
 Total requests=5

NTP Client	Requests	Options
172.16.100.130	4	<a href="#">Details</a>
192.168.101.11	1	<a href="#">Details</a>

**Activate Logging:**

Activates the feature on the LANTIME.

**Duration of Recording:**

The duration for which the LANTIME maintains the client list. When configuring continuous recording, old daily statistics are automatically cleared after a few days in order to save space.

**Log Level:**

Determines which version of the IP protocol is taken into account. Available are IPv4, IPv6 or both versions in combination.

**Available Log Files:**

If the client logging is activated, log files for display are provided at this point. Select the desired daily statistics from the selection box and use the "Show" button to display the statistics.

You will then receive a list of clients as well as other statistics.

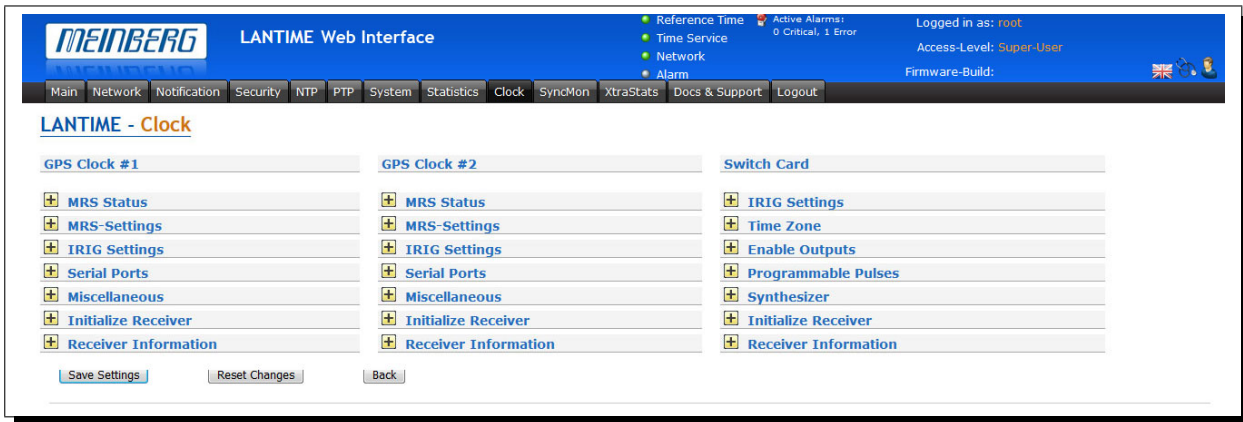
NTP Mode	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mode Other	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mode 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mode 4	55	55	55	55	55	55	55	55	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

A click on Details will now also show you detailed information about the received NTP packets of a particular client.

- Columns 0–23 indicate the hour of the day.
- The 3 additional lines provide information on whether the received NTP packet had mode 3, 4, or another. Modus 3, 4 oder einen anderen hatte.
- Modus 3 → Client
- Modus 4 → Server

### 9.1.10 Clock

On this page of the web interface, configurations can be made on the respective installed reference clocks or the changeover card.



Depending on the design of the system, which means whether it is a single reference clock or a system with two installed remote clocks and a changeover card, the web interface builds up accordingly. This also applies to the type of reference clock and its options. In case of a redundant receiver configuration the common settings for "IRIG In/Out", "Serial Ports", "Time Zone", "Enable Outputs", "Programmable Pulses" and "Synthesizers" appears into the "Switch Card" menu.

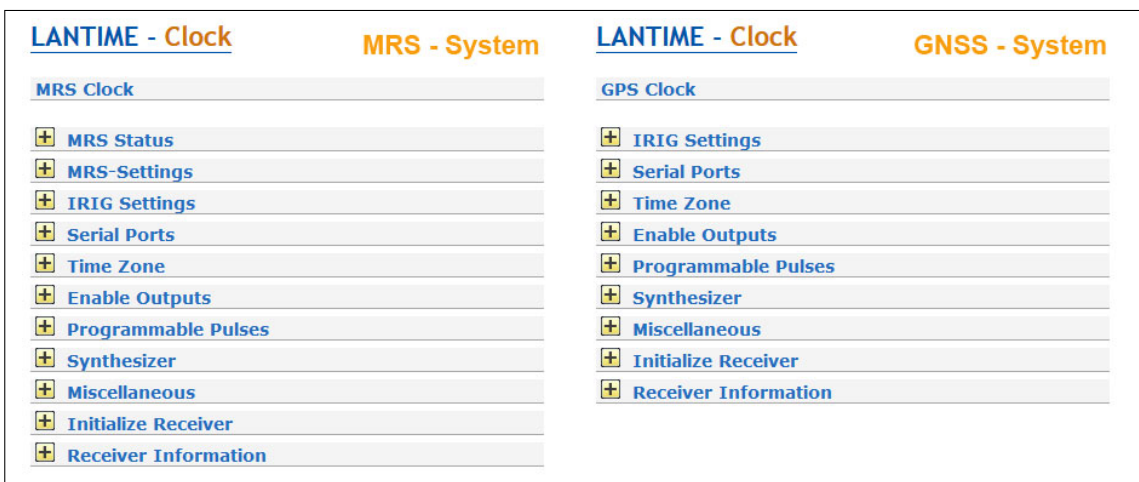


Figure: Menu "Clock" in case of a single receiver

### 9.1.10.1 MRS Status

Here the states of the reference inputs are shown:

<b>Priority:</b>	Arrangement of the time source according to your prioritization.		
<b>Source:</b>	Type of reference source.		
<b>Status:</b>	No Connection, No signal	→	the reference source is not available.
	Signal available	→	the reference source is available.
	Is master	→	the reference source is used to synchronize the system.
	Is locked	→	the system synchronizes itself to the reference source.
	Is accurate	→	Basic accuracy of synchronization reached.
<b>Offset:</b>	Time difference of the reference clock to the specified time source.		
<b>Statistics:</b>	Span	→	If the difference between the min / max value of the time source is over a defined statistical interval.
	Step-Compensation	→	Displays a hard time jump of the reference source (currently only available for PTP).
	Auto-Bias	→	Time offset determined for the source versus an offset-free time source.

Priority	Source	Status	Offset	Statistics
01	GPS	Signal available, Is master, Is locked, Is accurate	+1.0ns	
02	ext. Osc.	Signal available	-24.0ns	Auto-Bias: 0.000000000s Step-Comp.: 0.000000000s Span: 0.000000000s
-	NTP	Not prioritized	N/A	
-	PTP (IEEE1588)	Not prioritized	N/A	

Figure: An example of available reference signals in the priority order.



### 9.1.10.2 MRS Settings

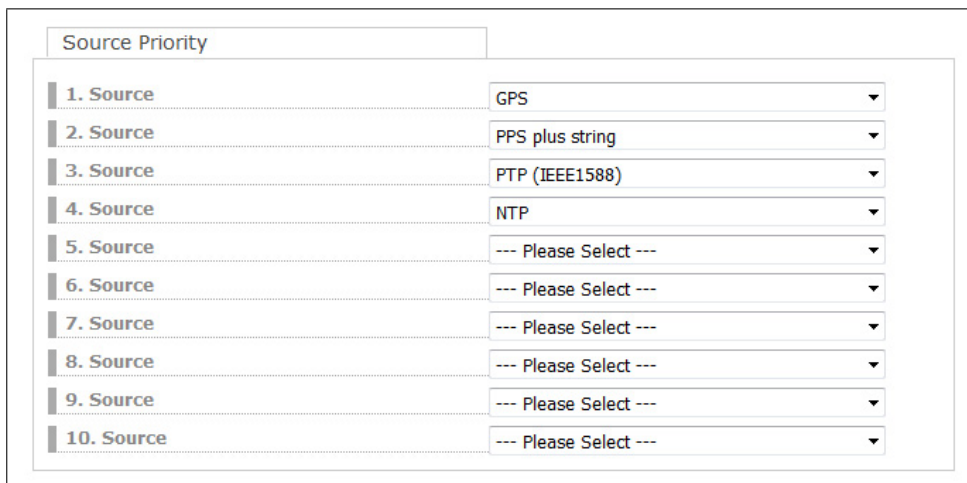
The MRS stands for a Multi Reference Source clock. This is a special functionality of a receiver that can in addition to GNSS use also other input signals as a reference for synchronization.

### 9.1.10.3 MRS Source Priority

In the MRS Settings you can configure a priority list of input signals how the switching will follow in case that a master reference becomes unavailable. The selection of signals in the list is automatically generated by the LANTIME according to the hardware configuration. The priority list of input signals should be configured in a descending order referring to the accuracy of signals.

Here is an example how to configure a priority list in a descending order:

1. Source: GNSS / GPS
2. PPS + String
3. PTP – IEEE1588
4. external NTP Server



Source Priority	
1. Source	GPS
2. Source	PPS plus string
3. Source	PTP (IEEE1588)
4. Source	NTP
5. Source	--- Please Select ---
6. Source	--- Please Select ---
7. Source	--- Please Select ---
8. Source	--- Please Select ---
9. Source	--- Please Select ---
10. Source	--- Please Select ---

Figure: Configuration example of reference signals in a descending order.

### 9.1.10.4 IRSA - Intelligent Reference Selection Algorithm

IRSA stands for an Intelligent Reference Selection Algorithm. In case that a master signal fails the IRSA takes care that the switching to the next reference signal in the priority list runs automatically and smoothly. The IRSA also takes into account the highly stable holdover performance of the local oscillator. It ensures that switching from the superior reference signal to the less accurate one is delayed as long as the highly stable oscillator can provide better accuracy in holdover than the next available reference signal in the priority list.

Reference Signal	Precision
GPS	100 ns
NTP	100000 ns
PTP (IEEE1588)	100 ns
SYNCE [MRI1]	0 ns
PPS plus string	100 ns
ext. Osc.	120 ns
PPS in (Chassis 0, Slot ESI1, Instance 0)	0 ns
10 MHz (Chassis 0, Slot ESI1, Instance 0)	0 ns
2048 kHz (Chassis 0, Slot ESI1, Instance 1)	0 ns
E1 framed (Chassis 0, Slot ESI1, Instance 2)	0 ns

Figure: Activated IRSA mode with estimated precision values for available references.

To ensure that IRSA is working properly, follow these steps:

1. Configure a priority list of available reference signals in descending order from the superior to inferior one in the MRS Settings menu (see chapter [MRS Source Priority](#)).
2. Activate IRSA in the IRSA menu. As per default the IRSA is deactivated.
3. Fill in the estimated precision values for the input reference signals in for this provided "Precision" column. According to the estimated precision values the holdover time between current source and the next source from the priority list will be calculated.

Here are some estimated precision values which you can load as defaults:

- GPS / GNSS as the first priority has the highest estimated precision :100 ns
- ext. Osc. (e.g. Rubidium): 120 ns
- PTP IEEE 1588: 100 ns
- PPS plus string: 100 ns
- NTP: 100 us

### 9.1.10.5 MRS Features

#### Advanced Source Selection

A firmware V6.24 and the following versions support a mixed combination of reference signals for synchronization. In the mixed mode you can select one source only for the ToD (Time of Day) synchronization and another source for phase and frequency. The phase and frequency can be provided by a highly stable and accurate source, for example an atomic clock, like Rubidium or Cesium.

The Time of Day (ToD) information represents a “wall clock time” – a specific time with hours, minutes, seconds and the corresponding date. The ToD information cannot be delivered by an atomic clock alone. Therefore, if you need the ToD in your system, you need to select one of the reference signal which includes the ToD information, for example GPS, NTP, PTP, PPS plus string.

If you use the mixed mode the reference clock will be steered first by a reference signal which includes the ToD. The oscillator will be roughly adjusted until it reaches the highest level of accuracy that can be achieved by this reference. After that the reference clock switches automatically to a more accurate source, for example a 1PPS coming from an external atomic clock that provides highly stable phase or a 10MHz signal to provide a stable frequency.

As per default both ToD and Phase are enabled for each available reference source. If you want to use the mixed mode, then select the ToD for one reference signal and phase for another. The reference sources you wish to use should be configured first in the Source Priority list. See MRS Settings → [MRS Source Priority](#).

Here is one configuration example for Advanced Source Selection:

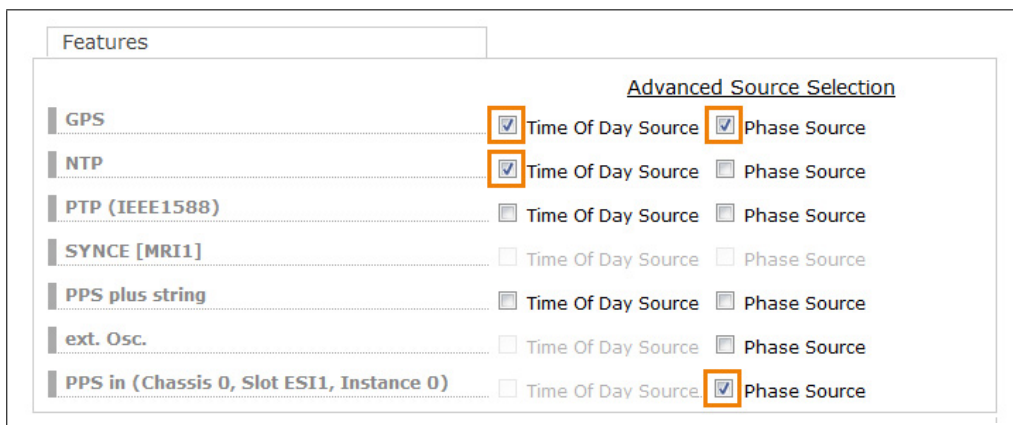


Figure: An example for a mixed combination of ToD and Phase source for given reference signals.

### 9.1.10.6 Extended Options

The Trusted Source (TRS) feature is a powerful tool to protect the GNSS<sup>1</sup> receiver from spoofing attacks. For the moment, the Trusted Source feature is supported only in combination with a Meinberg GPS or GNSS receiver and a Meinberg XHE external Rubidium holdover unit.

To activate this feature, select "Use Trusted Source" check box for the GPS reference signal. It means that GPS reference will be checked for consistency by another reference source which is acknowledged as a Trusted Source. In our case the trusted source is a Rubidium atomic clock. It is denoted as ext.Osc. (external oscillator) in the table of Extended Options. Therefore select this check box "Is Trusted Source".

Extended Options						
GPS	<input checked="" type="checkbox"/> Auto Bias Master	<input type="checkbox"/> Auto Bias Slave	<input type="checkbox"/> Is Trusted Source	<input checked="" type="checkbox"/> Use Trusted Source	<input type="checkbox"/> Asymmetry Step Detection	
NTP	<input type="checkbox"/> Auto Bias Master	<input type="checkbox"/> Auto Bias Slave	<input type="checkbox"/> Is Trusted Source	<input type="checkbox"/> Use Trusted Source	<input type="checkbox"/> Asymmetry Step Detection	
PTP (IEEE1588)	<input type="checkbox"/> Auto Bias Master	<input checked="" type="checkbox"/> Auto Bias Slave	<input type="checkbox"/> Is Trusted Source	<input type="checkbox"/> Use Trusted Source	<input checked="" type="checkbox"/> Asymmetry Step Detection	
SYNCE [MRI1]	<input type="checkbox"/> Auto Bias Master	<input type="checkbox"/> Auto Bias Slave	<input type="checkbox"/> Is Trusted Source	<input type="checkbox"/> Use Trusted Source	<input type="checkbox"/> Asymmetry Step Detection	
PPS plus string	<input checked="" type="checkbox"/> Auto Bias Master	<input type="checkbox"/> Auto Bias Slave	<input type="checkbox"/> Is Trusted Source	<input type="checkbox"/> Use Trusted Source	<input type="checkbox"/> Asymmetry Step Detection	
ext. Osc.	<input type="checkbox"/> Auto Bias Master	<input type="checkbox"/> Auto Bias Slave	<input checked="" type="checkbox"/> Is Trusted Source	<input type="checkbox"/> Use Trusted Source	<input type="checkbox"/> Asymmetry Step Detection	

Figure: An example of a Trusted Source mode of operation with an external rubidium.

The external Rubidium acts as an external oscillator that is synchronized by the GPS or GNSS Master as long as the master is available and its precision is better than the precision of the XHE. If the Master fails or for some reason uses corrupted or manipulated data the TRS will detect this as an offset limit violation. Consequently, the reference selection algorithm will discard the current master and the XHE Rubidium source will become the new master for synchronization.

Both GNSS and Rubidium reference signals need to be configured first in the Source Priority list, GPS or GNSS as "Source 1" and external Oscillator as "Source 2". All other positions should be left empty (see chapter MRS Source Priority).

Second, the IRSA Reference algorithm should be activated with corresponding precisions (see chapter IRSA - Intelligent Reference Selection Algorithm).

The precision for GPS or GNSS is at same time also the TRS limit, that the reference should comply with. If the TRS limit is violated the reference selection algorithm discards the current master and switches automatically to the Trusted Source - XHE Rubidium. For the GPS or GNSS precision value we take 250ns which is maximum time deviation allowed for the receiver.

Finally, the GPS or GNSS source should have enabled "Time of Day Source" and "Phase Source", which means that the receiver is a source for both Time of Day and Phase. At the XHE Rubidium only the Phase Source should be enabled, since the atomic clock alone does not deliver the ToD information (see chapter MRS Features).

#### Auto Bias Master / Auto Bias Slave

"Auto Bias" provides a technology for a situation where a constant offset which is present with a given input signal can be measured and compensated against a trusted reference automatically. The reasons for this constant offset could be a cable delay which introduces a fix offset (5ns per each m of coax cable and 3ns for fiber), a delay caused by an IRIG generator if IRIG is used as an input, or a constant offset via PTP due to a network or traffic asymmetry.

So, if you choose for example GPS as a reference signal at priority 1 while having "Auto Bias Master" activated for GPS, then GPS will be used as a measurement reference for all other sources as long as GPS is available.

If PTP is configured as a secondary priority with "Auto Bias Slave" activated, the constant offset of the PTP input signal is measured against the current "Auto Bias Master" reference (e.g. GPS) and will be compensated automatically.

<sup>1</sup>GPS / GNSS: The Trusted Source (TRS) feature will only work with GPS180 and GNS181 receivers.

Furthermore, even if PTP becomes a reference signal in case that a Master is not available, the PTP offsets will include a compensation for the initial offset measured against the previous Master automatically. In this operating mode a smooth transition from GPS to PTP will be possible without a time step in case GPS becomes unavailable.

If PTP is then a primary sync source and an asymmetry step suddenly occurs in the network (due to path rearrangements e.g.), the occurring asymmetry step will therefore be automatically compensated as well in case "Asymmetry Step Detection" is activated.

### **Asymmetry Step Detection**

When Asymmetry Step Detection is activated, the PTP slave does not follow hard time jumps. The soft synchronization is retained and the time jump is displayed as an offset in the MRS statistics.

With activated "Asymmetry Step Detection", the system measures the offset for approx. 10 minutes. After another 10 minutes, a determined value or offset is set, which is then displayed under MRS -> PTP status [Step Compensated]:

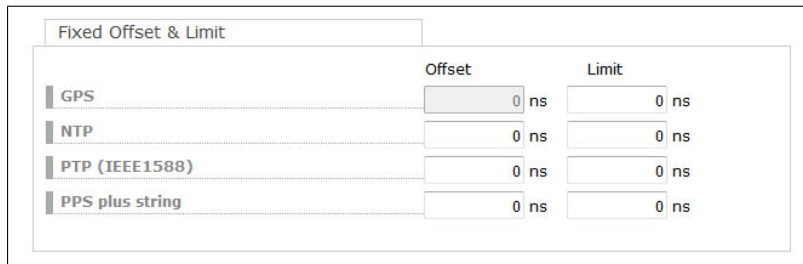
```
Auto-Bias:  0.000000000s
Step-Comp.: -0.000010001s
Span:      0.000000025s
```

### 9.1.10.7 Fixed Offset and Limit

The "Fixed Offsets" and "Limits" can be entered by using the corresponding fields. The "Fixed Offset" specifies a fixed offset for each reference clock to the reference time. With this value, known and constant deviations of a reference time source can be compensated. No constant offset can be set for GNSS references - this can only be done indirectly with the antenna cable compensation time.

#### Limit:

Here you can configure a limit value. If the reference source exceeds this limit, a notification is triggered. A configuration in the Web Interface is required on the Notification page "Notification → Notification Event → XMR Limit Exceed".



	Offset	Limit
GPS	0 ns	0 ns
NTP	0 ns	0 ns
PTP (IEEE1588)	0 ns	0 ns
PPS plus string	0 ns	0 ns

Figure: Configuration dialog for known offsets and limits.

### 9.1.10.8 IRIG Settings

The screenshot shows the 'IRIG Settings' configuration window. It includes the following fields:

- Input Timecode:** B006/B007 (DCLS)
- UTC Offset:** + 00 Hours 00 Minutes
- Output Timecode:** B006+B126
- Time Scale:** UTC

The text 'Input Settings for MRS Systems' is visible on the right side of the window.

Depending on the system configuration, the configuration of the incoming and / or outgoing time codes can be configured in this menu. There are three common time codes:

#### IRIG

B002+B122 - IRIG-B 100pps:  
DC Level Shift (DCLS), No carrier(DCLS),  
Time coding (HH,MM,SS,DDD)

Modulated, 1 kHz / 1 millisecond resolution,  
Time coding (HH,MM,SS,DDD), Control Functions

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

#### AFNOR NF S87-500

AFNOR NFS 87-500 is a standardized French timecode similar to the IRIG code, but with additional information such as day, day of month and year.

#### IEEE1344

In addition to a two-digit year, the offset to the UTC time, the current daylight saving time status and announcements from the start and the end of the summer time, as well as information about an upcoming leap second are transmitted.

#### Input Code:

Configuration of the incoming IRIG / AFNOR / IEEE 1344 time code (MRS systems only).

#### UTC Offset:

If the applied timecode is impinged with a constant time offset to UTC, this time offset must be configured here, so that the clock can convert the received time to UTC.

#### Output code:

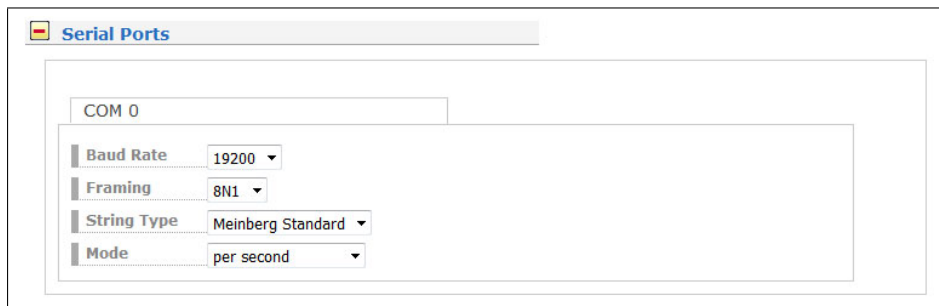
If the system has direct TC output options, you can set the parameters in this menu section.

#### Time Scale:

The output of the selected time code can be done with UTC or the local time. When "LOCAL TIME" is used, it refers to the configuration of the menu point "Time zone".

### 9.1.10.9 Serial Interfaces

Depending on the number and version of the system, the parameters for the serial interfaces can be configured in this menu.



**Baudrate:** The speed with which the serial telegram is to be transmitted:  
300, 600, 1200, 2400, 4800, 9600, 19200

**Framing:** Structure of the telegram:  
7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8E2, 8N1, 8N2, 8O1

**String Type:** Configuration of the time telegram to be sent.

**Mode:** You can configure an interval (per second, per minute, on request "?" Only) for the outgoing time string. If the operating mode is set on "Request", a connected client must send a "?" to receive the time telegram in response.

#### Features:

##### MRS PPS Plus String

If the system has the MRS "PPS plus string" option, the baudrate and framing for the incoming time string must be configured via this submenu.

##### Meinberg Capture *\*only for specific units\**

This option is for systems that have a cap input. The event is triggered by a negative edge.

Two operating modes are available for the output of the capture time stamps, "on request ? Only" and "automatically".

##### on request "?" only

The triggered events are stored in a buffer of the reference clock. As soon as a "?" is sent to the reference clock via a serial connection, the stored events are transferred from the buffer.

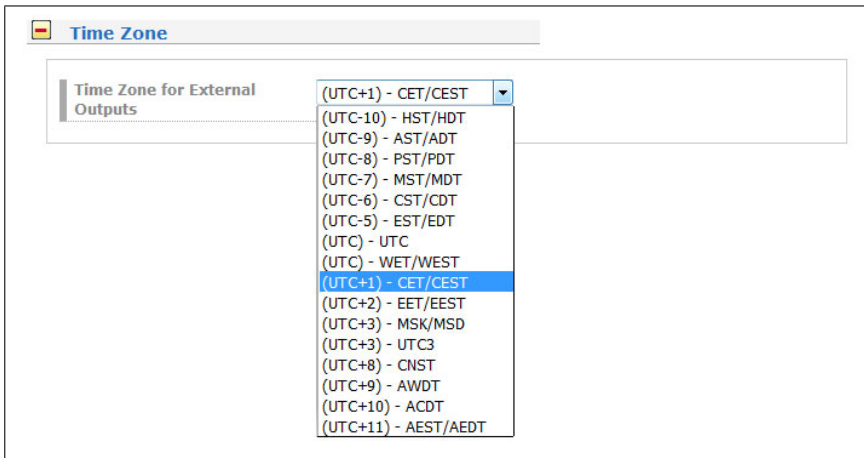
##### automatically

In this mode, the capture events are output directly on the serial interface.



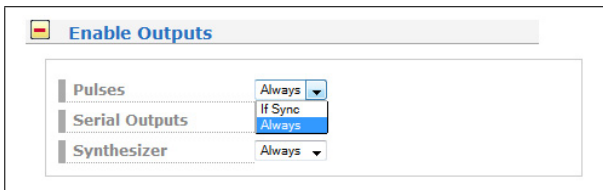
### 9.1.10.10 Time Zone

In this menu, you can configure the time zones (offsets) for the output signals (IRIG, serial interface, programmable pulses) of the reference clock.



The data of the time zone are used from the time zone table (see chapter 9.1.8.11 System → Display).

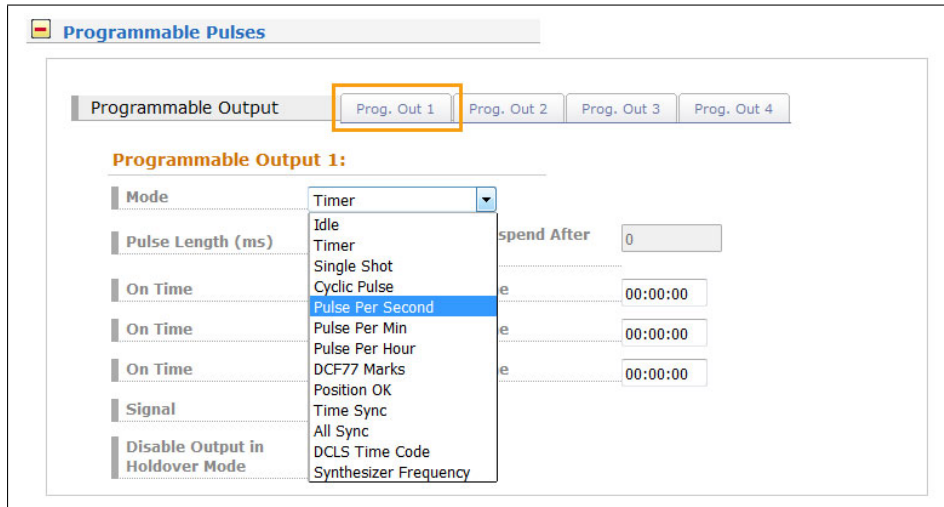
### 9.1.10.11 Enabling the Outputs



Optionally, the outputs of the reference clock can be set to always supply a signal when the device is switched on, or only when the internal clock is running synchronously.

### 9.1.10.12 Programmable Pulses

If the system has programmable switching outputs, you can configure the parameters in this menu.



**Mode:** Output signal configuration.

**Pulse length (ms):** Pulse length configuration.

**Cycle:** For "Cycle Pulse" mode, an interval can be configured in hh: mm: ss.

**Time:** In the configured mode "Single Shot", the time for the pulse can be parameterized in *hh:mm:ss*.

**DCF Suspend After (min):** In the "DCF77 Marks" mode, you can configure a shutdown time for the output port, so that in the case of an asynchrony of the reference clock, no DCF mark is available at the output.

**On / Off Time:** For the "Timer" mode, it is possible to configure start and stop times in *hh:mm:ss*.

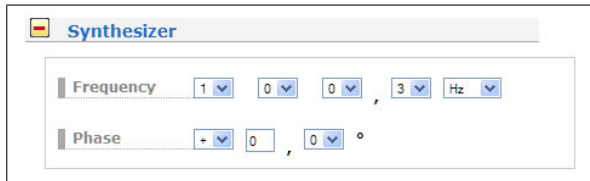
**Signal:** Configuration of the output signal active in high or low.

**Disable output in Holdover mode:** If the reference clock is asynchronous, the output signal is immediately deactivated when the checkbox is activated.

**Note:** In the clock-submenu "Enabling the Outputs" the Pulses option "if sync" must be select so that the outputs can be switched off in holdover mode.

### 9.1.10.13 Synthesizer

The output frequency and phase of the integrated synthesizer can be set here.



**Frequency:** Frequencies from 1/3 Hz up to 10 MHz can be set by entering four digits and a frequency range. By entering the frequency 0 Hz, the synthesizer can be switched off.

**Phase:** With phase you can enter the phase position of the set frequency in the range  $-180^{\circ}$  to  $+180^{\circ}$  with a resolution of 0.1. When the phase angle is increased, the delay of the output signal gets bigger. If a frequency higher than 10 kHz has been set, the phase cannot be changed.

### 9.1.10.14 Miscellaneous

This menu item displays specific options of the reference clock.

Miscellaneous
GNSS Receiver

Cable Delay Compensation Method
 By Length  By Delay

Antenna Cable Length
 m

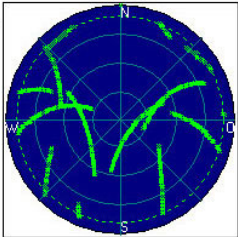
Compensation Time
 ns

---

GPS Simulation Mode

Log Satellite Visibility

Logged Satellite Visibility



GNSS Receiver

---

GPS Time Scale

SSM Quality Level Hold-off Time
 Minutes

SSM Quality Level Wait-To-Restore Time
 Minutes

PZF Receiver

---

Distance To Transmitter (km)

PZF Simulation Mode

TCR Receiver

---

TCR Simulation Mode

TCR Receiver

#### Antenna Cable Length (m):

The signal propagation time of the antenna cable can be compensated by this value. The received time grid is delayed by approx. 5ns / m antenna cable. This time error is automatically compensated by entering the cable length. The default value is 20m. The maximum input value should not exceed 2000m.

**GPS Simulation Mode:**

This menu allows the user to operate the time server without an antenna. Normally, the NTPD loses synchronization when the antenna or the external reference source is disconnected (red FAIL LED is turned on). By activating the simulation mode, the corresponding status information for the NTPD is permanently set to SYNC. This also makes it possible to transmit other times, which have been entered via the menu item "Initialize the receiver", to the NTPD. In normal cases, the checkbox should remain empty. If this box is activated, the status "Simulation mode" is displayed under "Info of the receiver" in the main menu.

**GPS Time Scale:**

**UTC** Coordinated Universal Time (including leap seconds which are continuously updated)

**GPS** since 1st of January 1980 - GPS System Time: monotonous time scale without leap seconds. Includes the leap seconds from 1970-1980.

**TAI** since the 1st of January 1970 - International Atomic Time: monotonous time scale without leap seconds. Difference to GPS Time: 19 seconds.

If you change the timescale in the drop-down menu a warning message will appear in the browser window.

**Please Note:**

If the GPS receiver is configured to output GPS or TAI timescale instead of UTC, the distributed time via NTP isn't based on UTC then. This is a protocol violation and this time server can't be used to synchronize standard NTP clients which expect UTC time.

**Log Satellite Visibility (GPS Receiver):**

If this item is activated, a graphic is generated on which the constellation of the visible satellites are displayed.

**SSM Quality Level in GPS Lock Mode:**

If the system has E1 / T1 outputs, the quality level of the SSM can be configured here.

**SNS Mode - Satellite Navigation System Mode (GNS Receiver):**

If you are using a GNS receiver (GNS or GNS-UC with Up Converter), this drop-down menu allows you to select one or more satellite systems to be used simultaneously. The following combinations are available:

GNS Receiver	GNS-UC Receiver
GPS only	GPS only
GLONASS only	Galileo only
Galileo only	GPS/Galileo
BeiDou only	
GPS/GLONASS	
GPS/Galileo	
GPS/BeiDou	
Galileo/GLONASS	
Galileo/BeiDou	
GLONASS/BeiDou	
GPS/Galileo/GLONASS	
GPS/Galileo/BeiDou	

**Distance to the Transmitter (km) - PZF / AM Receivers only:**

In the menu item "Distance to the Transmitter" you can enter the transmitter distance in km, which is used for the delay compensation of the incoming PZF-signal. The adjustment of the distance should be made as precisely as possible, because it has a direct influence on the absolute accuracy of the time raster.

**PZF Simulation Mode:**

This menu allows the user to operate the time server without an antenna. Normally, the NTPD loses synchronization when the antenna or the external reference source is disconnected (red FAIL LED is turned on). By activating the simulation mode, the corresponding status information for the NTPD is permanently set to SYNC. This also makes it possible to transmit other times, which have been entered via the menu item "Initialize the receiver", to the NTPD. In normal cases, the checkbox should remain empty. If this box is activated, the status "Simulation mode" is displayed under "Info of the receiver" in the main menu.

**9.1.10.15 Initialize Receiver**

The screenshot shows the "Initialize Receiver" menu. It features two buttons at the top: "Warm Boot Mode" and "Cold Boot Mode". Below these are three input fields for location data: "Latitude" (51° 58' 56" N), "Longitude" (9° 13' 33" E), and "Altitude" (171 m), each with a corresponding "Initialize Position" button. At the bottom, there are two more input fields: "Time (hh:mm:ss)" (11:35:41 HDT/HST) and "Date (dd.mm.yyyy)" (19.01.2017), with an "Initialize Date/Time" button. A text box on the right side of the menu states: "Time and Date appears in switch card menu in case of a redundant clock configuration".

**Warm Boot Mode only for GNSS receiver:**

This menu allows the user to switch the receiver to WARMBOOT MODE. This may be necessary if the satellite data in the battery-buffered memory is too old, or if the device is operated at a location that is several hundred kilometers away from the last operating location, since the calculation of the visibility of the satellites yields incorrect results.

**Cold Boot Modus only for GNSS receiver:**

This menu allows the user to reinitialize all GPS system values, this means that all stored satellite data will be deleted. Please note that the receiver takes about 15 minutes to read-in the information of the satellites again, to complete the cold boot!

**Coordinates (latitude, longitude, and altitude) \*only GNSS receiver:**

The absolute position of the GPS antenna can be entered here and can be sent to the GPS reference clock with "initialize Position". This option is useful when the system is operated at a different location and if started with the previously battery-buffered satellite data.

**Time/Date:**

With this function, the reference clock can manually be set to a specific date and time.

### 9.1.10.16 Receiver Information

■ Receiver Information

Common Receiver Information

Name	Value
Model:	GPS180
Serial Number:	052311436060
Software Revision:	v2.15 (Standard)
Oscillator Type:	OEXO DHQ
Supported Features:	Pulse Per Second, Programmable Synth., IRIG Out, IRIG In, Ignore Lock, Ext. Multiple Ref. Src. Cfg., Configurable Time Scale, Multiple XMRS Instances, Event Logging, IMS data
Number of Programmable Pulse Outputs:	4
Number of Serial Ports:	3

Special Receiver Information

Name	Value
GPS Status:	NORMAL OPERATION
GPS Position LLA:	LAT: 51.9827 LON: 9.2261 ALT: 165m
GPS Position LLA Degree:	LAT: 51° 58' 58" N LON: 09° 13' 34" E ALT: 165m
GPS Position XYZ:	X:3885656m Y: 631154m Z:5001745m
Number Of Satellites In View:	9
Number Of Good Satellites:	9
Selected Satellite Set:	30 18 13 19

This menu item lists all the important information and options of the reference clock.

#### Explanation of GPS Satellite Status "Satellites in View" and "Number of Good Satellites"

Satellites of the GPS and other GNSS systems are usually not stationary, but circle around the globe on well-known tracks, so each individual satellite may be above or below the horizon at a given location and time. Satellites that are below the horizon can't be tracked anyway, so the receiver uses its last known position and almanac data from the satellites to determine which satellites are currently expected to be above the horizon at its geographic position, and can potentially be tracked. All these satellites are called to be **in view**.

However, even some the satellites that are in view may be shielded by buildings, mountains, etc., so the receiver may be unable to track these satellites. Also, individual satellites may be temporarily in maintenance mode, so they must not be used even if they can be tracked. Only satellites that can be tracked and are not in maintenance mode are considered **good** and used to determine the current position and time.

So the number of **good** satellites can never exceed the number of satellites in view, but it can be significantly less if the antenna has been installed in a location with limited view to the sky. In worst case this can lead to limited accuracy, or only temporary synchronization.

### 9.1.10.17 Switch Card

The RSC (SCU) switch card is an automatic multiplexer for redundant systems with two Meinberg radio clocks. The card is used for the automatic switching of the pulse and frequency outputs as well as the serial interfaces of the connected clocks. The selection of the respectively active system is made, based on the state of the clock's generated TIME\_SYNC signals, which show the synchronous state of the clocks.

In order to avoid unnecessary switching operations, for example during periodic free running of a system, the order of the active and the reserve system is exchanged at every change-over. For example, if the active system switches to the free running mode while the reserve system is operating synchronously, it is switched over to the synchronous reserve system. A reset to the old state occurs only if the now active system (formerly the reserve system) loses synchronization, while the reserve system (previously active system) operates synchronously. If both systems operate in the free-running mode, no changeover is made and the current state is retained.

### 9.1.10.18 Receiver Information Switch Card

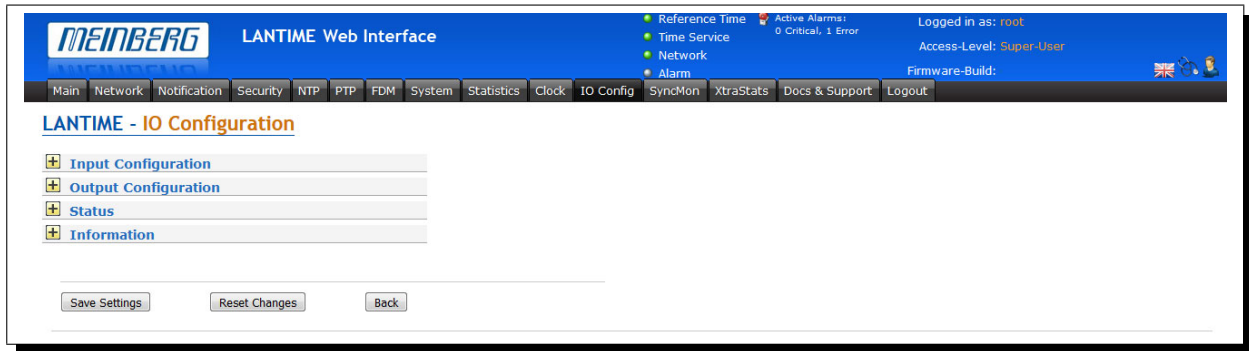
Common Receiver Information	
Name	Value
Model:	RSC180
Serial Number:	053211008860
Software Revision:	v1.18 (Standard)
Oscillator Type:	[unknown]
Supported Features:	
Number of Programmable Pulse Outputs:	0
Number of Serial Ports:	0

This menu item lists all the important information and options of the switch card.



## 9.1.11 I/O Configuration

This menu occurs in the case of an IMS system.



### 9.1.11.1 IMS Input Modules

#### 9.1.11.2 IMS-MRI (Multiple Reference Input)

If an application requires to use external synchronization sources instead of radio/GNSS signals, a MRI card enables the installed clock module to synchronize to 1PPS, 10MHz, DCLS and AM time codes.

Each MRI card is dedicated to one clock module. If a redundant solution requires external synchronization inputs for both clock modules, two MRI cards have to be installed. The MRI card is available with 4x BNC or 4x FO connectors

#### Basic reference input signals

- 1PPS
- 10 MHz
- IRIG-AM (B, AFNOR, IEEE1344 / C37.118)
- IRIG-DCLS (B, AFNOR, IEEE1344 / C37.118)

For further and detailed configuration settings of the MRI card please look at chapter 9.1.10 - "Web GUI → Clock → MRS Settings".

### 9.1.11.3 IMS-ESI (Extended Synchronization Interface)

The ESI (External Synchronization Input) card is capable of adding additional synchronization sources to an IMS system. It accepts E1 or T1 signals, both as framed signals (2.048MBit/s/1.544MBit/s, supporting SS-M/BOC) or clock inputs.

The clock inputs are configurable (1 kHz - 10 Mhz). Furthermore a 1PPS input is provided as well.

An ESI card is, as the MRI card, dedicated to one specific clock module (depending on the slot it is installed in) and can be installed in both ESI as well as MRI slots.

#### Extended reference input signals

- 1PPS, BNC
- var. frequencies (1kHz-10MHz) unframed, BNC
- var. frequencies (1kHz-10MHz) unframed, RJ45
- BITS E1/T1 framed, RJ45

**Input 1:** The input 1 is dedicated to 1PPS pulse synchronization.

The screenshot shows a web interface for configuring inputs. At the top, there are tabs for 'Input 1', 'Input 2', 'Input 3', and 'Input 4'. Below the tabs, the 'Input 1:' section is active. It features a 'Type' dropdown menu which is currently set to 'PPS in'.

**Type** – PPS in

**Input 2:** The input 2 accepts as input either 2048/1544 kHz frequency or configurable frequency in range between 1kHz and 10 MHz, also 1.544kHz if required.

The screenshot shows the configuration page for 'Input 2'. The 'Type' dropdown is set to 'Freq. In'. Below it, the 'Frequency' is set to '10' with a unit dropdown set to 'MHz'. The 'Maximum Slip' is set to '1.5' with a unit dropdown set to 'Cycles'. The 'Fixed Frequency' dropdown is set to 'T1 framed'. The 'Quality' dropdown is set to '00000' with the text 'Maximum BOC' next to it.

**Type:** Frequency input  
**Frequency:** 1 kHz-10MHz of input signal, 2048 kHz is set as default.  
**Maximum Slip:** A discontinuity of an integer number of cycles in the measured carrier phase resulting from a temporary loss of input signal. The maximum slip number can be selected in range between 0.5 – 3 cycles, with 1.5 as a default value.

#### Input 3:

See Input 2, but with RJ45 Connector and as default Frequency input 2048 kHz.

**Input 4:** As fixed frequency you can choose between E1 framed and T1 framed.

The screenshot shows a configuration window for 'Input 4' under the 'Configurable Inputs' tab. The settings are as follows:

- Type:** BITS In
- Frequency:** 0 MHz
- Maximum Slip:** 1.5 Cycles
- Fixed Frequency:** E1 framed
- Quality:** 0000 Maximum SSM
- Sa Bits:** Sa4

**Type:** BITS in.  
**Fixed Frequency:** E1 framed (2.048 MHz), T1 framed (1.544 MHz).  
**Quality:** Synchronization Status Messages (SSM), Bit-Oriented Code (BOC).  
**Sa Bits Group:** Location of transmitted SSM/BOC

**Quality Maximum SSM / Maximum BOC (quality levels for T1 framed signal)**

Synchronization Status Message (SSM) in accordance with ITU G.704-1998 standard includes 4 bit long SSM quality messages received via incoming E1 framed signal. The lower is the bit sequence the higher is quality of the source clock. The clock source quality levels according to G.704-1998 are as follows:

- 0000 QL-STU/UKN: Quality unknown
- 0001 QL-PRS: Primary Reference Source
- 0010 QL-PRC: Primary Reference Clock
- 0011 QL-INV3: not used
- 0100 QL-SSU-A/TNC: Synchronization Supply Unit A or Transit Node Clock
- 0101 QL-INV5: not used
- 0110 QL-INV6: not used
- 0111 QL-ST2: Stratum 2 Clock
- 1000 QL-SSU-B: Synchronization Supply Unit B
- 1001 QL-INV9: not used
- 1010 QL-EEC2/ST3: Ethernet Equipment Clock 2
- 1011 QL-EEC1/SEC: Ethernet Equipment Clock 1 / SDH Equipment Clock
- 1100 QL-SMC: SONET Minimum Clock
- 1101 QL-ST3E: Stratum 3E Clock
- 1110 QL-PROV: Provisionable by the Network Operator
- 1111 QL-DNU/DUS: Do not use for synchronization

With the Quality Selection box, you can select the Minimum SSM level of the incoming signal that is still acceptable as input signal. If clock reports a lower quality level than the configured minimum SSM level the system will not use it for synchronization.

**Example:**

User configured QL-SSU-B as Minimum QL for his system. An E1 input signal reporting either QL-SSU-A or QL-PRC will be allowed for synchronization, whereas a signal with quality level QL-EEC1/SEC will not be accepted.

**Sa Bits Group**

Here you can select between the Sa4 to Sa8 bit group to choose the location for SSM quality bits.

#### 9.1.11.4 IMS Output Cards

#### 9.1.11.5 IMS BPE

##### BPE (Basic Port Expansion)

The BPE is a passiv card, that provides the signals, which are generated by the reference clock. The customer can choose between different physical connectors and signal levels.

The BPE is pre-configured with the following signals:

- 1PPS, 10 MHz TTL
- 2048 kHz
- Programmable Pulses, provided by clock module
- IRIG DCLS+AM (B, AFNOR, IEEE1344 / C37.118)

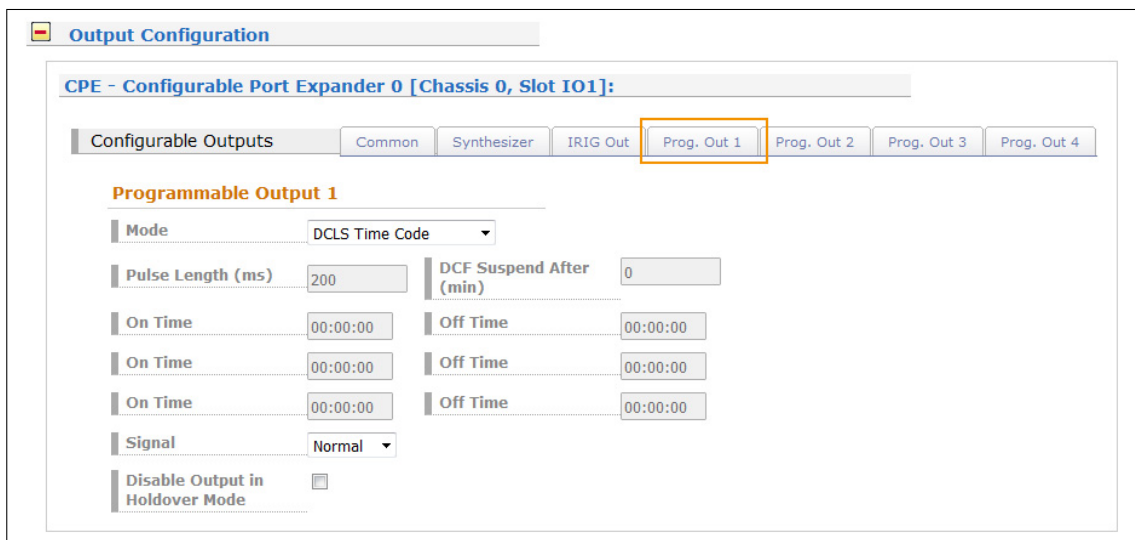
There are no other configuration settings for a BPE card in the I/O Chapter. For further detailed settings on output signals of the BPE card please proceed to the Clock Configuration Chapter 9.1.10.

### 9.1.11.6 IMS - CPE

This module consists of a half-size standard controller card (Back-End) and a dockable port expander card (Front-End), allowing a large variety of available and programmable output signals and physical connectors, including various electrical and optical interfaces.

#### IMS – CPE available Signals:

- 1PPS, 10 MHz
- Time Codes: IRIG A/B/E/G/AFNOR/IEEE1344/C37.118/NASA36
- Frequency Synthesizer (sine- wave + TTL)
- Programmable Pulses: 1PPS, 1PPM, 1PPH, Timer. Single Shot
- Cyclic Pulses; DCF77 Mark, Sync Status
- Serial Timestrings (RS232 o RS 422 / 485)



#### Mode:

**Idle Mode** Selecting "Idle" deactivates the output.

**Timer Mode** This mode simulates a programmable day assigned timer. Three turn-off and turn-on times are programmable for each output. If you want to program a switch time, change the turn-on time "On time" and the corresponding turn-off time "Off time".

A turn-on time later than the turn-off time would cause a switch program running over midnight. For example a program "On time" 10:45:00, "Off time" 9:30:00 would cause an active output from 10:45 to 9:30 (the next day!). If one or more of the three switching times are unused just enter the same time into the values "On time" and "Off time". In this case the switch time does not affect the output.

**Single Shot Modus** Selecting Single Shot generates a single pulse of defined length once per day. You can enter the time when the pulse is generated with the "Time" value. The value "Length" determines the pulse duration. The pulse duration can vary from 10 msec to 10 sec in steps of 10 msec.

**Cyclic Pulse mode** generating of periodically repeated pulses

The value of "Cycle" determines the time between two consecutive pulses. This cycle time must be entered as hours, minutes and seconds. The pulse train is synchronized at 0:00 o'clock local time, so the first pulse of a day always occurs at midnight. A cycle time of 2 seconds for example, would cause pulses at 0:00:00, 0:00:02, 0:00:04 etc. Basically it is possible to enter any cycle time between 0 and 24 hours, however usually a cycle times that cause a constant distance between all consecutive pulses make sense.

**For example:** a cycle time of 1 hour 45 minutes would cause a pulse every 6300 seconds (starting from 0 o'clock). The appearing distance between the last pulse of a day and the first pulse of the next day (0:00:00 o'clock) would be only 4500 sec. The value in entry field "Cycle" turns red, when entering a time that causes this asymmetry.

#### Pulses

Per Second, Per Min, Per Hour Modes

These modes generate pulses of defined length once per second, once per minute or once per hour. The value "Length" determines the pulse duration. The pulse duration can vary from 10 msec to 10 sec in steps of 10 msec.

#### DCF77 Marks

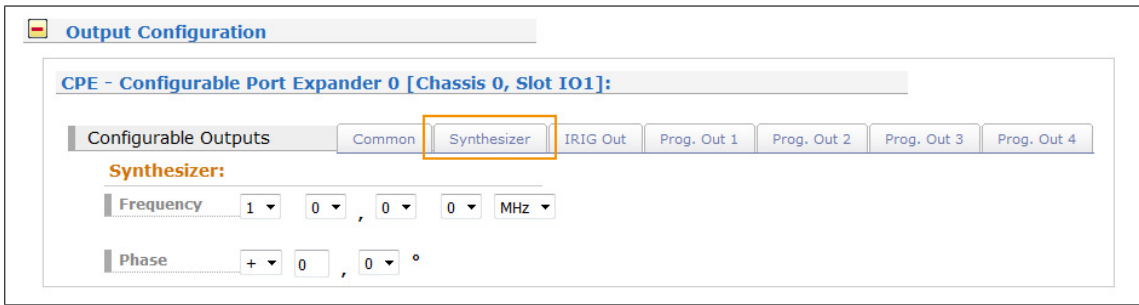
In "DCF77 Marks" mode the selected output simulates the telegram as transmitted by german time code transmitter DCF77. The generated time code is related to the local time zone. If you want DCF simulation to be disabled when the clock is in free running mode, you can enter the delay (given in minutes) for deactivating the DCF-Simulation with the "Timeout" value. DCF Simulation is never suspended, if the delay value is zero.

#### Submenu Common:



**Time Zone** - Choose local timezone

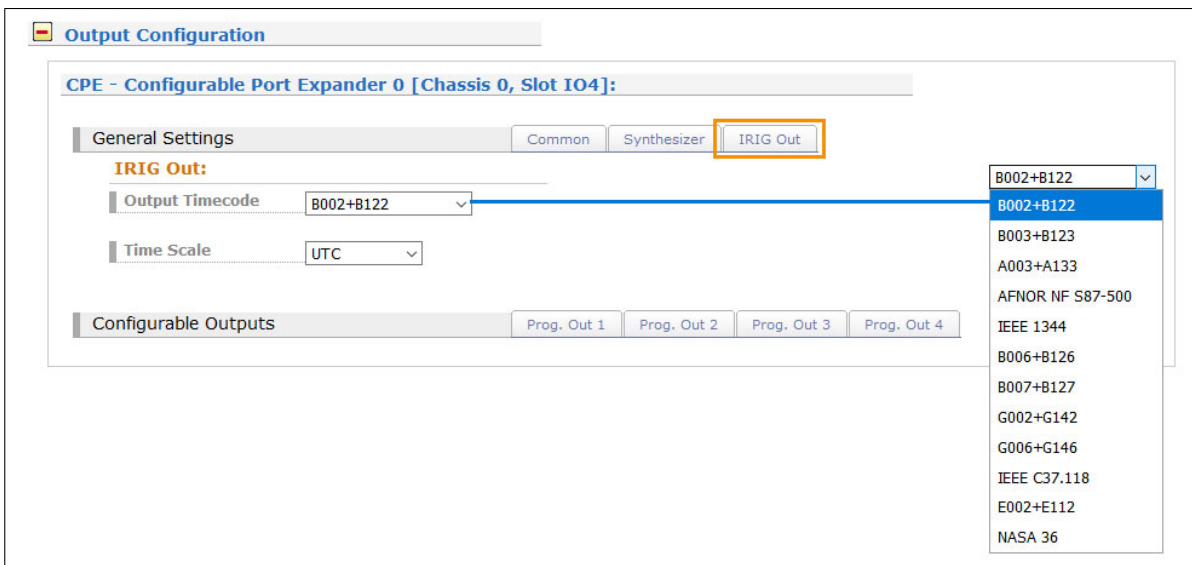
Submenu Synthesizer:



**Frequency**      1/8 Hz to 10 kHz: Phase synchronous to pulse per second  
 10 kHz to 10 MHz: deviation of frequency < 0.0047 Hz

**Phase**            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" It is possible to 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!

IRIG Out



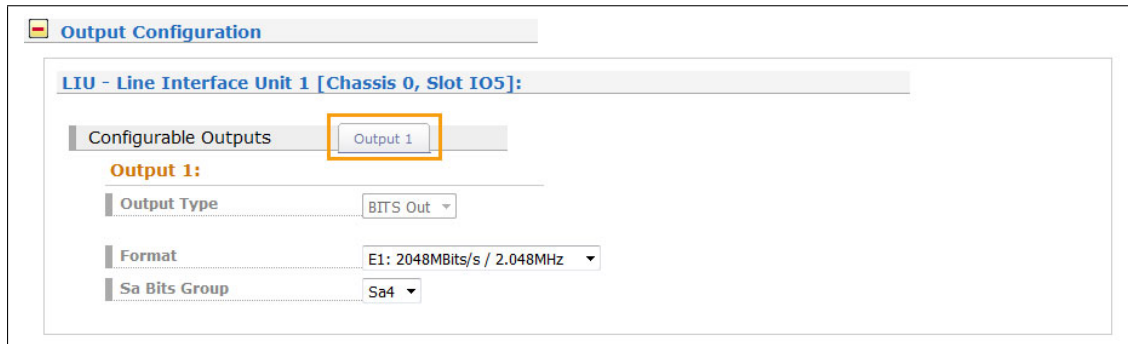
**IRIG Output Code**    Output code which is distribute in the system to all cards.

**Time Scale**            UTC or local time.

### 9.1.11.7 IMS - LIU (Line Interface Unit)

#### E1/T1 – generator available with 4 or 8 outputs

Generation of reference clocks for synchronization tasks the module LIU (Line Interface Unit) generates different reference clock pulses which are derived from the GPS-locked master oscillator of a preconnected GPS clock. The output signals are available with high accuracy and stability therefore.



#### Submenu Output 1:

##### Output Type

**Clock Outputs:** 2.048 MHz (E1-mode) or 1.544 MHz (T1-mode), G.703, 75 Ohm, unbalanced or 2.048 MHz (E1-mode) or 1.544 MHz (T1-mode), G.703, 120 Ohm, balanced.

**BITS** framed outputs with SSM/BOC support:  
2.048 Mbit/s (E1-mode) or 1.544 Mbit/s (T1-mode), 75 Ohm unbalanced  
or 2.048 MPs (E1-mode) or 1.544 Mbit/s (T1-mode), 120 Ohm, balanced.

**Format** E1 framed (2.048 kBit) or T1 framed (1.544 kBit)

**Quality** Sa Bit group location of SSM QL bits

With the pull-down menu "Output Configuration" the available outputs of the I/O slots can be configured:

#### Output Configuration of a LIU module (Line Interface Unit):

In this menu one can select between E1 or T1 mode for the LIU outputs. The selected mode is the same for all outputs.

#### T1 or E1?

T1 is a digital carrier signal that transmits the DS - 1 signal. It has a data rate of about 1.544 Mbit/second. It contains 24 digital channels and therefore requires a device that has a digital connection.

E1 is the european equivalent to T1. T1 is the North American term whereas E1 is a European term for digital transmission. The data rate of E1 is about 2 Mbit/second. It has 32 channels at the speed of 64 Kbit/second. 2 channels among 32 are already reserved.

One channel is used for signaling while the other is used for controlling. The difference between T1 and E1 lies in the number of channels here.

#### Sa Bits

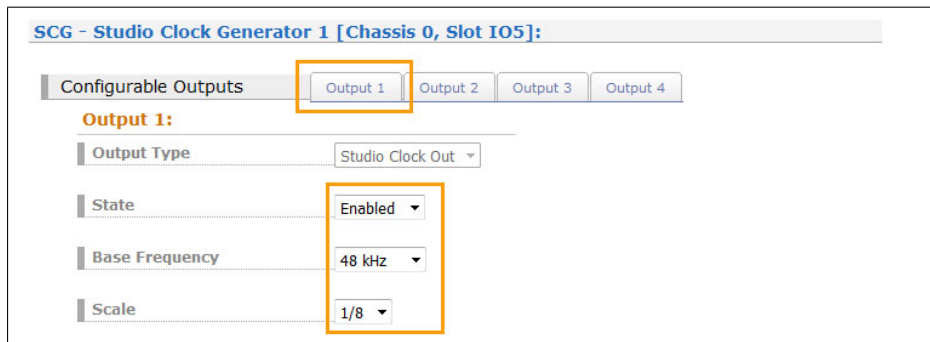
ITU-T Recommendations allow for bits Sa4 to Sa8 to be used in specific point-to-point applications (e.g. transcoder equipment) within national borders. When these bits are not used and on links crossing an international border they should be set to 1.



The Sa4 bit may be used as a message-based data link for operation, maintenance and performance monitoring. The SSM Bit (Synchronization Status Message) can be selected in the Web GUI for clock quality information. Sa4 is selected as default.

## 9.1.11.8 IMS - SCG Studio Clock Generator

## SCG-U - Word Clock Generator, unbalanced



This module is not only designed for our IMS series and generates various audio frequencies for studio applications. The SCG module can also operate in our 19-inch rackmount and 1U Multipac chassis.

- Programmable word clock rates: 24Hz – 12,888MHz
- reference inputs: 1PPS, 10MHz, serial timestring

<b>Output Type</b>	Studio Clock Out (Word Clock) or Digital Audio Out (DARS)
<b>State</b>	on or off
<b>Base Frequency</b>	32kHz, 44.1kHz, 48kHz
<b>Scale</b>	possible scales depends on base frequency choose a base frequency and a scale to get the right frequency at output x

**Example:** Output 3 state Enabled base 48kHz, scale 1/8

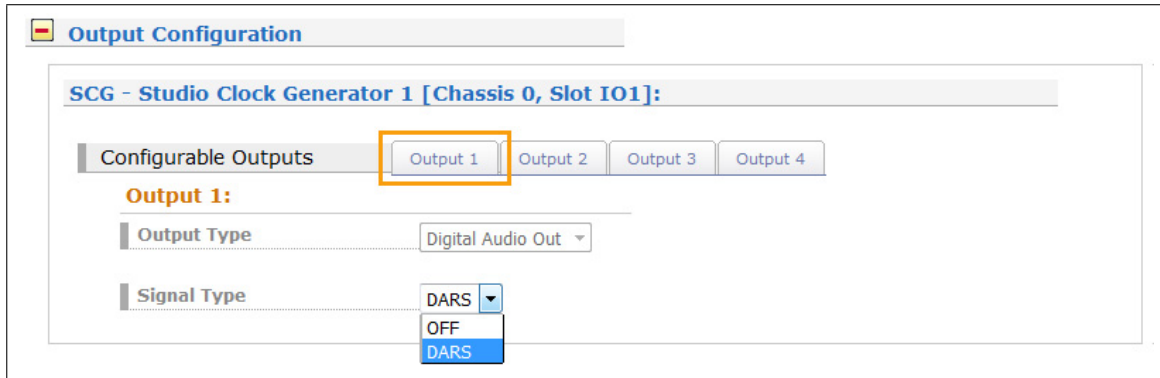
$48\text{kHz} * 1/8 = 6\text{kHz}$  on output1

Output1 = Base-Frequency \* Scale

### SCG-B - DARS Generator, balanced

The SCG-B is an additional card for generating "Digital Audio Reference Signals" for studio applications. The 25pin D-Sub female connector provides four DARS outputs, which can be configured here in the IO Config menu.

#### Sample Configuration: SCG-B Output 1



In the menu "IO Configuration" you can set the output on DARS for every output of the SCG-B. The four available outputs can optionally be switched off.

### 9.1.11.9 IMS - VSG

The VSG is a video signal reference for Studio Equipment with four BNC outputs. The Module generates 1x bi-level sync (Black Burst) and 1x Tri-Level Sync and 2x Sync Signals (H-Sync, V-Sync, ...). The LANTIME Web Interface can be used for output signal configuration and to query the state of the VSG.

#### Functionality

The board is synchronized by an external 10MHz signal. It generates configurable video signals in different formats. The generated signals have a phase reference to 1PPS.

- Four BNC outputs @ 75Ω with configurable video formats and Sync Signals
  - Out 1: HD-Syncs (Tri-Level Sync)
  - Out 2: SD-Syncs (Bi-Level-Sync)
  - Out 3: Sync Signale (H-Sync, V-Sync, ...)
  - Out 4: DARS
- Four LEDs: Signal status of module and outputs
- Supported Video-Formats:
  - PAL, NTSC(SD)
  - 720p/50Hz (SMPTE296M3)(HD)
  - 1080i/25Hz (SMPTE274M6)(HD)
  - 720p/59,94Hz (SMPTE296M1)(HD)
  - 1080i/29,97Hz (SMPTE274M7)(HD)

<b>Output Type:</b>	Video Out or DARS
<b>Epoch:</b>	start epoch of first frame
<b>Format:</b>	<b>Out1</b> supports HD formats only: 720p/50Hz (SMPTE296M3), 1080i/25Hz (SMPTE274M6), 720p/59,94Hz, 1080i/29,97Hz (SMPTE274M7) <b>Out2</b> supports SD Formats only: PAL, NTSC
<b>Phase-Offset:</b>	Phase offset in 10ns steps (range: -32768ns...32767ns)

**9.1.11.10 IMS - LNO (Low Noise Option)**

The IMS-LNO is a 10MHz generator card, which provides 10MHz sine signals with low phase noise to 4 external outputs. The card has a microprocessor system, which monitors the output signals and generates status signals for the upper-level management system accordingly. It can be used in our modular IMS Systems and also be applied in M900 timeserver platform and GPS based 3U housing, but without management functions.

The card has a high quality oscillator, which is locked to an external 10MHz signal. The microprocessor monitors the lock status of the PLL and the warm up phase of the oscillator. It activates the outputs only after the phase is locked.

This condition is signalized by the LEDs. In the phase locked state, the output levels of the four outputs are monitored, and in case of a failure signalized by an associated LED.

	Non-IMS-Systems	IMS-Systems
First LED	<b>Status Output 1</b> Green: Ok Red: Error	<b>St - Status of the LNO180 card</b> Green: 10MHz reference ok and PLL has locked Yellow: 10MHz reference ok but PLL is not locked yet Red: No 10MHz reference detected
Second LED	<b>Status Output 2</b> Green: Ok Red: Error	<b>In - 10MHz reference and PLL status</b> Green: Ok, 10MHz available at both outputs Red: Error, no signal at one or both outputs
Third LED	<b>Status Output 3</b> Green: Ok Red: Error	<b>A - Output 1-2 status</b> Green: Ok, 10MHz available at both outputs Red: Error, no signal at one or both outputs
Fourth LED	<b>Status Output 4</b> Green: Ok Red: Error	<b>B - Output 3-4 status</b> Green: Ok, 10MHz available at both outputs Red: Error, no signal at one or both outputs

*Output can not be active, before PLL is locked.*

### 9.1.11.11 Other Output Modules

#### Network Cards:

##### **LNE**

The LNE card adds additional network interfaces to the management CPU, increasing the number of NTP and management ports available.

The additional ports can be used to separate network traffic on physical network segments. For further configuration options please see the chapter "Ref -> Chp. Network".

For further detailed configuration settings for this card please see chapter 9.1.2, "Web GUI → Network menu".

##### **TSU - IEEE 1588 Time Stamp Unit**

The Meinberg time stamping unit provides a future-proof platform for your IEEE 1588 / SyncE / Carrier Grade NTP infrastructure. The high-power dual-core processor, the 1-step master clock and the 1GE interface with SFP slot supports a large number of PTP clients.

The ability to select Master and Slave operation for either Default, Power, Telecom or SMPTE profile makes this product the most flexible PTP solution on the market, suitable for a wide range of applications.

A lot of IEEE 1588 slave devices or NTP clients from different market segments can be synchronized, even over IPv6 networks, for example eNodeB's for LTE base stations, Linux servers with hardware-assisted time stamping support for high-frequency trading applications, IEEE 1588 compatible IEDs in Smart Grid environments or IP-interconnected Audio / Video devices in broadcast studios.

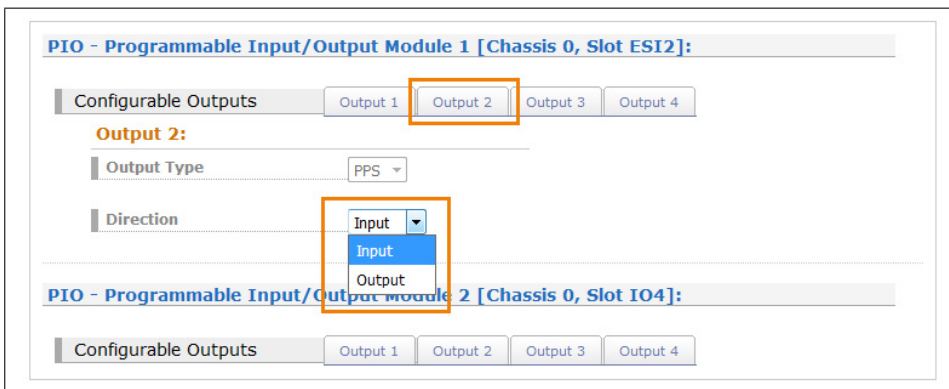
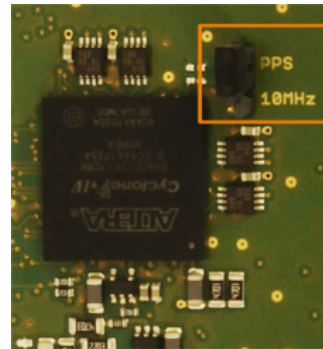
The Synchronous Ethernet function provides a high accurate frequency transport over Ethernet networks. The card can be used either to take a SyncE signal from the network as a source or generate SyncE as a Master.

For further information on PTP features and detailed configuration for this card please proceed to Chapter 9.1.6, "Web GUI → PTP menu".

9.1.11.12 IMS Input/Output Cards

9.1.11.13 PIO - PPS/10MHz Input/Output Module

The PIO module is pre-configured by a jumper. The default configuration of all ports is PPS (Pulse Per Second). If this pre-configuration needs to be changed to 10MHz, the card must be removed and the jumper position adjusted.



Via the web interface, each port can be set separately to "Input" or "Output". If a port is set to "Output", the system PPS or the 10 MHz reference frequency is output signal at this port. If a port is set to "Input" the incoming signal is compared to the system PPS or to the 10MHz reference frequency. The offset values are displayed in the status window.

**PIO - Programmable Input/Output Module 1 [Chassis 0, Slot ESI2]:**

Available Inputs	Type	Status	Offset
Input 1	PPS in	Input signal is currently lost	0.000000000s
Input 2	PPS in	Input signal is currently lost	0.000000000s
Input 3	PPS in	Carrier detected, Input signal is avail	-0.000000016s
Input 4	PPS in	Input signal is currently lost	0.000000000s

Temperature Sensor 1	Temperature Sensor 2
Current: 46.25°C	Current: 43.25°C

9.1.12 Sync Monitoring

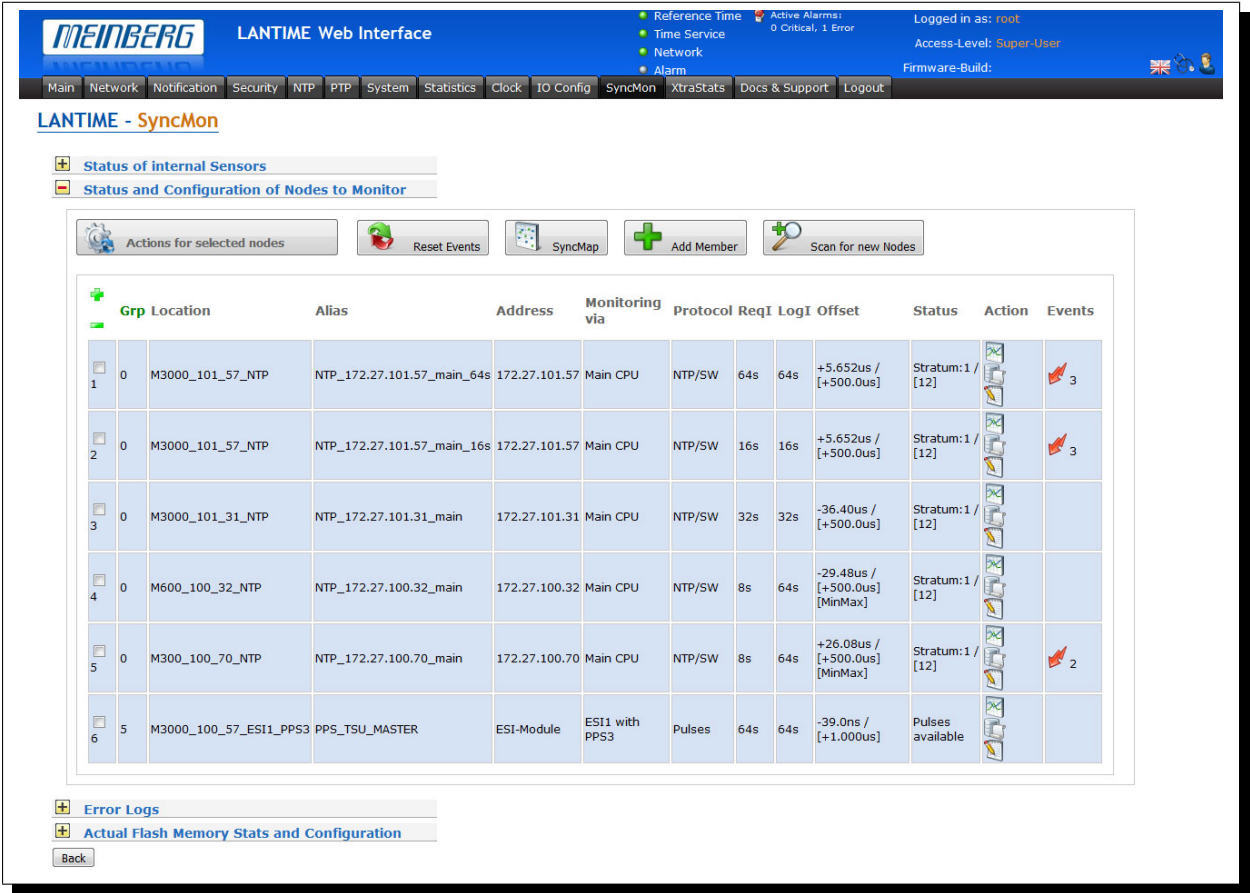


Figure: Sync Monitor dialog in the LANTIME Web GUI.



### 9.1.12.1 Sync Monitoring Introduction

The Sync Monitoring feature is used for measuring, monitoring and reporting of network nodes' accuracy against a UTC traceable source (eg. GPS, multi-GNSS or national timing service, e.g. NPL). The Sync Monitoring node can monitor nodes synchronized by network protocols PTP (IEEE 1588v2) or NTP (RFC1305).

PTP nodes need to support the Meinberg TLV approach or standard PTPv2 Management messages, otherwise they cannot be monitored. NTP nodes can only be monitored if they are configured to respond to NTP client requests (Note: A NTP client that is using the Windows Time Service W32Time does not respond to NTP client requests per default configuration. W32Time needs to be configured to act as client and server at the same time. Otherwise the node cannot be monitored via SyncMon).

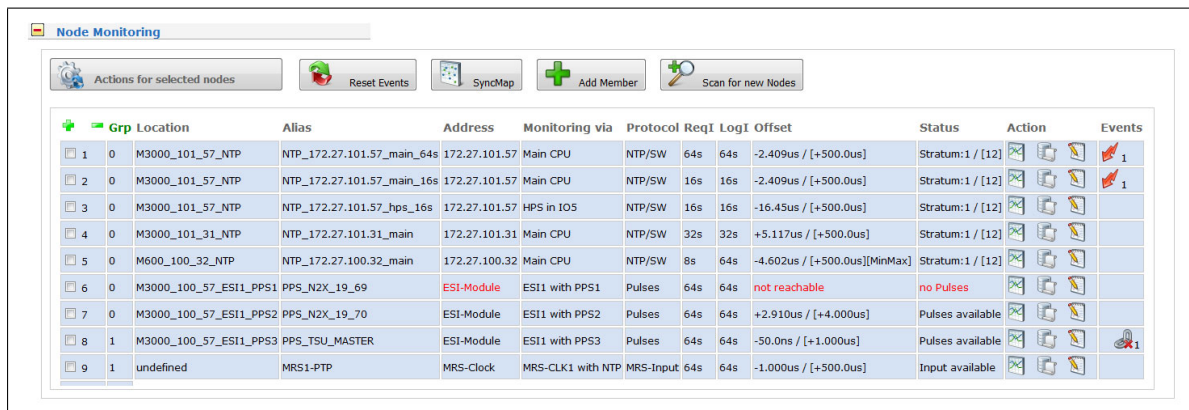
However, also all configured MRS and ESI inputs (like PPS and Freq inputs) can be monitored if an ESI (Extension Signal Input) card is available. The Sync Monitor feature is now available on Meinberg IMS Systems with firmware version 6.22 or later and for PTP monitoring with integrated HPS-100 PTP card with a minimum 1024 client performance license.

The Sync Monitor can run either as a node independent from a master clock. In this case a Sync Monitor node can be located basically anywhere in the network; but most probably as close as possible to the slaves to be able to measure their actual accuracy. At the same time you can monitor also the performance of a GM and measure the potential network asymmetry which is present in the link between a GM and the Sync Monitoring Node.

It is possible to configure up to 1000 nodes for monitoring in the Sync Monitoring interface running on a standard LANTIME or IMS System. You can specify monitoring and logging intervals for each individual node separately. Besides, an offset limit can be configured for each node which triggers an alarm notification (via SNMP, email, relay output or a user defined channel) if the limit for this particular node is exceeded. For NTP nodes you can define also a stratum limit, which can also trigger an alarming when the defined limit is exceeded.

Moreover, for each node it is possible to download all the monitoring data and its log files which can be used to generate a report or for further statistical analysis.

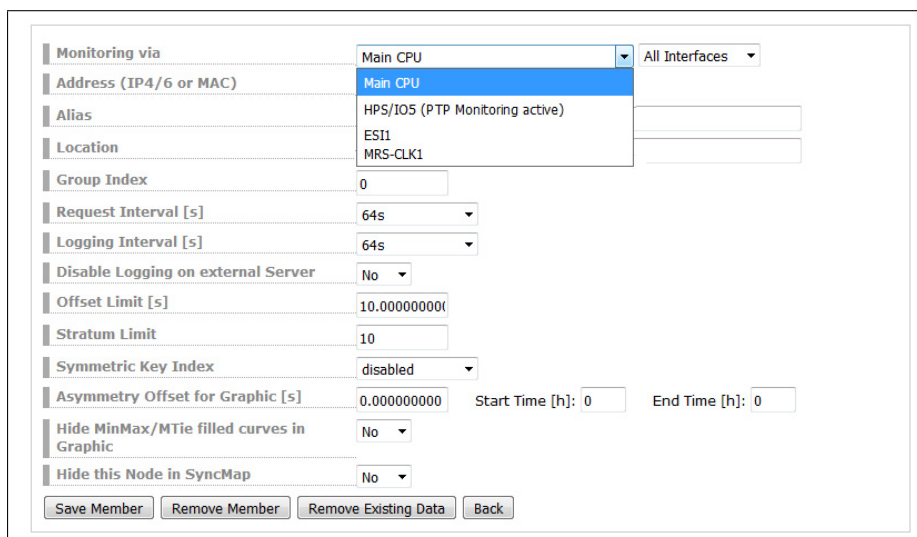
### 9.1.12.2 Sync Monitor Status and Configuration via WEB Interface



Grp	Location	Alias	Address	Monitoring via	Protocol	ReqI	LogI	Offset	Status	Action	Events
1	0	M3000_101_57_NTP	NTP_172.27.101.57_main_64s	172.27.101.57	Main CPU	NTP/SW	64s	64s	-2.409us / [+500.0us]	Stratum:1 / [12]	1
2	0	M3000_101_57_NTP	NTP_172.27.101.57_main_16s	172.27.101.57	Main CPU	NTP/SW	16s	16s	-2.409us / [+500.0us]	Stratum:1 / [12]	1
3	0	M3000_101_57_NTP	NTP_172.27.101.57_hps_16s	172.27.101.57	HPS in IO5	NTP/SW	16s	16s	-16.45us / [+500.0us]	Stratum:1 / [12]	
4	0	M3000_101_31_NTP	NTP_172.27.101.31_main	172.27.101.31	Main CPU	NTP/SW	32s	32s	+5.117us / [+500.0us]	Stratum:1 / [12]	
5	0	M600_100_32_NTP	NTP_172.27.100.32_main	172.27.100.32	Main CPU	NTP/SW	8s	64s	-4.602us / [+500.0us][MinMax]	Stratum:1 / [12]	
6	0	M3000_100_57_ESI1_PPS1	PPS_N2X_19_69	ESI-Module	ESI1 with PPS1	Pulses	64s	64s	not reachable	no Pulses	
7	0	M3000_100_57_ESI1_PPS2	PPS_N2X_19_70	ESI-Module	ESI1 with PPS2	Pulses	64s	64s	+2.910us / [+4.000us]	Pulses available	
8	1	M3000_100_57_ESI1_PPS3	PPS_TSU_MASTER	ESI-Module	ESI1 with PPS3	Pulses	64s	64s	-50.0ns / [+1.000us]	Pulses available	1
9	1	undefined	MRS1-PTP	MRS-Clock	MRS-CLK1 with NTP	MRS-Input	64s	64s	-1.000us / [+500.0us]	Input available	

Figure: Sync Monitor user interface on LANTIME systems with a FW 6.24 or later.

In the Sync Monitor Status and Configuration dialogue you can add new members for measuring their accuracy and monitoring their sync performance. By selecting a "+" Add member button you will proceed to an enter configuration dialog in order to add a new node for monitoring.



Monitoring via: Main CPU (dropdown), All Interfaces (dropdown)

Address (IP4/6 or MAC): Main CPU (dropdown)

Alias: HPS/IO5 (PTP Monitoring active)

Location: ESI1, MRS-CLK1

Group Index: 0

Request Interval [s]: 64s (dropdown)

Logging Interval [s]: 64s (dropdown)

Disable Logging on external Server: No (dropdown)

Offset Limit [s]: 10.00000000

Stratum Limit: 10

Symmetric Key Index: disabled (dropdown)

Asymmetry Offset for Graphic [s]: 0.00000000 Start Time [h]: 0 End Time [h]: 0

Hide MinMax/MTie filled curves in Graphic: No (dropdown)

Hide this Node in SyncMap: No (dropdown)

Buttons: Save Member, Remove Member, Remove Existing Data, Back

Figure: Add member configuration dialog.

The features in the "Add Member" configuration dialog have the following configuration options:

#### Monitoring via:

Select a monitoring instance from the drop down list. The drop down list appears differently in different HW configurations. The following options are available:

**Main CPU:** This monitoring instance is always available and is not dependent on HW configuration of the LANTIME system. It can monitor native NTP nodes only, which are responding to NTP client requests (Note: A NTP client that is using the Windows Time Service W32Time does not respond to NTP client requests per default configuration. W32Time needs to be configured to act as client and server at the same time. Otherwise the node cannot be monitored via SyncMon). All assigned interfaces can be monitored at the same time or you can select a particular interface from a list if available.

- HPS:** [Slot card position, e.g. I04] - this monitoring instance can monitor PTP nodes, supporting protocols PTP with TLV (proprietary for a Meinberg Sync Node), PTP with MGMT (defined in the IEEE 1588v2 standard) and NTP with software time stamping.
- ESI:** This monitoring instance can monitor PPS and Freq nodes with Extension Signal Input (ESI) card. From a dropdown list you can select which particular signal you wish to monitor. Options available are: PPS0, Freq In0, Freq In1, BITS In2
- MRS-CLK:** This monitoring instance can monitor all activated MRS/XMR input signals for each MRS-reference clock. From a dropdown list you can select which signal you want to monitor. Options available are: GNSS/ GPS, NTP, PTP, PPS, IRIG, 10MHz, E1, 2048kHz, - (depending on HW options → see [Clock](#) tab in the Web interface).

**Address (IP4/6 or MAC):**

IPv4 or IPv6 or MAC address of a node you want to monitor over the network.

**Alias:**

Alias name for a monitoring node to find it easily in the complete table overview. The alias name which is configured by the user will define the name of the directory on flash disc ('Base Path for logfiles for history of days') of each node. The alias name has to be unique and one word without blanks with a maximum length of 63 characters. It is possible to monitor the same node (e.g. the same IP-address) with different alias names - this may be useful if you want to monitor the same node from different monitoring modules (e.g. different HPS100 IMS cards with separate network paths).

**Location:**

Enter a physical location of a monitoring node for you to recognize this node easily in the complete table. The location name has to be one word without blanks with a maximum length of 63 characters.

**Group Index:**

You can group monitored nodes within a logical group by assigning them the same index, (e.g. nodes with the same group index may be of the same kind (NTP, PTP, PPS), or at the same location, etc.)

**Request Interval (s):**

Interval in seconds by which a monitoring node sends monitoring requests to the slaves / clients. The min request interval is 1s, the max is 3600s. A default interval is 64s. If the Request Interval is disabled (0) then no requests will be sent to the nodes and no data will be logged.

**Logging Interval (s):**

Interval in seconds by which the measured offset and stratum are written to a logfile. If the log-interval is disabled then no data will be stored to the logfile. If the request interval has been activated and the log-interval has been disabled then the nodes will be monitored and limits and notifications will be checked but no data will be stored. If the Request Interval is lower than the Logging Interval then the mean value of the measured offsets at request interval will be logged and the Minimum and Maximum values in the log-interval will be stored additionally.

**Disable Logging on external Server:**

The measured or logged data can be send via SYSLOG protocol to an external Syslog server. This can be disabled for each node (see System settings synchronization scripts).

**Offset Limit (s):**

Offset threshold value in seconds. The measured offset between a node and the reference will be compared to the configured threshold. If the calculated difference is higher than the configured offset limit the LANTIME will generate an alarm "Sync Monitor" (which can be sent as a notification eMail, SNMP trap or to an external syslog server).

**Stratum Limit:**

Threshold value for a NTP stratum level. If the stratum level of a monitored client is higher than the configured stratum limit, it will generate an alarm (sent by eMail, SNMP trap or to an external syslog server).

**Symmetric Key Index:**

If you want to use symmetric key authentication for SyncMon then select a key index from the list of already applied keys. If the keys are not yet defined, proceed to the NTP dialog in the Web GUI → NTP Symmetric Keys and generate a new key file, which should be stored and activated on the monitored node as well. For more information about Symmetric Key Generation please proceed to LTOS6 Configuration → NTP → NTP Symmetric Keys.

**Asymmetry Offset for Graphic:**

If a constant asymmetry of the measured nodes is known then you can set this value for the graphical output – the logged values will not be modified – the asymmetry offset is like a fix offset for graphic monitoring only.

**Start and End Time:**

These parameters will define a fix mask for displaying the graphic from Start Time to the End Time. The logged data will not be modified.

**Hide Min/Max/MTie filled curves in Graphic:**

If the request-interval is lower than the log-interval additional values for Min and Max will be stored in the logfiles. These Min/Max values will be displayed as a filled curve in a gray color behind the logged offset curve. This feature can be disabled.

**Hide this Node in SyncMap:**

You can disable a specific node in the SyncMap.

If a HPS card at a corresponding slot [IMS Slot card position, e.g IO5] is the selected monitoring instance with a PTP option then you will get an additional feature to configure instead of a stratum value and besides, no symmetric keys are available.

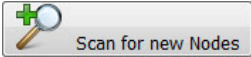
**Domain:**

A logical group of PTP devices defined within a physical network. Only nodes with the same domain number can see PTP messages from other nodes in the same domain.

When you are finished with configuration of a new monitored node, save the current configuration by clicking the "Save Member" button. By clicking the "Remove Member" button you will remove the currently selected node from the complete list of all monitored nodes. All sampled data for the particular node will be lost if you did not back-up the saved data prior its removal.

By clicking the "Remove Existing Data" button all data for only this specific node will be erased.

### 9.1.12.3 Scan for New Nodes



Scan for new Nodes is an automatic search for NTP and PTP nodes within your network.

Search for Nodes via HPS/IO5 (PTP Monitoring active)

**Found 10 PTP Nodes on HPS in IO5 (scanned with PTP Management Messages from domain 0)**  
 Last Scan of PTP Nodes has been done at 2017-11-02/UTC/15:38:08. Press Scan button to restart scanning for PTP nodes

PTP Domain

Location

Group Index

Request Interval [s]

Logging Interval [s]

Offset Limit [s]

PTP UUID	MAC Address	IP Address	Vendor	Feature	Dom	Status	Offset	Delay	Select
EC4670FFFE00CEC3	EC467000CEC3	192.168.100.010	Oreg	PTP/TLV	0	Slave	-0.000000163s	0.000009243s	<input checked="" type="checkbox"/> 1
EC4670FFFE00BF67	EC467000BF67	172.027.037.116	Oreg	PTP/TLV	0	Passive	0.000000000s	0.000000000s	<input type="checkbox"/> 2
EC4670FFFE00BF65	EC467000BF65	172.027.037.015	Oreg	PTP/TLV	0	Passive	0.000000000s	0.000000000s	<input type="checkbox"/> 3
EC4670FFFE00BD5C	EC467000BD5C	172.027.084.152	Oreg	PTP/TLV	0	Passive	0.000000000s	0.000000000s	<input type="checkbox"/> 4
EC4670FFFE00CFF1	EC467000CFF1	172.027.101.073	Oreg	PTP/TLV	0	Passive	0.000000000s	0.000000000s	<input type="checkbox"/> 5
001B21FFFE04AD5F	001B2104AD5F	172.027.037.008	ptpd	PTP/MGMT	0	Slave	0.000014162s	0.000061849s	<input type="checkbox"/> 6
EC4670FFFE0069F9	EC46700069F9	172.027.084.156	Oreg	PTP/TLV	0	Master	0.000000000s	0.000000000s	<input type="checkbox"/> 7
EC4670FFFE00BEE8	EC467000BEE8	172.027.037.066	Oreg	PTP/TLV	0	Passive	0.000000000s	0.000000000s	<input type="checkbox"/> 8
EC4670FFFE00604C	EC467000604C	172.027.019.235	MBG;	PTP/MGMT	0	Slave	0.000000000s	0.000014266s	<input type="checkbox"/> 9
EC4670FFFE006939	EC4670006939	172.027.019.094	Oreg	PTP/TLV	0	Master	0.000000000s	0.000000000s	<input type="checkbox"/> 10

Figure: Scan for new Nodes dialog. Only newly found nodes will appear in this temporary table. Select nodes which you wish to add in the overall monitoring node table.

#### Search for Nodes via:

First select an instance from a dropdown list to use for searching of new nodes. Possible options are "Main CPU" and "HPS" card. With the Main CPU you can search for NTP nodes only.

#### IP-Range start at:

Set the starting IP Address where the search will start with the automatic NTP scan. In the dropdown list you will find all subnet ranges of each network interface.

#### Number of IP Address to scan for:

This parameter will set a number of IP-addresses which will be scanned. To each IP address from the IP-Range a separate NTP packet request will be sent. If a NTP client answers to this request and its IP address has not yet been configured then this node will appear in the table.

With select-boxes new nodes can be added automatically to the list of the monitored nodes. The parameters for Location, Group Index, Request Interval, Logging Interval, Offset Limit and Stratum Limit can be defined at the next step, before adding them in the table with other monitored nodes.

Figure: To scan the network for PTP nodes a HPS card with activated monitoring has to be selected first in the Search for Nodes dropdown list.

#### PTP Domain:

The network connected to that HPS card will be scanned in the domain, which was defined here by user. The following mappings as defined in IEEE 1588-2008 will be scanned:

- UDP/IPv4/Ethernet,
- UDP/IPv6/Ethernet,
- Ethernet (IEEE 802.3, layer 2).

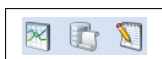
When starting the scan first a PTP Management message will be sent in broadcast mode to get the "port state" of each PTP node - this will be done with IPv4, IPv6 and Layer2.

All PTP nodes which answer to this request will ask for the "current status" and "clock status" with management messages that follow. The result will be displayed as a list of all available PTP nodes. Each new PTP Node will be entered in an overview table of the available nodes.

Only new nodes which have not yet been configured will be shown in the table. For each node the PTP-UUID, MAC-Address, IP-Address, Vendor name, Feature (if a node supports PTP with extended TLV for monitoring or PTP management messages only), Domain number, Status (the current PTP status like Slave, Master, Listening ...), Offset and Delay (current measured values from PTP management message) will be automatically displayed in the table. With select-boxes new nodes can be added automatically to the list of the monitored nodes. The parameters for Location, Group Index, Request Interval, Logging Interval, Offset Limit and Stratum Limit can be defined in the next step before adding the selected nodes.

The monitoring engine will start to send PTP/NTP requests in the configured intervals to each node from the list and measure the time received in the responses with its own time (which is traceable to UTC, GNSS sync for example). The current offset and status information can be checked in the status overview table in the Node Monitoring menu.

In the status overview table of monitored nodes, next to the status information you will find 3 action buttons: Graph, Error Logs and Edit.



By selecting the Graph button a Graphical Diagram for the selected node will show up. At this page you find several features for different representation options.

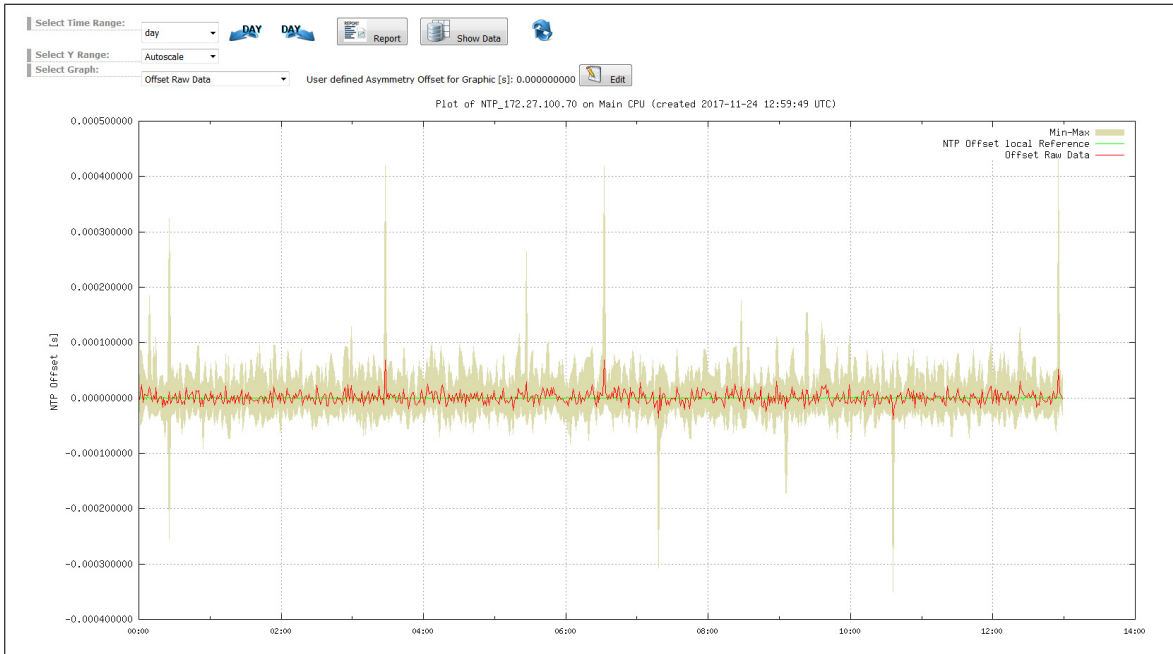


Figure: Graphical diagram of offset values for each node, selectable for different time ranges (day, week, month or manual selection). With given buttons at the "Select Time Range" you can select either past or future intervals for the graphical representation.

Offsets are collected for each NTP/PTP or PPS monitored node and can be depicted as graphical representation for selectable time intervals in the web UI of the SyncMon node.

The monitored data are continuously saved on the Sync node "Base Path for logfiles for current day" and will be saved automatically to the Flash Card ('Base Path for logfiles for history of days') at change of a day at 0:00 UTC. Data are available at any time for further statistic processing.

The red line represents the offset between a Sync node reference time and the measured time of a monitored device. For PTP and PPS signals, the sync node reference is an internal reference time from the receiver (e.g. multi GNSS (GPS, GLONASS, Galileo, Beidou), external UTC time service, IRIG TC, long wave time reference: eg. PZF, MSF, WWVB ...). The sync node reference is depicted as a green line. For multi GNSS reference clock in normal operation you will see something in the lower nano second range with 5ns resolution.

For NTP monitored signal the Sync node is synchronized the internal NTP that is in sync by an internal reference clock (multi GNSS or IRIG TC, long wave ...). In this case the green line in the graph represents the internal NTP system time.

**Select Time Range:**

There are different time ranges to choose from. By day, week, month and manual. When selecting the manual time range click on "select now" to display the graph with the selected time range. For other options it is also possible to go back to see data in the past.

**Select Y Range:**

Different options available: autoscale, or fixed Y ranges in decade intervals: 100ns, 1us, 10us, 100us, 1ms, 10ms and 100ms.

**Select Graph:**

Different graph options are available for NTP and PTP nodes.

For NTP nodes it is possible to view a graph either as **raw data** or with applied **Median Filter** or a graph of the internal reference only (the green line).

For PTP nodes, selected graph modes are:

**Reported offset from a PTP node** (data obtained from a PTP node by a standard MGMT protocol).

**Measured offset to a PTP node** (offset of a PTP slave measured against the internal reference). The measurements are available only for PTP slaves which support monitoring PTP protocol with TLVs. Along with the measured values obtained by reverse PTP, also reported value curve is available and MTIE filled curve if MIN and MAX value measurement is supported on the monitored node.

You can also select the internal reference graph only.

For PPS nodes monitored via an ESI input card at the Sync node, you will have the graph modes available: raw data, data with applied Median Filter and Internal Reference only (a PPS from an internal reference clock.)

If the request-interval is less than the log-interval then additional Min/Max values for that log-interval will be stored in the data files. These Min/Max values will be added automatically as a filled curve in the graphical diagram and the mean value will be shown as red line in that filled Min/Max curve.

### Report Button:



With this selection the current data of the monitored node will be prepared in a form of a report. You can also select a time frame for sampled data from which a report will be generated. The report includes the current status data, monitor configuration, monitoring statistical values over the selected time frame, a graphical diagram and a full sync map related to the monitored node.

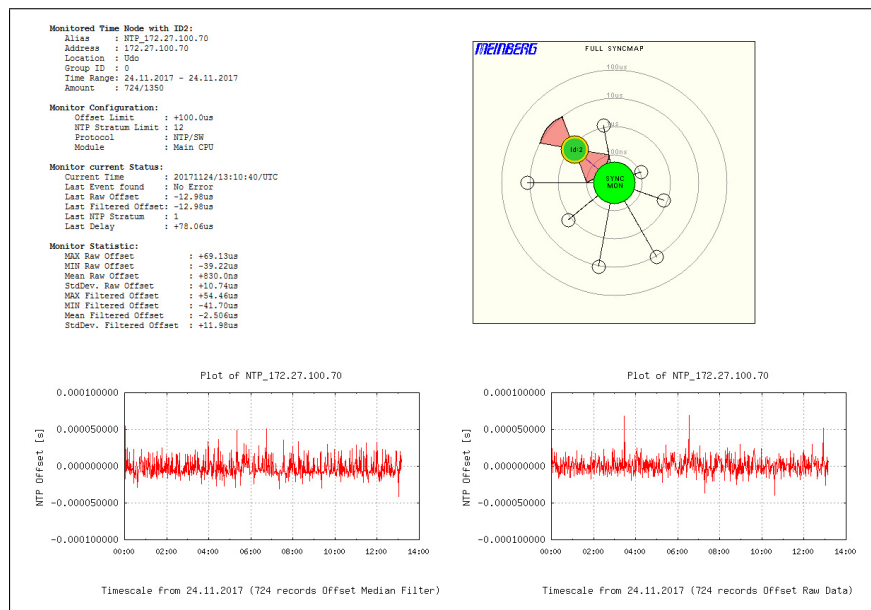
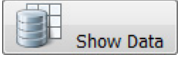


Figure: Generated report for a selected node. The report includes a status information of the selected monitored nodes, monitor configuration, main monitor statistics and graphical diagrams.



**Show Data button:**



With this selection the data of current selected time range of the monitoring node will be shown as a scrollable box with the raw measured data. These data can be selected manually and copied to other applications.

Datafile of selected time range

#	Day	Sec	Julian_day	time	Raw_offset	Median_offs	Path_delay	NTP_stratum	Min	Max	
58081	00024		2017-11-24T00:00:24+00:00		0.000030237	0.000030237	0.000140872	1	R	0.000000000	0.000030237
58081	00089		2017-11-24T00:01:29+00:00		0.000002682	0.000004362	0.000093865	1	R	-0.000032842	0.000054169
58081	00153		2017-11-24T00:02:33+00:00		0.000024279	0.000008389	0.000170566	1	R	-0.000021310	0.000104002
58081	00218		2017-11-24T00:03:38+00:00		0.000001534	0.000000266	0.000092187	1	R	-0.000019404	0.000037592
58081	00283		2017-11-24T00:04:43+00:00		0.000015304	0.000012309	0.000091835	1	R	-0.000025319	0.000066038
58081	00348		2017-11-24T00:05:48+00:00		0.000014540	0.000008414	0.000101569	1	R	-0.000020951	0.000066760
58081	00413		2017-11-24T00:06:53+00:00		0.000010747	-0.000010743	0.000181003	1	R	-0.000014673	0.000042334
58081	00478		2017-11-24T00:07:58+00:00		0.0000031090	0.000026389	0.000196147	1	R	0.000001075	0.000078020
58081	00543		2017-11-24T00:09:03+00:00		0.000014599	0.000006459	0.000103631	1	R	0.000000806	0.000046406
58081	00612		2017-11-24T00:10:12+00:00		0.000009234	0.000006681	0.000094021	1	R	0.000001562	0.000039096
58081	00677		2017-11-24T00:11:17+00:00		0.000014260	0.000006769	0.000093363	1	R	-0.000028968	0.000051814
58081	00741		2017-11-24T00:12:21+00:00		0.000025796	0.000024062	0.000052697	1	R	0.000003038	0.000052039
58081	00806		2017-11-24T00:13:26+00:00		0.000022460	0.000021979	0.000253600	1	R	-0.000018724	0.000081301
58081	00873		2017-11-24T00:14:33+00:00		0.000004844	0.000001679	0.000069882	1	R	-0.000048116	0.000093117
58081	00938		2017-11-24T00:15:38+00:00		0.000012125	0.000009623	0.000139677	1	R	-0.000038549	0.000117874
58081	01005		2017-11-24T00:16:45+00:00		0.000008890	0.000003395	0.000091664	1	R	-0.000018069	0.000032084
58081	01070		2017-11-24T00:17:50+00:00		0.000013319	0.000019734	0.000131674	1	R	-0.000030748	0.000070964
58081	01136		2017-11-24T00:18:56+00:00		0.000022358	0.000015952	0.000109257	1	R	-0.000029220	0.000072645
58081	01202		2017-11-24T00:20:02+00:00		0.000018194	0.000022432	0.000181356	1	R	0.000007054	0.000045194
58081	01268		2017-11-24T00:21:08+00:00		0.000013449	0.000008719	0.000101869	1	R	-0.000009175	0.000067424
58081	01335		2017-11-24T00:22:15+00:00		0.000002459	0.000001928	0.000151711	1	R	-0.000023112	0.000032371
58081	01400		2017-11-24T00:23:20+00:00		0.000019720	0.000021484	0.000099568	1	R	-0.000023112	0.000049166
58081	01464		2017-11-24T00:24:24+00:00		0.000027110	0.000021980	0.000257157	1	R	-0.000022388	0.000087817
58081	01529		2017-11-24T00:25:29+00:00		0.000009527	0.000007851	0.000065710	1	R	-0.000023777	0.000087817
58081	01594		2017-11-24T00:26:34+00:00		0.000019743	0.000005369	0.000093834	1	R	-0.000031018	0.000079621
58081	01660		2017-11-24T00:27:40+00:00		0.000007820	0.000005054	0.000132493	1	R	-0.000004789	0.000023492
58081	01724		2017-11-24T00:28:44+00:00		0.000022104	0.000007196	0.000078643	1	R	-0.000012279	0.000114766
58081	01788		2017-11-24T00:29:48+00:00		0.000011942	0.000028441	0.000097491	1	R	-0.000023553	0.000044590
58081	01853		2017-11-24T00:30:53+00:00		0.000013902	0.000016388	0.000095374	1	R	-0.000015044	0.000038877
58081	01921		2017-11-24T00:32:01+00:00		0.000024865	0.000017091	0.000163788	1	R	0.000003170	0.000052196

Figure: Raw data of a selected monitored node.

**Error Log**

Back in the main Sync Mon menu, by selecting the Error Logs button you will enter the Error Logs page of the selected monitored node. At this page the log messages are shown since the last system reboot. When the flash memory card gets full, the older logs will be overwritten.

**Error Logs of NTP\_172.27.100.32:**

20171124/01:56:05/UTC	172.27.100.32:	Normal Operation	NTP_172.27.100.32
20171124/01:55:00/UTC	172.27.100.32:	Error: Offset Limit exceeded (-112.6us/[+100.0us])	NTP_172.27.100.32
20171122/12:21:29/UTC	172.27.100.32:	Normal Operation	NTP_172.27.100.32
20171122/12:08:22/UTC	172.27.100.32:	Error: Offset Limit exceeded (-582.3us/[+100.0us])	NTP_172.27.100.32

Show all Error Messages

Figure: Error Log Messages for a selected monitored node.

At the bottom of the page there is a button "Show Global Error Logs" by which you can switch to view all Error Messages coming from all monitored nodes.

#### 9.1.12.4 Events

In the general overview table the last column Events is dedicated to different alarms, which are defined for monitored nodes:

- Offset limit exceeded
- not reachable
- Stratum limit exceeded
- monitoring not active



In case of "Offset Limit exceeded" and "not reachable" an icon with the count of events will be shown in the table of monitored nodes in the Events column. These events will be updated automatically every 10s. With the "Reset Events" button which can be found above the overview table you can reset the current counter for the events. These events are shown also in the SyncMap.

### 9.1.12.5 Actions for selected Nodes

In the firmware version 6.24 and following you are able to apply given actions at the same time to a number of selected nodes from the table. First select the nodes which you wish to manage, either by clicking individually a check box at the beginning of each node or by clicking on a "+" sign in the top row of the table if you wish to select all nodes together.

To deselect a node which has been selected, either click again into its check box and it will be deselected or click the "-" icon in the top row and you will deselect all nodes at the same time.

If you click the button "Actions for selected nodes" you will find actions which you can apply over the nodes.

**Select all "not reachable" nodes:**

Selection of all nodes, whose offset status shows "not reachable".

**Select all NTP nodes:**

Selection of all nodes, which are monitored via NTP.

**Select all PTP nodes:**

Selection of all nodes, which are monitored via PTP, either MGMT or with TLV messages.

**Show overview of the current day:**

If none of nodes has been primarily selected than graphical diagrams of the current day will be shown in a thumbnail form for all nodes in the table. Along with the graphical diagrams also the status information and statistics over the current day measurements will be displayed.

**Show overview of the time range:**

If none of nodes has been primarily selected than graphical diagrams of the selected time range will be shown in a thumbnail form for all nodes in the table. Along with the graphical diagrams also the status information and statistics over the selected time range measurements will be displayed.

**Show a Graphical Diagram for selected nodes (max 5):**

If you select up to five nodes in the table, they can be displayed in the same graphical diagram. First, you have to select a time frame in which the graphical diagram will be displayed.

**Create a Report for selected nodes (max 5):**

If you select up to five nodes in the table, the current data of the selected nodes will be prepared in a form of a report. First, you have to select a time frame for which the report will be generated. The report includes the current status data, monitor configuration, monitoring statistical values over the selected time frame and a graphical diagram which shows the offset trend.

Besides, the report also provides a light version of a sync map, which includes only the selected nodes from the table. In the sync map each individual node is highlighted and the rest are depicted in the background to get a comparison of how the given node is performing in relation to other nodes considered in the report.

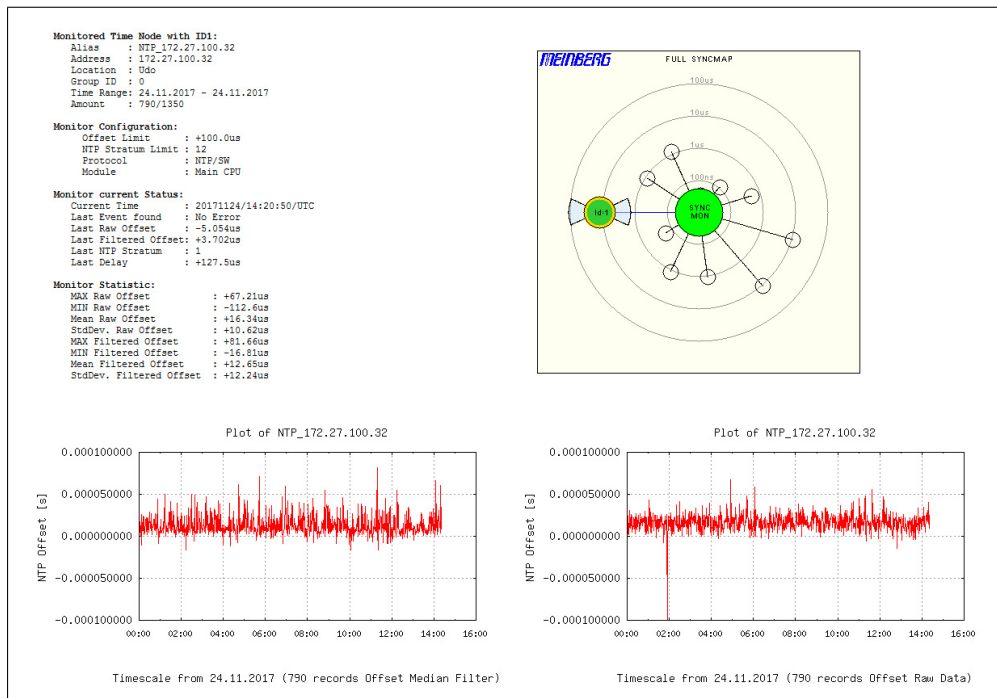


Figure: Generated report for selected nodes in the table. The report includes a status information of the selected monitored nodes, monitor configuration, main monitor statistics and graphical diagrams.

#### Disable measurements for selected nodes:

The nodes for which you disable measurements will get a status "Disabled". The measurements will no longer be requested and logged for this node. The latest measured offset will be shown in the Offset column. To start measurements again, select a node and choose "Enable measurements for selected nodes".

#### Set parameter for selected nodes:

For the selected nodes you can set or edit a list of monitoring parameters at the same time. When you select this feature the configuration dialog will show up where you can re-configure any of the parameters. The new configuration will be applied to all the nodes you have selected for this action after you confirm with the "Apply to Nodes" button.

#### Duplicate selected nodes:

The nodes which you have selected will be copied and pasted below their origin nodes. Afterwards you can edit their parameters.

#### Move selected nodes to the top of the list:

The selected nodes will be moved to the top of the list.

#### Move selected nodes to the bottom of the list:

The selected nodes will be moved to the bottom of the list.

#### Delete selected nodes:

The selected nodes will be permanently deleted from the list of nodes. The logged measurements up to this point will be preserved.

### 9.1.12.6 Meinberg Sync Map

The Meinberg SyncMap is a graphical representation of monitored nodes in a network visualized as a polar diagram. The idea of the SyncMap is to give a quick overview of the synchronization status of all monitored devices in a complex network structure.

The monitored devices are called nodes. Nodes have to support one of the following signals: NTP (RFC1305), PTP (IEEE 1588v2) or PPS connected to ESI (Extension Signal Input) IMS card.

The goal is to visualize an absolute offset of monitored nodes in terms of predefined offset limits. The data can be shown according to the current offset status or over a selectable time range (e.g. one day). It is also possible to animate the dynamic behavior of the monitored nodes of the last 60min, where SyncMaps are generated automatically every minute. This mode is called SyncMap Cyclic Mode.

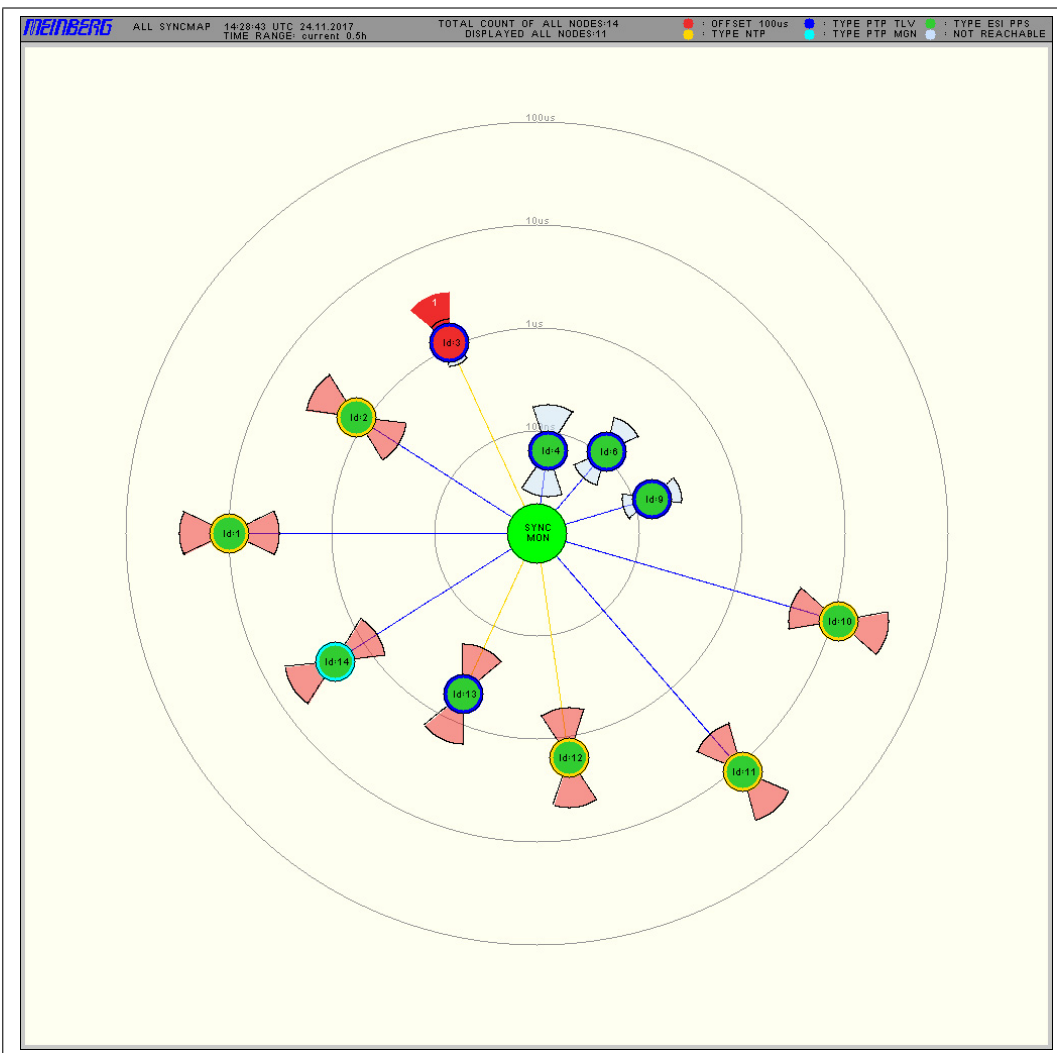


Figure: The SyncMap as a graphical representation of the monitored nodes in a network visualized as a polar diagram. It can display nodes which support: NTP, PTP (IEEE 1588v2) or PPS signals.

Each monitored node will be represented as a circle with different statistical information.

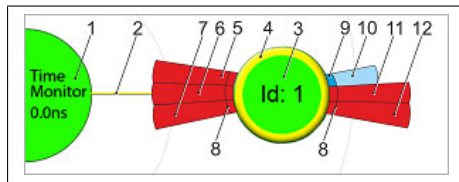


Figure: A node representation in the SyncMap. The meaning of different color codes and parts which belong to a node are explained in the text.

The Time Monitor reference with its reference clock stands in the middle, labeled as the "Time Monitor" [1]. It provides a timing reference by a controlled oscillator (synchronized by GPS, GLN, PZF, Galileo, Beidou or an external clock supply). The Time Monitor node in the center [1] is shown in green color when the reference clock is synchronous. In addition the current offset between the controlled oscillator and the reference time source is shown as a value [1].

Around the center four concentric circles representing the scaling of the polar diagram are drawn. All nodes [3] are connected concentrically by a line [2] from the central node. The distance from the center to the nodes represents the absolute average time offset between the Time Monitor and each individual node. The average value is calculated over the selected "Time Range". Each node is shown as a circle with a color inside [3] that corresponds the status and an outer ring [4], that corresponds its type.

Status:	green	= Offset < Limit
	red	= Offset ≥ Limit or outside the maximum scaling
Type:	yellow	= NTP
	dark blue	= PTP with TLV
	light blue	= PTP with Management Msgs
	green	= ESI PPS
	grey	= not available

Additionally, the statistical values: the standard deviation [8] is represented as circle segments. These values represent the temporal jitter of the measured values around the mean value. When the circle segment color is red, then the deviation is dependent on the scaling and it exceeds the half of range of the decade -> example: if the middle deviation is in the range 1us - 10us and the largest found maximum >5us, then the individual segment is drawn red, otherwise blue [10].

If one of the events occur "Offset Limit Exceeded" or "not reachable" then the circle segment will become dark red and a white value which represents the count of each event. The circle slide near the center [5,7] represent the Events "not reachable" and the outer circle slide [6,7] represent the Events "Offset Limit Exceeded".

While sliding with the mouse over a node in the syncmap without clicking a corresponding info window with the name and some statistical values will be shown:

ID 10 - M3000_Udo_100_31_Main	
Address:	172.27.101.31
GroupID/Location:	0, Udo
Offset/StdDev:	+8.588us / +29.70us
Offset Limit Exceeded=0 NotReachable=1	

By selecting a specific node in the SyncMap with a left mouse click the following menu will be opened:



"Show Graphic" will open the corresponding graphical diagram.

**Example of a full SyncMap**

The following picture shows a SyncMap of a network with 250 monitored NTP nodes running on a Sync Fire. This is a real measurement of our Test-Network for burn in tests in the Lantime production. The red signed nodes are DCF77 receivers with no compensation of the distance between a transmitter site and a receiver.

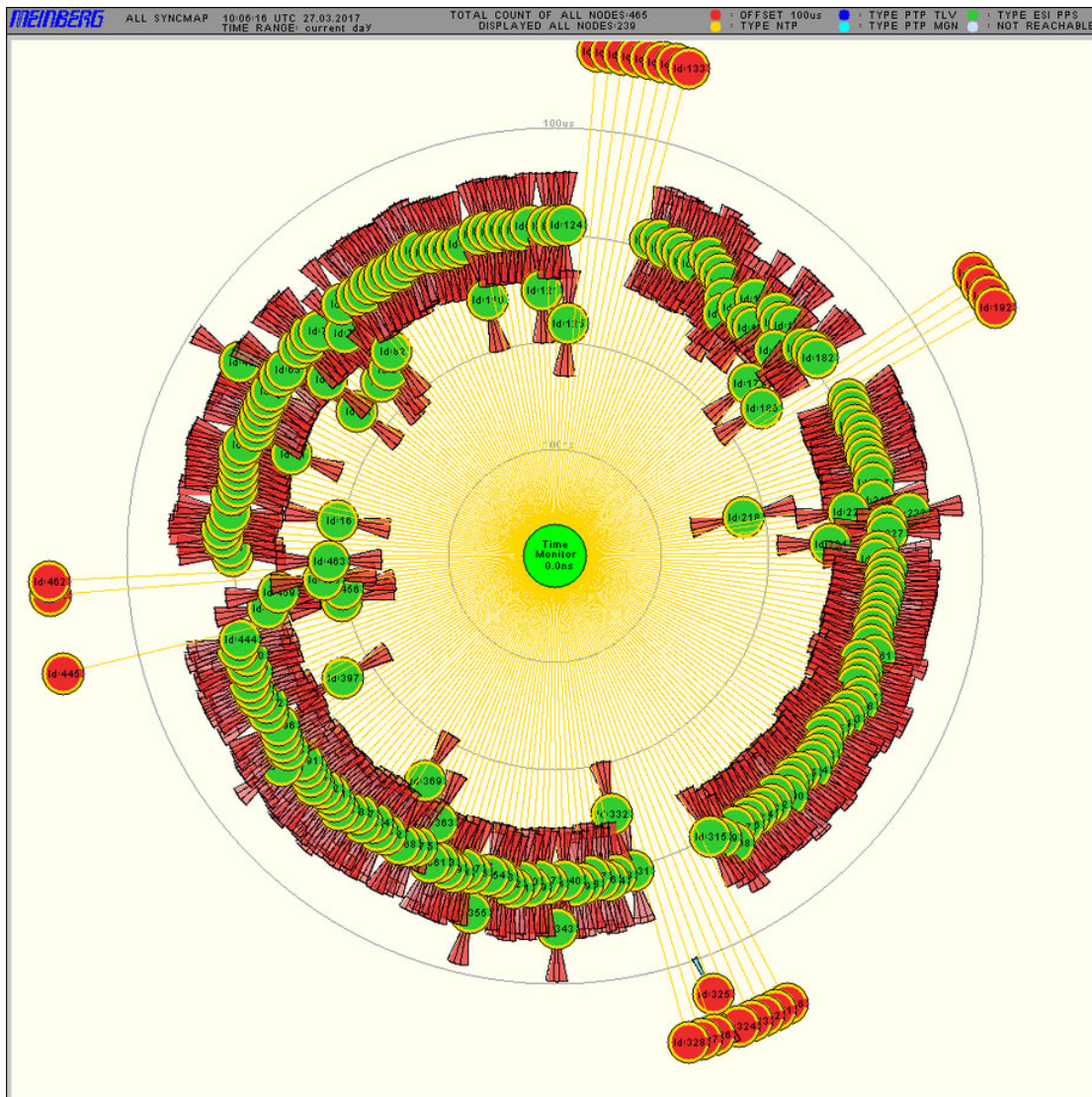


Figure: An example of a Sync map with 250 nodes.

**Sync Map Type:**

- Show reachable: currently reachable nodes are shown in the Sync Map.
- Show all Nodes: all nodes configured in the monitoring list are shown in the Sync Map, even unreachable ones.
- Show NTP only: only nodes which are monitored via NTP protocol are shown in the Sync Map. They will appear encircled with a yellow ring.
- Show PTP only: only nodes which are monitored via PTP protocol will be shown in the Sync Map. Nodes will appear with a dark blue ring if the PTP with TLV protocol is used for monitoring or with a light blue ring if the PTP protocol with Management Messages is used.

**Time Range:** the Sync Map can be generated using the monitoring data sampled in the past 30 min, past 5 min, in the past 24 hrs or within a manually selected time range. Also the statistical values are calculated using the data in the selected time interval respectively.

**Scaling:** possible scaling options: decade steps or linear for different time accuracy ranges. For PTP nodes it may be suitable to use scaling in lower microsecond range, whereas for NTP you can select ranges in a few 100microseconds or millisecond range.

**Refresh Button:** Immediately refreshes the Sync Map based on the currently available statistics of each single node. A new SyncMap with the selected time range will be generated- it is like a reload of this WEB page with the latest measurements.

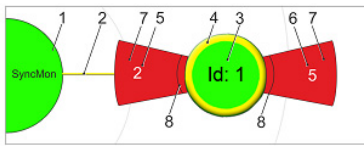
**Start Cyclic:** will activate the SyncMap animation mode. In this mode every minute a new SyncMap with the latest measurements will be generated. The last 60 SyncMaps will be then displayed as an animation. A new sequence will start with a blank SyncMap. The statistics time range will be set by default to 5min.

**Help Button:** will show the online help page for a SyncMap feature.



### 9.1.12.7 Sync Map - Help Window

#### Meinberg SyncMap Help Page



A short legend:

- 1 The Time Monitor node and the current offset measured between its oscillator and the reference time.
- 2 Line connecting each node with the SyncMon. Its length represents the absolute average time offset between Reference of SyncMon and the node.  
The color defines the sign of the average: yellow=negative blue=positive
- 3 A measured node, its color inside corresponds to its status.
- 4 Outer ring which corresponds the type of the node.
- 5 Event counter for "Node not reachable".
- 6 Event counter for "Node Offset Limit exceeded".
- 7 If Event counter > 0 then this slide is dark red. If Event counter = 0 the Standard Deviation is light red or light blue.
- 8 Standard deviation measurement. If light red, it exceeds the 100 percent of current offset, otherwise is blue.

### 9.1.12.8 System Monitoring

System Monitoring monitors other signals in the LANTIME system which do not belong to the monitored nodes (for example CPU-Utilization, local NTP, ESI inputs, MRS-References and Refclock parameters). The number and type of the internal signals depends on the integrated hardware components in a LANTIME system.

The System Monitoring is an optional feature and as per default it is disabled. It has to be enabled in the menu "SyncMon → System Settings" in the System Parameters dialog.

If the System Monitoring is enabled, then all signals will be measured and logged automatically in the same way like Node Monitoring, namely System Monitoring page will be visible.

System Monitoring			
<b>Internal parameters</b>			
Internal parameters	Offset/State	Action	Events
Local_NTP	+0.0ns		
Local_CPU-Utilization	13.38%		
<b>ESI Input</b>			
ESI Input	Offset/State	Action	Events
Local_ESI1-PPS-1	+66.85us		
Local_ESI1-Freq-2	no signal		1
Local_ESI1-Freq-3	no signal		1
Local_ESI1-BITS-4	no signal		1
<b>MRS Parameters</b>			
MRS Parameters	Offset/State	Action	Events
Local_CLK1-GPS-0	+6.0ns		
Local_CLK1-ext.-1	-20.0ns		
Local_CLK2-GNSS-0	+14.0ns		25
<b>RSC Parameters</b>			
RSC Parameters	Offset/State	Action	Events
Local_Diff-CLK1-CLK2	-60.0ns		
<b>Refrlock Parameters</b>			
Refrlock Parameters	Offset/State	Action	Events
Local_REF1-GPS180-state	sync		
Local_MRS1-GPS180-substate	GPS		
Local_REF1-GPS180-usage	selected		
Local_REF1-GPS180-SatInView	10 in view		
Local_REF1-GPS180-SatGood	10 good		
Local_REF2-GRC181-state	sync		
Local_MRS2-GRC181-substate	GNSS Receiver		
Local_REF2-GRC181-usage	not selected		
Local_REF2-GRC181-SatInView	8 in view		
Local_REF2-GRC181-SatGood	5 good		

Figure: An overview table for internal signals as shown in the System Monitoring page. The system signals you wish to monitor, need to be first selected in the Source Priority list for each reference clock individually.

The number of MRS References (CLK1-GPS-0, CLK1-NTP-1, CLK1-PTP-2 ...) depends on the activated Source Priorities for each reference clock – this can be configured on the "Clock" page in the "MRS Settings" for each clock.

### 9.1.12.9 Error Logs



Figure: Log Messages from all monitored nodes.

Global Error Log gives the option to track all error events.

**Error Log Statistics:** categorization of error logs for each specific node.

**Clear Error Logs:** deletes the list of logged errors.

### 9.1.12.10 System Settings

The menu for "System Settings" will show the current available space on the flash disc and will calculate the count of days which can be stored depending on the count of monitored nodes and the log-interval.

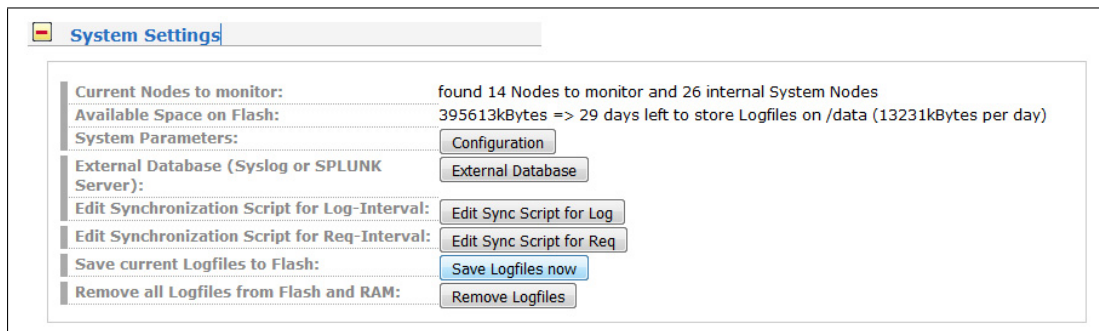


Figure: Memory card status, available space left and logfiles archiving options.

There is an indicator implemented which informs about the available flash space "Available Space on Flash" and the number of days left for monitoring of the current sync node setup. The current data will be stored on the flash card. However you can choose an additional path for saving the current data into a RAM. The data from RAM will be stored automatically to the flash card each day at UTC 0:00.

There is an extra button "Save Logfiles now" to store the files from the RAM to the flash card at any time.

With the button "Remove Logfiles" all files on the flash card will be removed without a backup.

Two extra synchronization scripts can be activated to copy each measured data to an external server. One will be activated after every request interval of each monitored node and the other will be activated after every log-interval. These scripts will be activated after every cycle when the monitoring of all devices has been finished. For example you can use the following command to copy all files to a server with rsync:

#### Example for Sync Script with rsync:

```
rsync -e "ssh -i /etc/ssh/ssh_host_rsa_key" -rv /data/stats/client_ip/* server
```

In the next example all changes at request or log-interval will be sent via syslog message to an external syslog server (these files can be edited via CLI in /config/syncmon\_sync\_script\_for\_req and /config/syncmon\_sync\_script\_for\_log):

```
#!/bin/bash
#
# /config/syncmon_sync_script_for_req
#
LAN_0="172.22.13.244"
LOG_PROG="syncmon"
LOG_LEVEL="info"
LOG_FILE="/var/log/syncmon_last_req_measurement.log"
while read LINE
do
logger -t $LOG_PROG -p $LOG_LEVEL "$LAN_0 $LINE"
done < $LOG_FILE
```

### Send Monitoring Data to external Server as a Backup

In order to backup the monitoring data and store them for later analytical processing, you can enable automatic sending of the data via syslog protocol to up to 3 external database servers. In this case every node measurement processed in a request-interval will be sent to a specified server.

In the following dialog you can configure the target servers where you want to store your data.

As **Network Protocol** options you can choose between the UDP or TCP/IP protocols, running as per default on a port:514.

**Name of this SyncMon device:** you can monitor your network by different Sync Monitoring devices. You can give them unique names to recognize it easily in the database server, where the data come from.

When you finish the server configuration, save it by clicking the "Save Syslog" button.

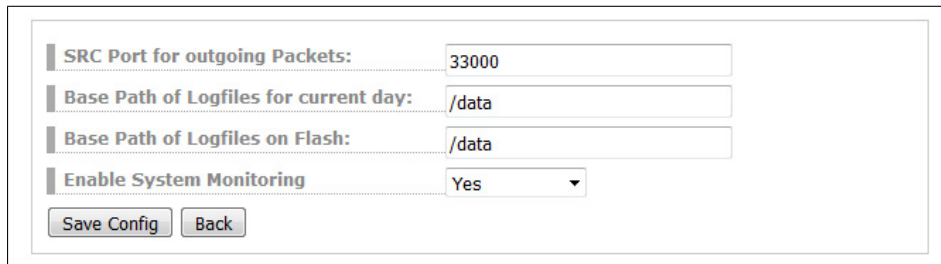
#### Config for sending measured data to external Database via Syslog protocol (external SYSLOG or SPLUNK Server)

Enable sending measured data to external Database Server	1	Yes
IP Address of external Data Server:	<input type="text"/>	
Network Protocol:	UDP	▼
Port number for outgoing packets:	514	
Name of this SyncMon device:	SyncMon	
Enable sending measured data to external Database Server	2	No
IP Address of external Data Server:	<input type="text"/>	
Network Protocol:	UDP	▼
Port number for outgoing packets:	514	
Name of this SyncMon device:	SyncMon	
Enable sending measured data to external Database Server	3	No
IP Address of external Data Server:	<input type="text"/>	
Network Protocol:	UDP	▼
Port number for outgoing packets:	514	
Name of this SyncMon device:	SyncMon	
Save Syslog	Back	

Figure: Configuration options for an external database server where the monitoring data can be automatically stored.

With the "Configuration" button some system configuration parameters can be set:

- Source Port of outgoing NTP packets: default is 33000.
- Base Path for logfiles for current day. The default path is the internal compact flash card with /data.
- Base Path for logfiles for history of days. The default path is the internal compact flash with /data. e.g. this could be changed to /mnt/usb-storage if an USB-Memorystick is used.



SRC Port for outgoing Packets:	33000
Base Path of Logfiles for current day:	/data
Base Path of Logfiles on Flash:	/data
Enable System Monitoring	Yes

Save Config Back

*Figure: System Parameters settings within the Sync Mon feature. Here you can set the current path where the data for the current day and history data is stored. Be aware when the flash card is full, the oldest data will be overwritten.*

**Enable System Monitoring:** the monitoring of internal signals like CPU-Utilization, local NTP, ESI inputs, MRS-References and Refclock parameters, depending on integrated hardware of the system will be activated. By default the monitoring of the system is disabled.

The measured data of the monitored nodes will be stored in separate directories on a flash disc. The base path of the stored data files can be configured by the user, therefore it is also possible to use an external flash disc (e.g. USB stick). The data will be stored separately for each day and each monitored node.

```

/data
 | /stats
 |   | /syncmon
 |   |   | /alias-name1
 |   |   |   | ntp_mon_stats.20170201
 |   |   |   | ntp_mon_stats.20170202
 |   |   |   | ntp_mon_stats.20170203
 |   |   |   | ...
 |   |   | /alias-name2
 |   |   |   | ntp_mon_stats.20170201
 |   |   |   | ntp_mon_stats.20170202
 |   |   |   | ntp_mon_stats.20170203
 |   |   |   | ...

```

Figure: Example for default path structure of history of days datafiles on the flash card.

The data file format:

1. MJD: Modified Julian Date - is the continuous count of days since the beginning of the Julian Period (started at 1858 Nov 17 - 0:00)
2. time past midnight in seconds
3. time stamp (ISO from MJD and time past midnight)
4. measured clock offset raw (If the request interval is less than the Logging interval then the mean value of the measured offsets at request interval will be stored)
5. in case of NTP: clock offset median (Median of the 5 last measured offsets at request-int  
in case of PTP: reported offset)
6. path delay in seconds
7. NTP stratum or PTP state
8. 'R' (optional indicator for min/max values of raw data: if the request interval is less than the log-interval then automatically the Min and Max values of the raw data will be stored in the next 2 lines)
9. see 8. (optional)
10. see 8. (optional)
11. 'M' (optional indicator for min/max values of MTie (Maximum Time interval error) values from PTP nodes which supports this option: if the PTP node support MTie feature with extended TLVs then the Min and Max values will be stored in the next 2 lines)
12. see 11. (optional)
13. see 11. (optional)

Samples of Monitoring Data stored in the history of days files:

**Example for NTP data files:**

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay NTP_stratum
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 1
```

**Example for PTP data files:**

```
# Day Sec Modified_Julian_day_time Meas_offset Report_offs Path_delay Port_state
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 9
```

**Example for NTP data files with request interval less than log-interval:**

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay NTP_stratum Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 1 R -0.0001 0.0001
```

**Example for PTP data files supporting MTie feature:**

```
# Day Sec Modified_Julian_day_time Meas_offset Report_offs Path_delay Port_state Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 9 M -0.0001 0.0001
```

The size of a data file per day depends on the logging interval and has a size of about 110kB if log-interval is 64s.

## System Utilization

With the latest SyncMon version it is possible to configure up to 1000 nodes to monitor. The request and logging interval can be set to 1s. Be aware that system CPU will be heavily used in case of high counts of nodes and low request and log-intervals. This could decrease the NTP server performance as well.

### Examples:

- 10 monitoring nodes with log-interval = 1s will store 70MBytes (69194kBytes) per day – the default size of the flash used for SyncMon logging is about 400MB – so 5 days can be stored on internal flash disk.
- 100 monitoring nodes with log-interval = 1s will store 700MB per day – then data logging will stop if the flash is full – the log rotating for SyncMon will be started at 00:00 UTC and will erase data files older than 2 days. The CPU utilization will increase about 10%.
- 100 monitoring nodes with request interval = 1s and log-interval = 64s will store about 12MBytes per day – so about 40 days can be stored on internal flash disk. The CPU utilization will increase about 7%.
- 900 monitoring nodes with request interval = 1s and log-interval = 64s will store about 100MBytes per day – so about 4 days can be stored on internal flash disk. The CPU utilization will increase about 45% – this is critical for the NTP server performance of the device.

## Sync Monitor Status files via CLI

The current status of the monitored nodes as displayed in the Web-GUI is stored in an ASCII file `/var/log/sync-mon_node_status`, updated after every full scan of the configured nodes and can be accessed over CLI.

```
# Net Sync Monitoring Status with total 15 Nodes (updated at ...)

# Node-Address      NTP:Offset      -filtered      Delay      NTP-Stratum  Auth MTIE  CntErr  CntErr  Error  Message
#                   PTP:OffsNode   -measured
# -----
172.16.100.65: -0.000113960  0.000055254  0.001663415  2      0  0  3  0  0  Normal Operation
172.16.3.11: -0.005109103  -0.005896857  0.001891819  1      0  0  0  0  0  Normal Operation
172.16.3.12: -0.028305041  -0.028305041  0.001669302  2      0  0  0  0  1  Error: Offset Limit exceeded
172.27.101.90: -0.000037604  -0.000002865  0.000352269  2      0  0  0  0  0  Normal Operation
172.27.100.32: 0.000008375  0.000008375  0.000209699  1      0  0  0  0  0  Normal Operation
172.27.100.1: 0.000000899  -0.000027105  0.000416735  1      2  0  0  0  7  Error: Authentication failed
ESI-Module: 0.000001819  0.000001839  0.000000000  0      0  0  0  0  0  Normal Operation
EC:46:70:00:8F:64: 0.000000000  0.000000000  0.000000000  0      0  0  0  0  6  Error: Time Monitor not active
172.27.19.68: 0.000000109  -0.000000013  0.000007451  9      0  0  0  0  0  Normal Operation
EC:46:70:00:8F:64: -0.000000049  -0.000000171  0.000006273  9      0  0  0  0  0  Normal Operation
172.27.19.70: 0.000000030  -0.000000035  0.000007749  9      0  0  0  0  0  Normal Operation
172.27.19.98: 0.000000000  0.000000000  0.000000000  0      0  0  0  0  3  Error: Not reachable
172.27.101.143: 0.000000000  0.000000000  0.000000000  0      0  0  0  0  3  Error: Not reachable
172.27.19.11: -0.000010202  -0.000090331  0.000052625  8      0  1  0  0  0  Normal Operation
172.27.101.90: 0.000000000  0.000000000  0.000352269  2      0  0  0  0  3  Error: Not reachable
```

Figure: The status information table accessed over a CLI.

## Configuration via CLI

The configuration file can be edited with a text editor directly in the command line (CLI) of the system or can be replaced by an external prepared file. For more information see chapter [Sync Monitor Status and Configuration via CLI](#).



### 9.1.12.11 Export Data from SyncMon

#### How to export and use data from the SyncMon?

In SyncMon Menu in the Web Interface menu "System Settings → System Parameters → External Database" you can configure up to 3 external Servers, where the measured data is sent at each log interval via the Syslog protocol.

**Config for sending measured data to external Database via Syslog protocol (external SYSLOG or SPLUNK Server)**

Send data to external Database Server 1	Disabled
IP Address of external Data Server:	Disabled
Network Protocol:	UDP
Destination Port:	514
[Optional] Name of SyncMon device:	SyncMon
[Optional] Add IP Address of internal Interface:	Disabled

Output format dropdown menu options: Disabled, MBG Data Format, SPLUNK friendly, **JSON format**

For each of these external servers the following parameters can be set:

- network protocol: UDP or TCP
- a port number (default is 514 for standard syslog)
- a device name
- optionally the IP Address of the network port used for the measurement can be activated
- configuration of the output format:
  - Meinberg Standard Format
  - Key-Value-Pairs (Splunk friendly)
  - Jason Format

The Meinberg Standard Format corresponds to the SyncMon data format stored in a file system on a LANTIME. This will be later used for the SyncMon Manager. The SyncMon Manager is currently in development and will be able to visualize the data stored on an external server and generate reports.

#### An excerpt of the SyncMon format:

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0_test 58154 34813 2018-02-05T09:
40: 13 + 00: 00 0.000000494 0.000041453 0.000073266 1 R -0.000011100
0.000041453
```

For more Details about SyncMon formats see chapter [SyncMon Formats](#).

### 9.1.13 XtraStats

**XtraStats Diagrams :**

Created (UTC)	Graph	Data	Data Size
2017-02-13 09:34:04	<a href="#">mrs_stats_0_FRQ</a>	<a href="#">mrs_stats_0_FRQ_data.txt</a>	2636 records - 403308 bytes
2017-02-13 09:42:53	<a href="#">mrs_stats_0_GPS</a>	<a href="#">mrs_stats_0_GPS_data.txt</a>	2676 records - 409428 bytes
2017-02-13 09:45:20	<a href="#">ntp_counters</a>	<a href="#">ntp_counters_data.txt</a>	3000 records - 62362 bytes

**Available XtraStats Definitions :**

Name	Description	Actions
<a href="#">mrs_stats_0_FRQ</a>	MRS Stats for FRQ Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">mrs_stats_0_GPS</a>	MRS Stats for GPS Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">mrs_stats_0_IRIG</a>	MRS Stats for IRIG Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">mrs_stats_0_NTP</a>	MRS Stats for NTP Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">mrs_stats_0_PPS</a>	MRS Stats for PPS Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">mrs_stats_0_PTP</a>	MRS Stats for PTP Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">mrs_stats_0_STR</a>	MRS Stats for STR Reference	<a href="#">[Data]</a> <a href="#">[Graph]</a>
<a href="#">cpu</a>	CPU Utilization	<a href="#">[Start]</a>
<a href="#">gps_sats</a>	GPS Satellite Reception Status	<a href="#">[Start]</a>
<a href="#">memory</a>	System Memory Status	<a href="#">[Start]</a>
<a href="#">ntp_basic</a>	NTP Basic Statistics	<a href="#">[Start]</a>
<a href="#">ntp_counters</a>	NTP Access Statistics	<a href="#">[Data]</a> <a href="#">[Graph]</a> <a href="#">[Stop]</a>
<a href="#">ntp_offset</a>	NTP Offset	<a href="#">[Start]</a>
<a href="#">ntp_rem</a>	NTP Basic Statistics for 127.0.0.1	<a href="#">[Start]</a>
<a href="#">ntp_sysstats</a>	NTP Access Statistics	<a href="#">[Start]</a>

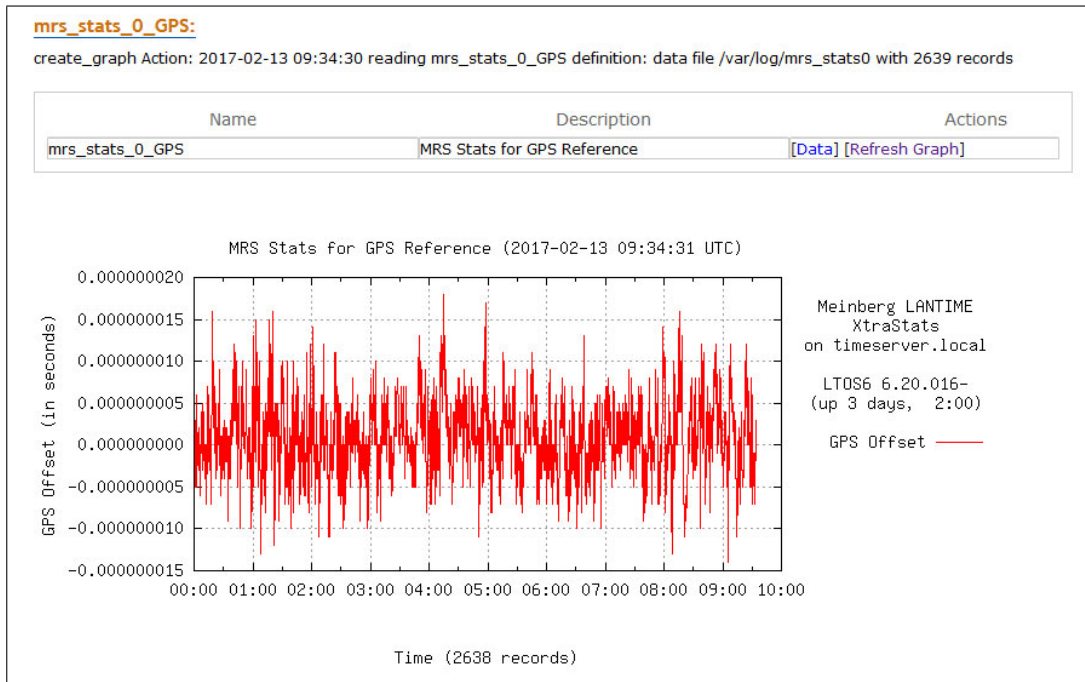
The XtraStats page is used for monitoring available reference sources and system parameters like CPU load and memory consumption. To start recording data for a certain aspect of the system just press the "Start" link in the Actions column. If enough data is available a new link appears to show the data as a text file or as a graph. The graph will be created when clicking the link. Only the data that has been collected so far will be shown. To update the graph just reload the page.

It's recommended to stop the monitoring if not needed anymore to reduce the workload and disk storage consumption of the unit.

The system comes with a certain set of predefined statistics definitions and will add new ones based on the hardware and software configuration of the unit. It is also possible to add own definitions. To do this please contact the Meinberg Tech Support and they will provide a guideline.

All collected data are available in the /var/log for further processing. The data is saved in the volatile memory and will be lost if the unit is shut down. If the data is needed for further processing please make sure to save them externally.

Available XtraStats: Example MRS Stats for GPS Reference



An MRS LANTIME logs the offset statistics of all configured MRS time sources independently.

**Data:**

A selection of daily statistics. *mrs\_stats0* always stands for the present day.

**Graph:**

Select the MRS source for which a graphic is to be generated. The link "Graph" is used to create the graphic.

### 9.1.14 Documentation & Support

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

Available Documents:					
Filename	Language	Type	Date	Size	Option
ltos6-cli	german	pdf	2016-12-08	320.96kb	<a href="#">View</a>
ltos_6-20	german	pdf	2016-12-08	10562.43kb	<a href="#">View</a>
ltos6-cli	english	pdf	2016-12-08	311.20kb	<a href="#">View</a>
ltos_6-20	english	pdf	2016-12-08	10016.24kb	<a href="#">View</a>
4 Documents available					

The LANTIME documents can be downloaded from here in order to read / print them on your workstation.

The "Docs & Support" Tab does also provide some important weblinks. It furthermore gives you information about the Meinberg Sync Academy - MSA.

Meinberg Sync Academy:	
Description	<p>If you wish to learn more about:</p> <ul style="list-style-type: none"> <li>• <b>Time &amp; Frequency Synchronization,</b></li> <li>• <b>LANTIME features, Web GUI configuration and management,</b></li> <li>• <b>NTP / PTP fundamentals,</b></li> <li>• <b>Meinberg Product's hardware and software for successful troubleshooting,</b></li> </ul> <p>then join us at one of the upcoming Trainings at <b>Meinberg Sync Academy!</b></p> <p>MSA offers trainings and workshops in the field of time- and frequency synchronization, held by highly experienced Instructors. The tutorials consist of theoretical lectures and „hands-on labs“ for a better understanding and realistic experience.</p>
Internet	<a href="http://www.meinberg.academy/">http://www.meinberg.academy/</a>
Email	<a href="mailto:office@meinberg.academy">office@meinberg.academy</a>
Courses	<a href="http://www.meinberg.academy/courses/">http://www.meinberg.academy/courses/</a>
Customized Trainings	<a href="http://www.meinberg.academy/customized-trainings/">http://www.meinberg.academy/customized-trainings/</a>
Apply Now	<a href="http://www.meinberg.academy/registration-form/">http://www.meinberg.academy/registration-form/</a>

The Meinberg Sync Academy offers and develops tutorials in the field of time- and frequency synchronization, such as NTP, PTP IEEE-1588 and many more. This Part of the LANTIME "Docs & Support" Tab provides basic information about the Sync Academy followed by some links to helpful informations on <http://www.meinberg.academy>.

The Support Information chapter gives you all necessary information how to contact the technical support. Apart from that it provides a link to the firmwareportal of Meinberg.

Support Information:	
 Phone	+49(0)5281 930980
 Email	<a href="mailto:techsupport@meinberg.de">techsupport@meinberg.de</a>
 Firmware Updates	<a href="https://www.meinbergglobal.com/english/sw/firmware.htm">https://www.meinbergglobal.com/english/sw/firmware.htm</a>
 RMA	<a href="https://www.meinbergglobal.com/english/support/rma.htm">https://www.meinbergglobal.com/english/support/rma.htm</a>

## 9.2 Via CLI

### 9.2.1 Introduction

The configuration and management of a Meinberg LANTIME network time server can be performed using a number of different user interfaces. The graphical user interface of such a device is accessible using a web browser and offers the possibility to review the current status of the system and to visualize statistical values using the web based diagram software called xtrastats.

The command line interface (CLI) of the sixth LANTIME firmware generation is using a text-only (non-graphical) approach. It can be accessed using local connections (serial console ports) or remote network connections (SSH or Telnet). The CLI is based on a standard Unix shell interpreter called Bourne Again Shell (Bash), offering comfortable editing of a command line by using the cursor keys and delete/backspace. By accessing a command history using the up/down cursor keys, the shell allows to modify an already used command or simply execute it again, without modification, if required. The tabulator key (Tab) can be used to auto-complete a command and saves the user from having to type in the full command name.

By using a standard shell the LTOS6 firmware environment can benefit from a number of additional advantages. A Unix system administrator will certainly already know how to work with a shell and by making use of the script language elements of the shell, very sophisticated or recurring command sequences can be automated.

In addition to the Bourne Again Shell the so-called Debian Almquist Shell ("Dash") and the standard Almquist Shell ("ash") are available on the system and can be used in addition or as a replacement to the standard shell.

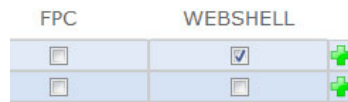
This reference manual does not contain a description for every of the more than 400 commands that are available on a LTOS6 system. It tries to cover the most popular commands, especially those that are LANTIME specific and that are not existing on other Unix- or GNU Linux based systems. A number of commands allows to read a short help text describing the parameters and use of the command by executing "commandname -h".

For any questions regarding the LANTIME command line interface, please contact your Meinberg Technical Support.

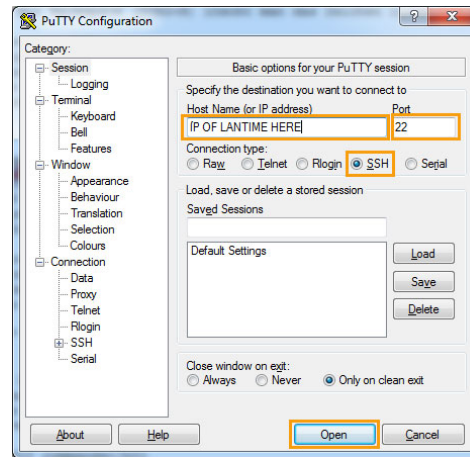
## 9.2.2 Accessing and Using the CLI

In order to access the CLI, you need to log in to one of the CLI-supporting user interfaces, by using a serial console port or a network connection with either the SSH or TELNET protocol. If only a web browser is available, it can also be used to access the CLI via the so-called WEBSHELL service (Port: 4200 - e.g. `http://172.44.100.10:4200`; default user: `root` / default password: `timeserver`).

**Please note:** The webshell service must be activated first via Web Interface chapter 9.1.2 "Network → Network Services".



Activate Webshell service in Web GUI



Login via Putty console

### Serial Console

Serial console ports are located on the front panel or (in modular systems) on the CPU module (some devices come with both a front port and a CPU console port). These ports can be accessed with a serial terminal running at 38400 baud and using 8 data bits, no parity, 1 stop bit (8N1).

### Logging in

The default configuration knows one user account (`root`) with a standard password (`timeserver`). Other users can access the CLI only if their access level has been set to "Super User". If that is not the case, the system will reject the user and does not allow to access the command line interface.

A "Super User" will be presented with a system status overview after successfully authentication, followed by a shell prompt.

### Automatic Logout

The CLI will automatically terminate a CLI session if a user does not enter a command for more than 300 seconds (5 minutes). This timeout can be disabled by entering the `"no_shell_timeout"` command. It can be changed by using the `"set TMOUT=x"` command (x represents the new timeout in seconds).

### Entering CLI commands

Commands are case-sensitive, almost all commands are lower-case and do not contain any uppercase characters. It is possible to enter only the beginning of a command and then use the TAB key (CTRL+I) to let the system automatically complete it. If the entered part is not uniquely corresponding to one command, a list of all possible commands that match the entered text is shown.

To edit a command line, the left/right cursor keys (or, alternatively, CTRL+B and CTRL+F) can be used to move the cursor. Entering ESC+F and ESC+B will move the cursor to the beginning of the next or previous word. And BACKSPACE (CTRL+H) deletes the character to the left of the cursor.

## Command History

Already entered and processed commands can be recalled within a CLI session by using the cursor up/down keys (or CTRL+P and CTRL+N). It is possible to search for an already entered command line by pressing CTRL+R and then starting to enter a search pattern. If more than one command line matches the entered pattern, repeatedly pressing CTRL+R will toggle through the matching entries. The **"history"** command lists all previously entered and processed commands.

## Logging Out, Termination of a CLI session

To log out of the CLI, you can use the **"exit"** or the **"logout"** command. It is also possible to terminate a CLI session by pressing STRG+D at the shell prompt.



### 9.2.3 Command Reference

This chapter describes all available CLI commands and their parameters.

#### Conventions

The command names in this chapter are shown in **bold** characters, parameters (if supported) are represented in *italic* characters. If a parameter or part of the commandline is optional, i.e. it does not have to be entered, it is surrounded by brackets [ ].

The character "#" at the beginning of a line represents the shell prompt, which will contain different characters depending on the configuration and status of the device.

Examples:

# **pwd**

(shows the name of the currently selected directory)

# **ls** [**path**]

(shows the content of the specified path [*path*] or - if no [*path*] parameter has been entered, the content of the current directory.

### 9.2.3.1 Configuration Management

The 6th LANTIME firmware generation offers a number of commands to manage the configuration of a device. This includes saving a configuration set under a certain name and, at a later time, restoring/reactivating it. Other commands are aimed at comparing the currently used configuration with the so-called startup configuration that is automatically loaded when the device is (re)starting.

### 9.2.3.2 `lsconfig` - List Saved Configsets

#### Purpose

This command lists all files included in a saved configuration (i.e. a so-called "configset") for a given package. It can also list all saved configsets for a given package.

#### Call and Parameters

```
# lsconfig package [configset]
```

If both **package** and **configset** have been specified, the command will show all files included in the specified configset for the given package. If only the **package** is provided, `lsconfig` will output a list of all available configsets that include saved configuration files for the specified package. If "all" is specified as the package name, the command covers all installed packages.

#### Examples

```
# lsconfig network myconfig1
```

(shows all files of the network configuration which are included in the saved config set "myconfig1")

```
# lsconfig snmp startup
```

(lists the SNMP related configuration files in the startup configset. This configset is automatically loaded during system startup.)

```
# rmconfig all myconfig2
```

(this lists the files for all packages in the configset myconfig2)

### 9.2.3.3 rmconfig - Delete a Configset

## Purpose

This command deletes a saved configuration (i.e. a so-called "configset"). Attention: `rmconfig` does not ask for a confirmation, it immediately removes the selected configuration from the flash memory of the device. This is non-reversible and therefore requires you to be very careful when using this command.

## Call and Parameters

```
# rmconfig package configset
```

The parameter **package** specifies the package whose configuration should be deleted. This could be "network" or "lantime" or "snmp". The available packages can be found by looking at the contents of the `/package` directory, in which you can find a subdirectory for each package installed. If the given package name is "all", the whole configuration set will be deleted.

The *configset* parameter defines the saved configuration ("configset") from which the package configuration shall be deleted. It is not allowed to use "default" because the default configuration of a package cannot be deleted. By specifying the configset "startup", the default package configuration will be restored during the next system start.

## Examples

```
# rmconfig network myconfig1
```

(removes the network configuration from the saved config set "myconfig1")

```
# rmconfig snmp startup
```

(removes the startup configuration of the snmp package, the SNMP default configuration will be restored during the next boot process)

```
# rmconfig all myconfig2
```

(removes the entire configset "myconfig2", i.e. the configuration of all packages)

### 9.2.3.4 diffconfig - Show unsaved Configuration Changes

#### Purpose

With this command a saved configuration (i.e. a so-called "configset") can be compared with the current configuration. This allows to check for unsaved configuration changes.

#### Call and Parameters

```
# diffconfig package configset
```

The parameter **package** specifies the package whose configuration should be compared. Examples would be "network" or "lantime" or "snmp". If the given package name is "all", the complete configuration set will be compared. This is the default behavior if no package name is specified on the command line.

The *configset* parameter defines with which saved configuration ("configset") the currently running configuration should be compared. If this is not specified on the command line, the configset "startup" is used as a default.

#### Examples

```
# diffconfig network myconfig1  
(compares the current network configuration with the saved config set "myconfig1")
```

```
# diffconfig  
(shows the differences between the current configuration to the "startup" configset, i.e. for all packages)
```

### 9.2.3.5 checkconfig - Check for unsaved Configuration Changes

#### Purpose

This command shows whether an unsaved configuration change has been detected or not. It does not show any details on configuration changes (like diffconfig).

#### Call and Parameters

```
# checkconfig
```

This command must be run without any parameters.

#### Examples

```
# checkconfig  
No configuration changes.
```

### 9.2.3.6 saveconfig - Save Configuration Changes

## Purpose

This command saves the currently active configuration in a configuration set ("configset"). It can be used to persistently store configuration changes (by saving them to the "startup" configset that is loaded during the powerup/boot sequence) and to backup a configuration.

## Call and Parameters

```
# saveconfig package configset
```

**package** specifies the package whose configuration should be saved. Examples for this are "snmp" or "ssh" or "network". If no package name is provided on the command line, the configuration for all packages is saved as a standard behavior.

The *configset* parameter defines the saved configuration ("configset") to which the package configuration(s) shall be saved. It is not allowed to use "default" because the default configuration of a package cannot be overwritten/changed. By specifying the configset "startup", the configuration will be restored during the next system start. If no configset name is specified, the startup configuration set ("startup") is used as a default.

## Examples

```
# saveconfig snmp
```

(saves the SNMP configuration to the startup configuration "startup")

```
# saveconfig network backup1
```

(saves the network configuration to a configset "backup1")

```
# saveconfig all myconfig2
```

(saves the entire configuration to the configset "myconfig2", i.e. the configuration of all packages)

### 9.2.3.7 loadconfig - Load Configset

#### Purpose

The `loadconfig` command loads the configuration for the whole system (all packages) or a given package from a previously saved configuration set ("configset"). It can be used to restore the default configuration, the startup configuration or a configuration backup.

#### Call and Parameters

```
# loadconfig package configset
```

The **package** parameter specifies the package whose configuration should be loaded. Using "all" will load the configuration for all packages. If no package name is provided on the command line, "all" is assumed as the standard behavior.

With the *configset* parameter the name of the previously saved configuration ("configset") is defined. The package configuration(s) is loaded from this configuration set. Specifying "default" will load the default values of the package and "startup" loads the startup configuration set that is automatically loaded during the powerup/boot process. If no configset is given, the "startup" configset is loaded.

#### Examples

```
# loadconfig snmp  
(loads the SNMP configuration from the startup configuration "startup")
```

```
# loadconfig network backup1  
(loads the network configuration from the "backup1" configset)
```

```
# loadconfig all myconfig2  
(loads the entire configset "myconfig2", i.e. the configuration of all packages)
```

### 9.2.3.8 File Management

The management of files in the flash memory of a LANTIME device is normally handled automatically by the LANTIME firmware itself. However, in certain situations it might be required that an administrator has to manually delete, copy or rename a file. From time to time the contents of a file have to be checked, for example when looking at a log file or a status file.

The following CLI commands enable you to perform these tasks.

### 9.2.3.9 pwd - Print Working Directory

#### Purpose

The pwd command prints the name and path of the current working directory.

#### Call and Parameters

```
# pwd
```

This command does not require any parameters.

#### Examples

```
# pwd snmp  
/var/run
```

### 9.2.3.10 cd - Change Working Directory

#### Purpose

The cd command changes the current working directory.

#### Call and Parameters

```
# cd [directory]
```

The system changes the working directory to the given directory or, if no directory has been specified, to the home directory of the current user.

#### Examples

```
# cd /etc  
(sets the working directory to /etc)
```

```
# cd  
(changes to the home directory of the current user, e.g. /root for the root user)
```

### 9.2.3.11 ls - List Directory Contents

#### Purpose

With this command, the contents of a given directory can be listed.

#### Call and Parameters

```
# ls [Options] [directory]
```

The content of the given directory are printed. A large number of options is available which control how the ls command lists all the files and subdirectories. Please use the "-help" option to get a list of all supported options.

#### Examples

```
# ls /var/log
```

(shows the content of the /var/log directory in standard output format)

```
# ls -l /var/run
```

(lists the files and subdirectories of the /var/run directory, using the "long" output format (-l) which shows a number of details like file sizes)



### 9.2.3.12 cp - Copy Files and/or Directories

## Purpose

The "cp" command copies files or whole directories.

## Call and Parameters

```
# cp [Options] [Source(s)] [Target]
```

An overview with all supported options can be requested with

```
cp -help
```

The option "-v" ("verbose") for example shows the name and path of the file that is currently worked on during the copy operation.

One or more files can be specified as the source(s), wildcards (like \* or ?) are allowed. The target can either be a directory or, if the source is one single file, a target filename.

Copying a whole directory structure is possible by using the "-r" (recursive) option.

## Examples

```
# cp /etc/hosts /var/tmp
```

(copies the file hosts from the /etc directory into the target directory /var/tmp where it will be stored under the same name, i.e. hosts)

```
# cp /config/global_configuration /var/tmp/mycopy
```

(copies the file global\_configuration from the /config directory into the target directory /var/tmp using the target filename mycopy)

```
# cp /etc/ssh/ssh_* /tmp/
```

(copies all files form /etc/ssh with a filename beginning with "ssh\_" into the directory /tmp)

```
# cp -r /etc/udev /tmp/
```

(creates a copy of the /etc/udev directory with all subdirectories and containing files in the target directory /tmp)

### 9.2.3.13 mv - Move Files and/or Directories or Rename them

#### Purpose

The "mv" command moves files or whole directories from one location to another. It can be used to rename files and directories, too.

#### Call and Parameters

```
# mv [Options] [Source(s)] [Target]
```

An overview with all supported options can be requested with

```
mv -help
```

One or more files can be specified as the source(s), wildcards (like \* or ?) are allowed. The target can either be a directory or, if the source is one single file, a target filename. In this case, the original file will be moved and renamed at the same time.

Moving a whole directory structure is possible by specifying a directory as the source.

#### Examples

```
# mv /dir_a/file_a /dir_b/file_b
```

(moves the file file\_a from the /dir\_a directory into the target directory /dir\_b and renames it to file\_b)

```
# mv /dir_a/file_a /dir_b/
```

(moves the file file\_a from the /dir\_a directory into the target directory /dir\_b but preserves the filename)

```
# mv /dir_a/file_*.txt /tmp/
```

(moves all files from /dir\_a with a filename beginning with "file\_" and ending on ".txt" into the directory /tmp)

```
# mv /dir_a/ /tmp/
```

(moves the whole directory /dir\_a with all its subdirectories and included files into the /tmp directory)

### 9.2.3.14 rm - Delete Files and/or Directories

## Purpose

The "rm" command deletes one or more files or whole directories (including all their content, i.e. files and subdirectories). It is possible to use wildcard characters to delete a group of similar named files, e.g. "\*.bak" includes all filenames that end on ".bak". Since deleting files and directories can lead to system malfunction and all kinds of failures, the "rm" command should only be used if you are 100% sure that the specified files/directories are not required for proper operation of the LANTIME system. If you are in doubt, please contact Meinberg support.

Deleted files and directories cannot be restored and are lost forever. Because of this, the "rm" command should be used with the greatest caution.

## Call and Parameters

```
# rm [Options] [File1] [File2] ...
```

An overview of all supported options can be requested with

```
rm -help
```

One or more files can be specified, wildcards (like \* or ?) are allowed. If a whole directory and all its contents shall be deleted, the "-r" option needs to be specified.

**There is no "Are you sure?" prompt shown before the deletion is carried out, the system will immediately delete the specified files. In order to avoid system failures, please triple check whether the file(s) and/or directories you specify are really OK to be deleted.**

## Examples

```
# rm /dir_a/file_a  
(deletes the file file_a from the /dir_a directory)
```

```
# rm -r /dir_b/  
(deletes the whole /dir_b directory and all included files and subdirectories - forever)
```

### 9.2.3.15 cat - Show File Contents

#### Purpose

The "cat" command shows the contents of a given file.

#### Call and Parameters

```
# cat [filename]
```

The content of the given file is printed. The "cat" command can be combined with the "less" command to allow paginated output and offers an easier way to review a file.

#### Examples

```
# cat /var/log/messages
```

(shows the content of the file messages in the /var/log directory)

```
# cat /var/log/lantime_messages | less
```

(shows the contents of the file /var/log/lantime\_messages, the "less" command offers a way to navigate the file using the arrow keys, space (=next page) and offers a search function ("/"). Closing the file can be achieved by pressing the "q" key).

### 9.2.3.16 Firmware Management

LTOS V6 allows the installation of multiple firmware images in parallel. Selecting which of the installed images is going to be loaded at the next system start - and commands that allow to remove or install a firmware release manually without using the web user interface - are described in this section.

### 9.2.3.17 fwlist - List Installed Firmware Images

#### Purpose

The "fwlist" command prints a list of all firmware images which are installed on the device.

#### Call and Parameters

```
# fwlist [-v] [searchpattern]
```

The [searchpattern] parameter can be used to filter the list of installed firmware images. If no searchpattern is specified, all installed images are listed. The "-v" option will show the version number of each firmware image behind its name.

#### Examples

```
# fwlist  
(shows all installed firmware images)
```

```
# fwlist -v fw_*  
(shows all installed firmware images with a name beginning with "fw_" and their respective firmware revision)
```

```
# fwlist OSV  
(shows the installed firmware image with the name "OSV")
```

### 9.2.3.18 fwselect - Select/Show Activated Firmware Image

#### Purpose

With the "fwselect" command it is possible to activate an installed firmware image, i.e. that firmware image is started during the next boot sequence. If an error occurs during the activation, the system will roll back to the previous state.

If fwselect is started without any parameters, it will show the name of the activated firmware image, i.e. the image that is going to be used at the next system start.

#### Call and Parameters

```
# fwselect [FWImage]
```

The [FWImage] parameter specifies which firmware image is going to be used at the next system start. Without this parameter, "fwselect" will print the name of the currently selected image and exits.

#### Examples

```
# fwselect
(shows the currently activated firmware image)
```

```
# fwselect fw_6.12.004
(selects the image "fw_6.12.004" and tries to prepare the system to use this image at the next boot sequence)
```

### 9.2.3.19 fwrn - Delete Firmware Images

#### Purpose

The "fwrn" command can be used to delete one or more firmware images from the internal flash memory to regain space.

#### Call and Parameters

```
# fwrn [FWImage]
```

or

```
# fwrn [-wipe-all [keep=X]] [FWImage]
```

The *FWImage* parameter defines which image will be deleted. The second form (-wipe-all) deletes *all* firmware images except the OSV image, the currently running image and - if different from the running image - the firmware image that has been selected to be activated at the next system start. The optional "keep" parameter allows to specify how many firmware images should be preserved in addition to the non-deletable images mentioned above.

The -wipe-all option can be shortened by using -W instead.

#### Examples

```
# fwrn fw_6.14.021
(deletes the firmware image fw_6.14.021)
```

```
# fwrn -wipe-all keep=2
(deletes all firmware images except the currently active image, the OSV image and the firmware image that has been selected (by fwselect) to be activated at the next system start)
```

### 9.2.3.20 fwuncompress - Extract Firmware Image

## Purpose

Starting with version 6.15 all firmware updates will be installed in compressed form to preserve flash space. Such an image is read-only and cannot be modified, i.e. it is not possible to add or remove files or change their content in any way. Under normal circumstances this is not required and therefore it is recommended to use compressed images instead of uncompressed ("standard") ones. If it is necessary for a specific user requirement to change the contents of a firmware image, the "fwuncompress" command can extract the contents of a compressed image and create a new, uncompressed copy of it. The (compressed) source image will not be touched or changed in any way by "fwuncompress" and, if not required anymore, would have to be deleted manually afterwards using the "fwrn" command.

It is possible to uncompress the currently running firmware image without any problems.

## Call and Parameters

```
# fwuncompress FWImage
```

The specified image (name usually starts with "fw\_") will be used to create an uncompressed copy of it. The newly created image will get a prefix "u", i.e. uncompressing a firmware image "fw\_6.15.015" will create an uncompressed image named "ufw\_6.15.015".

## Examples

```
# fwuncompress fw_6.16.002
```

(extract the contents of the compressed firmware image fw\_6.16.002, creating a new image named ufw\_6.16.002)

### 9.2.3.21 User Account Management

The system supports multiple local user accounts and remote authentication methods using external RADIUS and TACACS+ servers. Managing the accounts and checking the current status is possible with several commands.



### 9.2.3.22 Network Configuration

A number of CLI commands enable you to change the LANTIME network parameters in addition to the front panel menu (if available) or, in case the initial network configuration has already been set up, by using the web interface. This can be very useful when network connectivity is lost or in case a special network setup is required that is not supported by the web UI.

The main configuration file for network related settings is `/etc/mbg/net.cfg` which contains definitions and parameters for all physical and logical ("virtual") network interfaces. This file, its structure and content, is described in detail in the Configuration Files chapter.

### 9.2.3.23 netconfig - Check for Network Configuration Changes and Apply them

#### Purpose

With `netconfig` the system will compare the state of all network interfaces (both physical and virtual) with their configuration. If any required changes are detected, they will be applied.

If, for example, a virtual interface has been configured but is missing, it will be created and configured according to the `net.cfg` contents.

#### Call and Parameters

```
# netconfig
```

This command does not support any parameters.

#### Examples

```
# netconfig
```

(checks all network interfaces and applies changes, if the configuration differs from the current state)

### 9.2.3.24 nicinfo - Show Physical Network Interface Configuration State

#### Purpose

**nicinfo** displays the configuration status of physical network interfaces. It lists the MAC address, the assigned bonding group, the link speed and duplex mode as well as the IPv6 mode.

#### Call and Parameters

```
# nicinfo [Optionen] [INTERFACE]
```

This command understands the following options:

**-c** Check Link Mode

Shows only the current link state (e.g. 100FDX) and whether the network port is monitored or not (LINK\_CHECK).

**-s** Short Mode

This option leads to a very compact output, only indicating the current configuration state of an interface:

```
+ Not existing, needs to be created
! Changed, requires reconfiguration
- Existing but not configured, needs to be removed
= Configuration is correct, no changes required
```

If an interface name is specified with the INTERFACE parameter, "**nicinfo**" will only show information about the specified interface (e.g. lan0). If this parameter is not specified or empty, the command will output information about all interfaces.

#### Examples

```
# nicinfo
```

```
Please wait ...
```

```
Current state of physical interfaces:
```

```
lan0 matches configuration (lan0 00:13:95:00:6b:ef - 100FDX AUTO=ON
IPV6=ACTIVATED+AUTOCONF)
```

```
lan1 matches configuration (lan1 00:60:6e:7a:d3:4d - 10HDX AUTO=ON
IPV6=ACTIVATED)
```

```
lan2 matches configuration (lan2 00:60:6e:7a:d3:4e - 10HDX AUTO=ON
IPV6=DEACTIVATED)
```

```
lan3 matches configuration (lan3 00:60:6e:7a:d3:4f - 10HDX AUTO=ON
IPV6=DEACTIVATED)
```

(shows the status of all physical interfaces)

```
# nicinfo -s
```

```
=lan0
```

```
!lan1/1
```

```
=lan2
```

```
=lan3
```

(shows configuration state for all interfaces, in this case there is a pending change for lan1)

```
# nicinfo -c lan0
```

```
Please wait ...
```

```
Current state of lan0:
```

```
Status of physical interface lan0 is 100FDX LINK_CHECK=ON
```

(shows the link state of lan0 - 100Mbit/s Full Duplex - and whether it is monitored or not)

### 9.2.3.25 nicmgr - Management of Physical Network Interfaces

## Purpose

The "nicmgr" command allows to add unconfigured physical network interfaces to the network configuration in order to be able to assign virtual network interfaces to them. This is necessary whenever new network interface cards are added to an existing system, for example by inserting a new LNE module into a device. It is also possible to remove network interfaces from the configuration with nicmgr, if those physical network interfaces have been permanently removed from the system.

## Call and Parameters

```
# nicmgr help
or
# nicmgr assign [FREE_IF] [IFNUMBER]
or
# nicmgr remove [IFNUMBER]
or
# nicmgr autoassign
or
# nicmgr autoreplace
```

The FREE\_IF parameter represents an unconfigured/uninitialized network interface. These interfaces are named ethX (X is a running number which is assigned at startup or directly after a network expansion module has been inserted into the system). When a LANTIME Network Expansion (LNE) card is added to the system, the four new interfaces will be named "eth0, eth1, eth2 and eth3. As soon as they have been correctly added to the configuration, they will be renamed lanX (where X is also a number that has been assigned by the user or the system). The first physical network interface is always located on the management CPU module and is named "lan0".

IFNUMBER is the number of an already added (configured) port, therefore IFNUMBER=1 refers to the physical interface lan1, a "5" means lan5 and so on.

The two commands "autoassign" and "autoreplace" simplify the addition or the replacement of multiple ports. "autoassign" automatically adds all detected and currently unconfigured network interfaces to the configuration. The "autoreplace" command searches for configured but missing interfaces (e.g. if a LNE card has been removed due to a failure, its interfaces are still in the configuration but they are missing). If it finds missing interfaces and unconfigured interfaces, it will replace the configuration of the first missing interface with the first unconfigured interface, the second missing interface with the second unconfigured interface and so on.

## Examples

```
# nicmgr assign eth0 7
(adds the currently unconfigured interface eth0 as lan7 to the system)
```

```
# nicmgr remove 6
(removes lan6 from the system configuration)
```

```
# nicmgr autoassign
(automatically adds all unconfigured/unassigned interfaces to the system configuration)
```

```
# nicmgr autoreplace
(replaces all missing physical network ports with available unconfigured ethX interfaces)
```

### 9.2.3.26 netinfo - Show Logical Network Interface Configuration State

#### Purpose

**netinfo** displays the configuration status of logical ("virtual") network interfaces, it shows IP addresses and the configuration state of the interface(s), i.e. if an interface state corresponds to the configured state.

#### Call and Parameters

```
# netinfo [Optionen] [INTERFACE]
```

This command understands the following options:

**-a** Advanced Info Mode

Shows more detailed information for each interface, e.g. the MAC address of the assigned physical interface and the administrative state.

**-s** Short Mode

This option leads to a very compact output, only indicating the current configuration state of an interface:

```
+ Not existing, needs to be created
! Changed, requires reconfiguration
- Existing but not configured, needs to be removed
= Configuration is correct, no changes required
_ No Configuration, empty configuration for this interface
```

If an interface name is specified with the INTERFACE parameter, "**netinfo**" will only show information about the specified interface (e.g. lan0:0). If this parameter is not specified or empty, the command will output information about all interfaces.

#### Examples

```
# netinfo
Current state of logical interfaces:
bond0:2 matches configuration (STATIC 10.99.109.11 255.255.255.0 - NONE)
lan0:0 matches configuration (DHCP - - - NONE)
lan1:1 [Virtual Interface 1] is not active and requires to be configured
bond0:3 has no configuration
```

(shows the status of all logical interfaces)

```
# netinfo -s
=bond0:2
=lan0:0
+lan1:1
_bond0:3
```

(shows configuration state for all logical interfaces)

```
# netinfo -s -i lan0:0
=lan0:0/0
```

(like above, but now contains the interface number, too: /0)

### 9.2.3.27 System Services

The installed system services fulfill a number of duties, most of them provide a certain network protocol service like SSH (Secure SHell) oder HTTP (Hyper Text Transport Protocol, the web GUI). Starting and stopping these services is normally managed automatically depending on the configuration of the system. If the TELNET service has been disabled on all interfaces, it will automatically be stopped by the system. When the user re-enables it on at least one interface, the system will restart the corresponding TELNET service.

In certain situations, it can be necessary to check the status of a service or manually start or stop it. After a manual configuration file change it is often required to restart a related service to force it to apply the changed configuration.

With the command "status all", the running state of all registered services will be listed and therefore can be used to find out which services are available on a certain device.

This chapter describes the various CLI commands that control the system services.

### 9.2.3.28 status - Show Status of System Services

#### Purpose

The status command shows whether a specified system service is currently running or not. It is also possible to get the status for all services.

#### Call and Parameters

`# status service`

The only parameter is the name of the service for which the running state should be shown. Specifying "all" instead of a certain service name will result in showing the state of all services.

#### Examples

```
# status ssh
(shows whether the SSH service is currently running or not)
```

```
# status all
(lists the state of all system services)
```

### 9.2.3.29 start - Start a System Service

#### Purpose

With this command, a specified system service can be started if it is not already running.

#### Call and Parameters

```
# start service
```

The *service* parameter specifies which service should be started. The system first checks whether the service is already running or not. If it is, nothing will happen. You can check the running state of a service with the **status** command.

#### Examples

```
# start ssh  
(starts the SSH service if it is not already running)
```

```
# start http  
(starts the HTTP service)
```

### 9.2.3.30 stop - Stop a System Service

#### Purpose

The **stop** command will stop a specified system service, i.e. the relevant processes are terminated.

#### Call and Parameters

```
# stop service
```

With the *service* parameter you can specify which service should be stopped. The system first checks whether the service is currently running or not. It will only try to stop the service if it is running, otherwise nothing will happen. The system stops a network related service automatically if it has been disabled on all interfaces. Stopping such a service will immediately result in terminating any active connections and disables connectivity on all interfaces.

#### Examples

```
# stop ssh  
(stops the SSH service if it is running - ATTENTION: this will immediately terminate any active SSH connection, including the one that you used to enter this command)
```

```
# stop https  
(stops the HTTPS service)
```

### 9.2.3.31 restart - Restart a System Service

#### Purpose

The **restart** command stops a service (if it is running) and then restarts it. If it was not running when the restart command has been called, it is started normally (omitting the "stop" command).

#### Call and Parameters

```
# restart service
```

*service* specifies which service should be restarted. The system first checks whether the service is already running or not. If it is, it will stop the service and then restart it. A non-running service will simply be started.

#### Examples

```
# restart ssh  
(restarts the SSH service, active connections are terminated)
```

```
# restart http  
(restarts the HTTP service)
```

### 9.2.3.32 reload - Reload Configuration of a System Service

#### Purpose

The **reload** command forces a service to reload its configuration, for most services this is achieved by restarting them. See "restart" command, but "reload" automatically chooses the applicable way for each service.

#### Call and Parameters

```
# reload service
```

The *service* parameter specifies for which service the configuration should be reloaded.

#### Examples

```
# reload ssh  
(reloads the SSH service configuration by restarting it)
```

```
# reload http  
(reloads the HTTP service configuration by restarting it)
```

### 9.2.3.33 `svccfg` - Check for System Service Configuration Changes and Apply them

#### Purpose

The `svccfg` command will check for all services if one of the registered configuration files changed (since the last start of the service). If such a change is detected, the corresponding service is forced to reload its configuration (with the `reload` command). A list of all registered configuration changes can be found in the `/var/run/services/svccfg.db` file. This file can be inspected by using the `cat` command.

#### Call and Parameters

```
# svccfg
```

This command does not support any parameters. It will always check all registered files for all services.

#### Examples

```
# svccfg
```

(checks all registered configuration files for all services and, if a file change has been detected, reloads the corresponding service)



### 9.2.3.34 Showing Current Status Information - show and monitor

LTOS offers a number of status information displays to allow the user to view the current status of the system. A whole range of detailed information options is available by using the standard system commands, but often these commands produce a very detailed output that contains a lot of unimportant or unnecessary information and uses a hard to read format for presenting the information. In order to overcome this limitation, LTOS V6 includes a number of commands that generate an optimized output in an easy to understand format, concentrating on the most important status information variables.

This information can be requested by using one of the two commands "show" and "monitor". While "show" will display the current status and then returns to the command prompt, "monitor" will keep running and updates its output in a fixed time interval. In order to return to the command prompt, "monitor" has to be stopped by pressing CTRL+C.

After the "show" or "monitor" command word it is necessary to specify which type of information should be displayed. The different types of information are provided by so-called plugins, each of them generating a specific type of status information. The "ip" plugin for example can generate and output a list of all IP addresses currently used by the system. In order to get this information, the user either has to enter the command "show ip" (will generate and show a list of all IP addresses and then returns to the command prompt) or "monitor ip" (the IP address list is shown and will for example be updated every 10 seconds until CTRL+C is pressed to stop the monitor command).

The following sections will explain the available plugins and, if necessary, their additional parameters.

### 9.2.3.35 cpuload - Show CPU Utilization Metrics

#### Purpose

The "cpuload" module shows the current CPU utilization metrics of the system.

#### Call and Parameters

```
# show cpuload
```

or

```
# monitor cpuload
```

This command does not have any additional parameters. The following output line will be generated once (using the "show" command) or every 5 seconds (using the "monitor" command):

```
Tue Jan 21 12:52:26 UTC 2014 Cpu(s):  3.0%us, 4.8%sy, 0.0%ni, 92.1%id,
0.0%wa, 0.0%hi, 0.1%si, 0.0%st Loadavg:  0.36 0.21 0.19 1/80 12803
```

"Tue Jan 21 12:52:26 UTC 2014" is the current date/time, "Cpu(s): 3.0%us, 4.8%sy, 0.0%ni, 92.1%id, 0.0%wa, 0.0%hi, 0.1%si, 0.0%st" indicates the CPU utilization for each CPU state (us=User, sy=System, ni=nice, wa=I/O wait, hi=Hardware IRQ, si=Software IRQ, st=Steal Time), "Loadavg: 0.36 0.21 0.19" represents the load average values for the last 1, 5 and 10 minutes and "1/80 12803" shows the number of currently running/total processes and the last assigned process ID.

#### Examples

```
# show cpuload
```

(shows the current CPU utilization)

```
# monitor cpuload
```

(continuously shows the CPU utilization every 5 seconds)

```
# s c
(shortcut for "show cpuload")
```

```
# m c
(shortcut for "monitor cpuload")
```

### 9.2.3.36 devices - Meinberg Hardware Module and Components List

#### Purpose

The "devices" module shows the system details and a list of detected Meinberg hardware components.

#### Call and Parameters

```
# show devices
```

or

```
# monitor devices
```

This command does not have any additional parameters. The following output line will be generated once (using the "show" command) or every 10 seconds (using the "monitor" command):

```
System Details
System ID: M200
Backplane: P
CPU Carrier: V33
Platform: AMDCONGA
CPU Board: E900
CPU ID: CPU=AuthenticAMD CPUID=AuthenticAMD MODELID=...
RAM: 100868 kB

Found 1 reference clock[s]
GPS170 :2.29 S/N: 11123120 BinaryPort:2 TimeStrPort:0

System Components
Bus/Id Device Product Ver Serial Status
USB 001/005: 1938:0101 Meinberg CPC - Control Panel Controller 1.12 1.0.0
0x0001
```

#### Examples

```
# show devices
(shows the system details and the list of detected Meinberg components)
```

```
# monitor devices
(continously repeats the "show devices" command until CTRL+C has been pressed)
```

```
# s d
(shortcut for "show devices")
```

```
# m c
(shortcut for "monitor devices")
```

### 9.2.3.37 ip - List all active IPv4 and IPv6 Addresses

## Purpose

The "ip" plugin generates a list of all currently active IP addresses.

## Call and Parameters

```
# show ip [Filter]
```

or

```
# monitor ip [Filter]
```

The "[Filter]" parameter is optional and allows to filter the output of "show ip" or "monitor ip" using a search keyword.

In the "monitor" mode, the list of IP addresses is automatically refreshed every 10 seconds, until CTRL+C has been pressed.

The output of "show ip" / "monitor ip" looks like this (example):

```
Currently Active Network Interfaces:
lan0:0 linklocal ipv6 fe80::213:95ff:fe0a:580b/64
lan0.120 static ipv4 172.16.25.200/255.255.000.000
lan0:0 static ipv6 bad:babe:25::200/64
lan1:1 dhcp ipv4 192.168.10.12/255.255.255.000
```

The first column represents the interface name, which is composed from the name of the physical port (e.g. "lan0" for the first Ethernet port or "bond2" for an interface that is part of the bonding group 3) and the ID of the logical ("virtual") network interface. This can be either the interface number (":0" for the first virtual interface) or the VLAN ID (".120" for VLAN ID 120) .

The second column lists the type of the address, this can be "static" for manually configured static IP addresses, "dhcp" for IP addresses automatically assigned by DHCP/DHCPv6, "linklocal" for IPv6 Linklocal addresses or "ra" for IPv6 addresses assigned by a router advertiser.

Whether an IP address entry is an IPv4 or IPv6 address is specified in the third column.

The fourth and last column finally shows the IP address and either the netmask (for IPv4) or the prefix length (for IPv6).

## Examples

```
# show ip
```

(shows the current list of all active IP addresses)

```
# monitor ip
```

(like "show ip", but automatically refreshes every 10s)

```
# show ip lan0
```

(shows all IP addresses assigned to the physical port "lan0")

```
# show ip ipv6
```

(shows only the IPv6 addresses)

```
# show ip dhcp
```

(lists all IP addresses assigned by DHCP or DHCPv6)

```
# monitor ip bond
```

(lists all IP addresses assigned to one of the bonding interfaces and refreshes automatically every 10s)

### 9.2.3.38 lantimelog - Show LANTIME Log File

#### Purpose

This "show" plugin lists the entries of the LANTIME log file (/var/log/lantime\_messages), a file that only contains the most important events.

#### Call and Parameters

```
# show lantimelog [Filter]
```

or

```
# monitor lantimelog [Filter]
```

In the "monitor" mode, only the most recent protocol entries are shown, afterwards the command will wait for new entries and prints them as soon as they are created. The CTRL+C key combination aborts waiting for new events and returns to the command prompt.

If a Filter parameter has been added, only those lines in the log file will be printed that contain the given filter string (this is not case sensitive). If no filter is specified, all entries will be listed.

The output of this command looks like this:

```
# show lantimelog
2014-11-20 13:26:55 UTC: LANTIME -> OSCILLATOR ADJUSTED [Refclock: 1 ]
2014-11-20 13:26:07 UTC: LANTIME -> NORMAL OPERATION
2014-11-20 13:26:03 UTC: LANTIME -> NETWORK LINK UP [Affected LAN
Interface: 1 ]
2014-11-20 13:25:57 UTC: LANTIME -> NTP RESTART
2014-11-20 13:25:57 UTC: LANTIME -> NTP SYNC TO GPS
#
```

#### Examples

```
# show lantimelog
```

(shows the full LANTIME protocol file )

```
# show lantimelog ntp
```

(shows all protocol entries in the log file that contain the string "NTP")

```
# monitor lantimelog
```

(lists the last 20 entries and then waits for new entries, cancel waiting with CTRL+C)

```
# s la
```

(short form of "show lantimelog")

```
# m la
```

(short form of "monitor lantimelog")

### 9.2.3.39 linkstate - Show Connection Status of Physical Network Interfaces

## Purpose

The "linkstate" plugin shows the current network connection state of one or more physical network interfaces.

## Call and Parameters

```
# show linkstate [Filter]
```

or

```
# monitor linkstate [Filter]
```

The "[Filter]" parameter is optional and can be specified to limit the output to only those network interfaces containing the filter string either in their name or MAC address.

The "monitor" mode automatically refreshes the output every 10 seconds until CTRL+C has been pressed.

The output of "show linkstate" or "monitor linkstate" looks like this:

```
Current LINK state:...
lan0:  [00:13:95:12:65:36] 100FDX
lan1:  [ec:46:70:ef:3f:e8] NO_LINK
lan2:  [ec:46:70:ef:3f:e9] 1000FDX
lan3:  [ec:46:70:ef:3f:ea] NO_LINK
```

The first column contains the name of the interface, e.g. "lan0" for the first physical port.

The second column represents the MAC address of the interface and the third column indicates the current connection state. This can be either "NO\_LINK", if no active connection could be established, or it shows the current connection speed (10, 100, 1000 or 10000) in MBit/s plus the duplex mode (FDX for full duplex or HDX for half duplex).

## Examples

```
# show linkstate
(shows the connection state of all physical network interfaces)
```

```
# monitor linkstate
(like "show linkstate", but refreshing the output every 10s until CTRL+C has been pressed)
```

```
# show linkstate lan0
(shows only the state of lan0)
```

```
# s li
(short form of "show linkstate")
```

```
# m li
(short form of "monitor linkstate")
```

### 9.2.3.40 modules - Kernel Driver and Module List

## Purpose

This "modules" plugin shows a list of all loaded kernel modules and drivers. If you want to show all detected hardware modules and components in your system, please check out the "show devices" command.

## Call and Parameters

```
# show modules
```

or

```
# monitor modules
```

This command does not have any additional parameters. The following output line will be generated once (using the "show" command) or every 10 seconds (using the "monitor" command):

```
Loaded kernel modules:
Module Size Used by
ip6table_filter 708 0
ip6_tables 8129 1 ip6table_filter
usb_storage 31278 0
rndis_host 3875 0
cdc_subset 1165 0
cdc_ether 2996 1 rndis_host
bonding 63801 0
ax88179_178a 10848 0
dmfe 13263 0
xt_state 780 0
8021q 11207 0
ipv6 174754 20
squashfs 16978 1
pata_cs5536 2138 1
ext3 85915 0
mbcache 3228 1 ext3
jbd 28294 1 ext3
libahci 14214 0
cgosdrv 18409 0
mdio_bitbang 1515 0
libphy 13845 1 mdio_bitbang
usbnet 10270 4 rndis_host,cdc_subset,cdc_ether,ax88179_178a
ftdi_sio 25482 2
```

## Examples

```
# show modules
(shows all currently loaded kernel modules)
```

```
# monitor modules
(continously repeats the "show modules" command until CTRL+C has been pressed)
```

```
# s m
(shortcut for "show modules")
```

```
# m m
(shortcut for "monitor modules")
```

### 9.2.3.41 network - Show current Network State

## Purpose

This command shows an overview of the currently active network configuration, including the assigned IP addresses, the link state of the physical network interfaces and, if appropriate, the state of bonding groups.

## Call and Parameters

**# show network**

This command does not have any additional parameters. The following output line will be generated:

```
=== Physical Interface lan0 : 00:13:95:12:65:36
Speed: 100Mb/s
Duplex: Full
Link detected: yes

Assigned Virtual Interfaces: [:0]
Active Virtual Interfaces: -----
lan0:0 static ipv4 172.16.25.204/255.255.000.000

=== Physical Interface lan1 : ec:46:70:00:3f:e8
Speed: 10Mb/s
Duplex: Half
Link detected: no

Assigned Virtual Interfaces: [:1]
```

## Examples

```
# show network
(shows the currently active network configuration)
```

```
# s n
(shortcut for "show network")
```

### 9.2.3.42 Processes - List System Processes

#### Purpose

The "show processes" command generates a list of all processes currently running on the system. In combination with a filter string it is possible to check if a certain command or software component has been started and is still running.

#### Call and Parameters

# **show processes** [*Filter*]

or

# **monitor processes** [*Filter*]

The "[Filter]" parameter is optional and allows to filter the output of "show processes" or "monitor processes" using a search keyword (case insensitive). The filter string can contain either a part of a command name or a process ID.

In the "monitor" mode, the list of processes is automatically refreshed every second until CTRL+C is pressed.

The output of "show processes" / "monitor processes" looks like this (example):



```

PID TTY STAT TIME COMMAND
1 ? Ss 1:23 /sbin/init
2 ? S 0:00 [kthreadd]
3 ? S 16:12 [ksoftirqd/0]
5 ? S< 0:00 [kworker/0:0H]
7 ? S< 0:00 [kworker/u:0H]
8 ? S< 0:00 [khelper]
9 ? S 0:00 [kworker/u:1]
146 ? S 0:00 [bdi-default]
147 ? S< 0:00 [kblockd]
155 ? S< 0:00 [ata_sff]
162 ? S 0:00 [khubd]
268 ? S< 0:00 [rpciod]
279 ? S 0:00 [kswapd0]
280 ? S 0:00 [fsnotify_mark]
281 ? S< 0:00 [nfsiod]
282 ? S< 0:00 [crypto]
552 ? S< 0:00 [deferwq]
554 tty4 Ss+ 0:00 /sbin/getty 38400 tty4
556 tty2 Ss+ 0:00 /sbin/getty 115200 tty2
557 tty3 Ss+ 0:00 /sbin/getty 38400 tty3
600 ? S 0:00 cat /proc/kmsg
615 ? S 1694 ? S 0:00 [scsi_eh_0]
1699 ? S 0:00 [scsi_eh_1]
1704 ? S 1:22 [kworker/u:2]
1777 ? S< 0:00 [kworker/0:1H]
1941 ? S< 0:00 [loop0]
4861 ? S 0:01 [kworker/0:2]
6056 ? S< 0:00 [bond0]
6091 ? S< 0:00 [bond1]
6126 ? S< 0:00 [bond2]
6161 ? S< 0:00 [bond3]
6196 ? S< 0:00 [bond4]
7885 ? Ss 2:55 crond
7903 ? Ss 0:00 /sbin/dbus-daemon -config-file=/etc/dbus-1/system.conf
8998 ? S 0:02 [kworker/0:1]
9153 ? S 1:53 ifplugd -M -f -a -b -d 1 -p -q -i lan0
9179 ? S 1:51 ifplugd -M -f -a -b -d 1 -p -q -i lan1
9205 ? S 1:51 ifplugd -M -f -a -b -d 1 -p -q -i lan2
...

```

The first column represents the process ID and the second column contains the terminal name (TTY), which can be "?" for internal processes not bound to a specific terminal.

The third column shows the current process state:

```

D Uninterruptible sleep (usually IO)
R Running or runnable (on run queue)
S Interruptible sleep (waiting for an event to complete)
T Stopped, either by a job control signal or because it is being traced.
X dead (should never be seen)
Z Defunct ("zombie") process, terminated but not reaped by its parent.

```

In the fourth column the cumulative CPU time used by this process and - after that - the command itself, typically with its parameters, is listed.

## Examples

```
# show processes
```

(shows the current list of all processes currently running on the system)

```
# monitor processes
```

(like "show ip", but automatically refreshes every second)

```
# show processes ntp
```

(shows all processes which contain the search term "ntp" in their command line, this is not case sensitive)

```
# s p
```

(short form of "show processes")

```
# m p ntp
```

(short form of "monitor processes ntp")

### 9.2.3.43 route - List all active IPv4 and IPv6 Network Routes

## Purpose

The "route" plugin show all currently active IP routes and routing rules.

## Call and Parameters

```
# show route [Filter]
or
# monitor route [Filter]
```

The "[Filter]" parameter is optional and allows to filter the output of "show route" or "monitor route" using a search keyword. This can be used to limit the output to only those entries that contain the specified search term.

In the "monitor" mode, the routing entry list is automatically refreshed every 10 seconds, until CTRL+C has been pressed.

The output of "show route" / "monitor route" looks like this (example):

```
Routing Table Entries:
TABLE DEV TARGET
main lan0 default
main lan0 172.16.0.0/16 proto kernel scope link src 172.16.25.204
local lo broadcast 127.0.0.0 proto kernel scope link src 127.0.0.1
local lo local 127.0.0.0/8 proto kernel scope host src 127.0.0.1
local lo local 127.0.0.1 proto kernel scope host src 127.0.0.1
local lo broadcast 127.255.255.255 proto kernel scope link src 127.0.0.1
local lan0 broadcast 172.16.0.0 proto kernel scope link src 172.16.25.204
local lan0 local 172.16.25.204 proto kernel scope host src 172.16.25.204
local lan0 broadcast 172.16.255.255 proto kernel scope link src
172.16.25.204
main lo local ::1 proto none metric 0
0 lo unreachable default proto kernel metric -1 error -101

Routing Rules:
0: from all lookup local
32766: from all lookup main
32767: from all lookup default
```

## Examples

```
# show route
(shows the current list of all active IP network routes)
```

```
# monitor route
(like "show route", but automatically refreshes every 10s)
```

```
# show route lan0
(shows all network routes assigned to the physical port "lan0")
```

```
# s r
(short form of "show route")
```

```
# m r
(short form of "monitor route")
```

### 9.2.3.44 syslog - Show System Log File

## Purpose

This "show" plugin lists the entries of the system log file (/var/log/messages), a file that contains all events and status changes.

## Call and Parameters

```
# show syslog [Filter]
```

or

```
# monitor syslog [Filter]
```

In the "monitor" mode, only the most recent protocol entries are shown, afterwards the command will wait for new entries and prints them as soon as they are created. The CTRL+C key combination aborts waiting for new events and returns to the command prompt.

If a Filter parameter has been added, only those lines in the log file will be printed that contain the given filter string (this is not case sensitive). If no filter is specified, all entries will be listed.

The output of this command looks like this:

```
# show syslog
Dec 15 10:41:08 timeserver root: Restarting syslog due to configuration
change ...
Dec 15 10:41:08 timeserver syslog-ng[7864]: Termination requested via
signal, terminating;
Dec 15 10:41:08 timeserver syslog-ng[7864]: syslog-ng shutting down;
version='2.0.9'
Dec 15 10:41:08 test_tr0_lt04 syslog-ng[22289]: syslog-ng starting up;
version='2.0.9'
Dec 15 11:19:40 test_tr0_lt04 sshd[5061]: Accepted password for root from
172.16.3.120 port 41449 ssh2
Dec 15 11:19:40 test_tr0_lt04 sshd[5061]: pam_unix(sshd:session): session
opened for user root by (uid=0)
Dec 15 11:19:46 test_tr0_lt04 sshd[5061]: Received disconnect from
172.16.3.120: 11: PECL/ssh2 (http://pecl.php.net/packages/ssh2)
Dec 15 11:19:46 test_tr0_lt04 sshd[5061]: pam_unix(sshd:session): session
closed for user root
#
```

## Examples

```
# show syslog
```

(shows the full system protocol file )

```
# show syslog failed
```

(shows all protocol entries in the log file that contain the string "failed")

```
# monitor syslog
```

(lists the last 20 entries and then waits for new entries, cancel waiting with CTRL+C)

```
# s s
```

(short form of "show syslog")

```
# m s
```

(short form of "monitor syslog")

```
# s  
(short form of "s s")
```

```
# m  
(short form of "m s")
```

### 9.2.3.45 version - Show Current Firmware Version

## Purpose

The "version" module shows the firmware version of the currently running firmware image.

## Call and Parameters

# **show version**

```
Running LTOS V6.16.005 [standard]  
System Version : Linux heiko_tr0_lt04 3.7.1 #16 Wed Jul 16 10:33:54 UTC  
2014 i586 unknown
```

## Examples

```
# show version  
(shows the firmware version)
```

```
# s v  
(shortcut for "show version")
```

### 9.2.3.46 System Commands

The monitoring of system resources like flash or RAM capacity is supported by a group of CLI commands that are described in this section. Most of them are intended to show the status of certain resources (like "free RAM space"), assisting you with detecting and diagnosing a problem.

### 9.2.3.47 `reboot` - Full System Restart

#### Purpose

The **reboot** command initiates a restart of the whole system. This includes stopping all services and resetting the CPU. Please note that any unsaved configuration changes are not automatically saved, therefore the system comes back up with the last startup configuration that was saved using **saveconfig**.

It is possible to specify a delay, i.e. the **reboot** process waits for a given time before carrying out the system restart. Such a delay can be applied in the background, allowing a user to continue to work in the foreground, e.g. changing configuration files and applying changes. A backgrounded **reboot** process can be canceled at any time during the waiting period, allowing a user to set a reboot time before trying to change the system configuration. If one of these changes results in the system becoming unreachable (e.g. due to a network IP address configuration error), the backgrounded **reboot** process will automatically restart the system after the specified time and restores the last saved startup configuration, resulting in a restore of the network connectivity. Once the user completed and tested all configuration changes successfully and verified that the system is still reachable, the waiting **reboot** process can be canceled.

**reboot** notifies all logged in users in active SSH, TELNET and serial console sessions about the reboot and the specified waiting period. This enables everyone to save any changes made and log out correctly or cancel the restart, as long as the **reboot** process is still in a waiting state.

#### Call and Parameters

```
# reboot [DELAY|stop]
```

If a delay is specified, the `reboot`-command will wait for the given time before restarting the system. This delay can be specified as a simple numeric value representing the number of seconds to wait. It can also be specified in minutes or hours by using a "m" or "h" suffix to the numeric value (see examples).

In order to be able to continue to work in the same SSH/TELNET/serial console session, the **reboot** command can be told to wait in the background instead of blocking the shell prompt. This background mode is enabled by adding a "&" character at the end of the command line.

A waiting **reboot** process can be canceled by specifying "stop" instead of a delay. This can be used to stop a restart process that is waiting in the background but it can also be used to cancel the reboot process of another user.

If no parameter is given, **reboot** will restart immediately, i.e. after the default waiting time of 2 seconds.

#### Examples

```
# reboot
(immediately restarts the system, i.e. after the 2s default waiting period)
```

```
# reboot 20
(restarts in 20 seconds)
```

```
# reboot 1h
(restarts in 1 hour)
```

```
# reboot 5m &
(restarts in 5 minutes, but waits in the background allowing the user to enter additional commands in the meantime)
```

```
# reboot stop
```

(cancels any waiting reboot process, no matter if that is a backgrounded process or had been initiated by a different user)

### 9.2.3.48 `make_noise` - Visual and Audio Identification of a Device

#### Purpose

The `make_noise` command allows to identify a device in a server room or rack via beep sounds and periodical blinking (Alarm LED). This is useful if a device needs to be physically identified, for example in a large server room.

The audio-visual signals can be switched off if the device has a display and front panel buttons. In that case the display shows a note saying that the F2 button can be used to stop this mode. It is also possible to cancel the command by pressing CTRL+C, which will also result in stopping the audio-visual identification mode.

#### Call and Parameters

```
# make_noise
```

This command does not support any parameters. It causes the device to beep every 2 seconds and switch the red Alarm LED on and off periodically.

#### Examples

```
# make_noise
```

(initiates the audio-visual identification mode, can be stopped/canceled by pressing CTRL+C or the F2 front panel button of the device)

## 9.2.4 Sync Monitor Status and Configuration via CLI

The configuration of all monitored nodes will be stored in one central ASCII file `/etc/mbg/syncmon.cfg`. Each line will represent the configuration of one node to monitor.

```
# Time Monitoring Node
Configuration
#
@ SourcePort: 33000
@ BaseLogPath: /data
@ BaseCurrDayPath: /data
# Supported Time Protocols: 0:NTP 1:MBG-PTP
# Support ESI Module: Protocol value define the input port
#
# IP4-Address      CPU-Module  Interface  Protocol  Offset-Limit[s]  Stratum  Req-Intv  Log-Intv  Group  Alias  Location
NtpKey   NtpKey
# IPv6 or MAC     NtpKey
Index    Type      (MainCPU=-1)  Name      Index      Domain    Index
-----
addr=172.75.75.3      cpu=08  intf=all   prot=1  offs=0.000001000  domain=7  req=64   log=64   grp=0  alias=Master_TLV  loc=M3000_training_rack
addr=172.75.75.3      cpu=08  intf=all   prot=2  offs=0.000001000  domain=7  req=64   log=64   grp=0  alias=Master_MGMT  loc=M3000_training_rack
addr=172.75.75.1      cpu=08  intf=all   prot=1  offs=0.000001000  domain=7  req=64   log=64   grp=0  alias=Slave1_TLV  loc=M3000_training_rack
addr=172.75.75.1      cpu=08  intf=all   prot=2  offs=0.000001000  domain=7  req=64   log=64   grp=0  alias=Slave1_MGMT  loc=M3000_training_rack
addr=172.27.75.225    cpu=08  intf=all   prot=2  offs=0.000001000  domain=10  req=64   log=64   grp=0  alias=Boundary_Clock_1  loc=training_rack
addr=172.75.75.10     cpu=08  intf=all   prot=1  offs=0.000001000  domain=10  req=8    log=8    grp=0  alias=Slave2_TLV  loc=M500_training
addr=172.75.75.10     cpu=08  intf=all   prot=2  offs=0.000001000  domain=10  req=8    log=8    grp=0  alias=Slave2_MGMT  loc=M500_training
addr=172.27.100.194   cpu=-01  intf=lan0:0  prot=0  offs=0.001000000  strat=10  req=64   log=64   grp=0  alias=NTP_M500_unit  loc=M500_training
kidx=-1
addr=ESI-Module      cpu=10                                prot=1  offs=0.000001000                                req=8    log=8    grp=0  alias=PPS_Slave2  loc=training_rack
```

addr : IP4/6 or MAC address of the node to monitor  
cpu : ID of the IMS card: main cpu=-1 HPS100=0 – 9 ESI IMS card=10-11  
prot : Synchronization Protocol for monitoring: NTP=0 PTP/TLV=1 PTP/Mngt=2  
offs : Offset Limit  
stra : NTP Stratum Limit  
domain : PTP domain  
req : Request Interval [s]  
log : Log-interval [s]  
grp : Group ID  
alias : Alias name defined by user  
loc : location string  
kidx : NTP Key ID ('-1' if not used)  
ktyp : NTP Key Typ (M=MD5 see NTP documentation)  
ksecr : NTP Key Secret (see NTP documentation)

This file can be edited with a text editor directly in the command line of the system or can be replaced by an external prepared file. The monitor program will check this configuration file for changes automatically after every full scan of the configured nodes.



## 9.2.5 Text Editors

Manually modifying a configuration file is an often used task within the CLI environment. LTOS V6 provides two different text editors for this: **nano** and **edit**. Both can be used to edit textfiles, the main difference between them is their feature list and the way the functions are accessed. It is completely up to you which one you choose, it may happen that one of the two offers a better compatibility with your terminal software or that you simply prefer the operating concept of one of them.

On earlier versions of LANTIME OS the nano text editor could be started with the command

```
vi [filename]
```

which is still available on V6 for compatibility reasons. However, this command will show a short note telling you about the two possible editors available on V6 and then asks you to choose which one to use for editing the file *[filename]* you specified on the commandline.

### 9.2.5.1 nano

The nano text editor is a fast, small and easy-to-use opensource program (see <http://www.nano-editor.org/> for further information). This editor has been used as the standard CLI tool for modifying text files in earlier LTOS versions (in which it was started using the vi command).

## Start and Parameters

```
# nano [filename]
```

starts nano and opens the file *[filename]*. If no filename is specified, nano will start with an empty file and will ask for a filename when you use the save/close function afterwards.

## Using the Editor – Main Functions

### Command Keys

The "nano" editor uses key combinations to access its functions. Most key combinations use the control key (CTRL) which has to be held down while pressing and releasing another key to execute a certain editor command.

### Saving Modified Files

In order to save the currently modified file you have to press CTRL+O (for WriteOut). After pressing CTRL+O you will be asked for the filename and path where the changed file should be saved. If you want to overwrite the original file, just press ENTER. You can cancel the save function and return to the editor by pressing CTRL+C.

### Closing the Editor

With CTRL+X the editor can be closed. If there are unsaved changes, you will be asked whether you want to save the changes (press "Y") or not ("N") and you can cancel leaving the editor by pressing CTRL+C at this point.

### Search/Replace

To find a certain search term in the current file, press CTRL+W. If you want to replace a search string, use the CTRL+\ key combination. The nano Editor supports regular expressions as search terms.

### More Functions

A number of additional editor commands and functions can be accessed with specific key combinations. A help screen listing all of them is available with the CTRL+G command key combination.

### 9.2.5.2 edit

The edit text editor is a part of the Midnight Commander opensource project and is normally called mcedit (see <http://www.midnight-commander.org/> for further information). This editor has a rich feature set, a menu system and color options (if supported by the terminal).

## Start and Parameters

# edit [filename]

starts edit and opens the file [filename]. If no filename is specified, the editor will start with an empty file and will ask for a filename when you use the save/close function afterwards.

## Using the Editor – Main Functions

### Function Keys

This editor uses Function Keys to perform most program functions. If your terminal does not support sending the correct key codes for the function keys or if you cannot use the function keys for some other reason, you can emulate a function key by pressing the escape key (ESC) first, followed by the digit 1-9 (for F1 to F9) or 0 (for F10). F10 is important as it is used to quit the editor and return to the CLI prompt.

### Saving Modified Files

In order to save a modified file the F2 key needs to be pressed. This will not leave the editor. After pressing F2 (or ESC+2), a confirmation dialogue appears in which you can enter "S" (save) or "C" (cancel, do not save).

### Closing the Editor

With F10 (or ESC+0) the editor can be closed and you are returned to the CLI prompt. If the currently opened file has been modified and the changes have not been saved yet, the editor will show a dialogue in which you can choose to save the changes and close ("Y"), close with saving any unsaved changes ("N") or cancel and return to the editor ("C").

### Search/Replace

In order to search for a certain search string in the file, please press F7 (ESC+7). If a search string needs to be replaced by another string, press F4 to open the search/replace dialogue. This function has a large number of options which can be selected, for example the "prompt on replace" option to bring up a confirmation dialogue before each replacement is performed or the "replace all" flag to select that multiple/all occurrences of the search string shall be replaced.

### More Functions

The mcedit Editor has a large number of functions and useful features, most of them are accessible via the on screen menu. In order to open the menu, please press F9 (or ESC+9) and then navigate with the cursor keys and ENTER to select a menu option or ESC to leave the menu and return to the file editor.

### 9.2.5.3 vim

The Vimproved text editor ("vim") is a powerful but complex opensource program (see <http://www.vim.org/> for further information). It is not recommended for beginners and requires a lot of training and learning to become useful.

## Start and Parameters

```
# vim [filename]
```

starts vim and opens the file [filename]. If no filename is specified, vim will start with an empty file and requires you to specify a file name later, when you save the file.

## Using the Editor – Main Functions

### Editor Commands and Modes

The "vim" editor is a modal editor and has three basic modes of operation. The "normal mode" is the mode which is active after starting vim from the command line. You can call most editor functions in this mode by pressing a alphanumeric key. Entering the command mode is possible by pressing the colon (":") key. To enter the text edit/insert mode, press "i" for insert or use the Insert key on your keyboard (Ins). You can always return to the "normal mode" by pressing escape (ESC) multiple times.

### Saving Modified Files

Saving the current file is performed in command mode. Enter the command "w" and press ENTER to save the file without leaving the editor. After the save operation has been completed, you will return to normal mode.

### Closing the Editor

To close the editor, use the "q" command in command mode. If there are unsaved changes, you need to use either the "wq" command (to save and exit) or the "q!" command (to exit without saving). In normal mode you can also press "z" twice to save and exit, without having to enter command mode first.

### More Functions

The vim editor is a very powerful text processing editor and offers a large feature set. More about vim and its functions can be found on the Internet. The freely available PDF eBook "The Vim Tutorial and Reference" by Steve Oualline has 800 pages.

## 9.3 Via Front Panel Display

### 9.3.1 LANTIME Display Types

For our LANTIME NTP server, there are four different display types – this is due to the design, housing and by the functionality of the systems. In principle the functionality and menu navigation in all four display types the same. The difference arises from the used receiver system and the available device options.

The high-resolution VF-Display, which is used in our LANTIME M600 systems, also offers a graphical representation of the measured input signals (NTP, PTP, IRIG, PPS ...). The graphic VF-Display is described in the following chapter.

The illustrations of the configuration menus is reacted with a four-line graphics, the menus of the respective systems may differ in the display of it (see Figure 1.0).

```
GPS: NORMAL OPERATION   Mon , dd.mm.yyyy
NTP: Offset PPS:  -4µs   UTC 12:00:00
```

M200 / M300

```
GPS: NORMAL OPERATION
NTP: Offs. PPS: 0µs
Mon. 26.04.2010
UTC: 11:06:32
```

M400 / M900 / IMS-Series

```
07:23:25 UTC
Thu, 30.12.2010
NTP: Offs. PPS: 5µs      Stratum: 1
GPS: NORMAL OPERATION   Satellites: 8/8
PTP2: ok INITIALIZING   GM: 90.....
Press F1 for help or F2 for setup overview
```

M600

```
NORMAL OPERATION
NTP: Offs: -5µs
THU, 26.06.2010
UTC 12:12:00
```

SyncFire

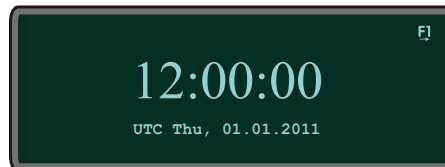
Figure 1.0 - LANTIME Displays

SyncFire	LC-Display, 4 x 20 characters
M200/M300	LC-Display, 2 x 40 characters
M400/M900/IMS	LC-Display, 4 x 16 characters
M600	Vacuum Fluorescent Graphic Display (VFD), 256 x 64 Dots

### 9.3.1.1 Description of the graphical menu: VF-Display

The graphical menu is used to graphically display offset values <sup>1</sup> between a given input signal <sup>2</sup> and the oscillator of a GPS card. The program can be started with the ↑ button in the corresponding status menu. Furthermore, a list of various offsets for the input signals respectively is available in the MRS status function. To access it please press the ↓ button if you are in the main menu (where the current time is displayed).

The main menu of the Lantime (where time and date in the selected time zone are displayed).

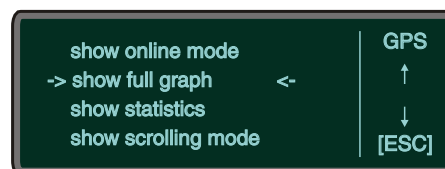


Choose Reference Time ↓, MRS Management, MRS Status and Setup, and eventually MRS Status. Now you can choose whether the numerical offsets of all available input signals should be displayed or if a graphical display program should start. If the graphical option is selected you have to choose one of the input signals as a reference.

By pressing buttons ↑ and ↓ one can change among several reference signals and select one by pressing the OK button. In the graphic mode one can choose among four different display options how the offset of a given reference signal shall be displayed (online mode, full graph, statistics and scrolling mode).

The cursor position and consequently the option selection can be modified with the ↑ and ↓ buttons. In the upper right corner one can find the selected reference source signal, which offset is graphically displayed. With the OK or → button the selected graphical mode can be started.

Main menu of the graphical display with various options:



Each of these modes contains an information menu accessed by F1. One can find here some current status information as well as selection buttons and options of the current mode. With the ESC button one can always return to the menu on the upper level.

<sup>1</sup>Offset: an offset is a time difference between two systems. In our example, the offset is time difference between a given input signal and an oscillator, which disciplines its local clock.

<sup>2</sup>Input signals: GPS, PTP, PPS, NTP, TCR, FRQ- which of these input signals are available can be identified from the numerical status (Numerical Status)

Each graphic mode is displayed within a range of values: <sup>3</sup>

Display of the selected mode (here: SCROLLING MODE)

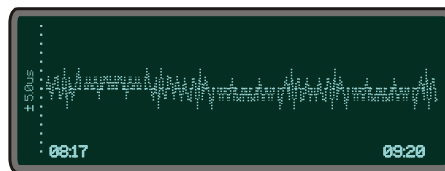


After one of the graphical menu options is selected, the current mode appears for one second on the display. Under the current mode the origin file from which the graphic is generated appears in small fonts.

**The first mode is the “ONLINE MODE“**

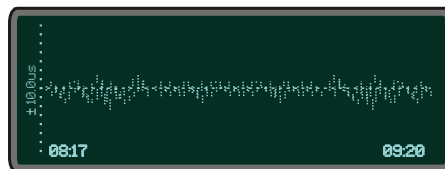
This mode displays the last 255 offset values and it checks regularly for new offsets. When a new value appears the graphic display shifts six pixels to the left to make space for the new values. Additionally, the time range is displayed below and the offset range on the left.

Graph of the Online Mode (not zoomed)



With the ↑ (zoom in) and ↓ (zoom out) buttons the range of the y-axis can be changed any time in order to display graph larger or smaller.

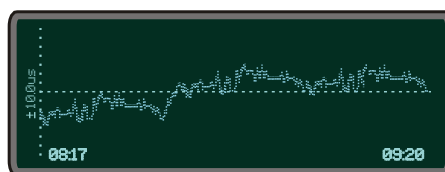
Graph of Online Mode (zoomed out)



**The next mode is the “FULL GRAPHIC MODE“**

After the status mode is displayed, offset values start being plotted. All values from the statistic file are displayed as long as no more than 255 values are available. If more values than a display length (255 points) are available, only each xth offset value <sup>4</sup> is displayed.

Thus a mean value graph is generated which looks similar to this one: An example of a generated graph with the corresponding range of values (here: FULL GRAPHIC)

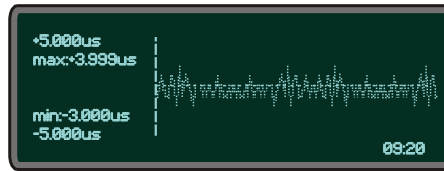


<sup>3</sup>The display has an x and y axis: the y-axis displays the offset value, which is the higher between absolute minimum and maximum value and is computed automatically at the first start of the menu. It is step-wisely ordered as follows: +- 1, 2, 5, 10, 20, ... (in 30 day [d] units – one picosecond [ps]). The x-axis is a time axis. It shows from and until when particular offset values occur.

<sup>4</sup>The xth value is the number of available values divided with the display length.

The range of values is automatically adjusted. The x-axis starts with the first chronological value available in the given file. The last value is not necessarily also the last value from the given file. If more than 255 values are available then only each xth value is displayed.

A legend can be displayed by pressing the F2 button. It contains the value range, as well as the minimum and maximum of the graphic. By pressing a F2 button for the second time the legend disappears.



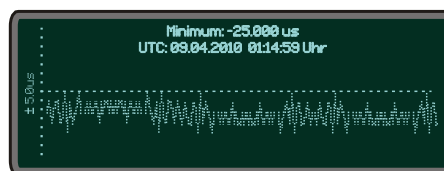
The help menu appears by pressing the F1- information button in the "FULL GRAPHIC MODE". It shows all available options in this mode. Other options are only partially available from here. To end this function one has to press ESC-, OK- or again the F2- button.

In the "FULL GRAPHIC MODE" the graph can be maximized or minimized with ↑ (zoom in) and ↓ (zoom out) buttons. If the legend is currently displayed, selecting the zoom-buttons causes that the range of y-axis gets automatically adjusted and the legend renewed. With the ESC-button one can get back to the main menu of the graphical program where the legend is not displayed. Alternatively, a display returns back to a "FULL GRAPHIC MODE" with a default value range.

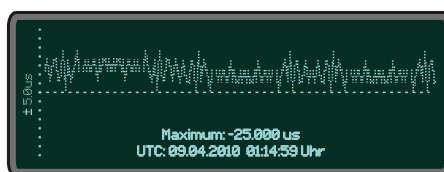
The „Statistic“ - option comes next in the graphic menu. When you select it, you can decide if the minimum or the maximum value of the current statistics file shall be displayed or not.

The minimum or the maximum values are plotted in the middle of a display, as long as at least 128 values (a half of the display length) are available. A legend is shown on the display at the same time and apart of the minimum or maximum value also the corresponding UTC time is displayed <sup>5</sup>.

Display of the minimum including the legend:



Display of the maximum including the legend:

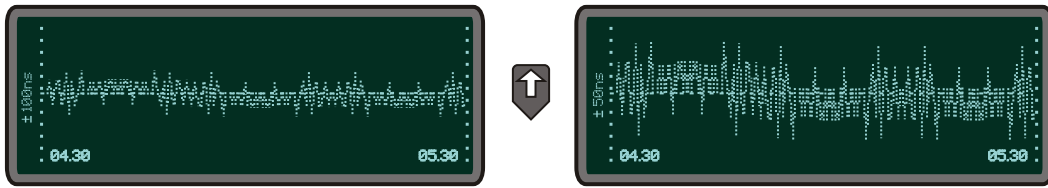


**The "SCROLLING MODE" comes as last in the graphical mode**

After the status mode is displayed the whole available offsets are shown in a scrolling way. The ↑ or ↓ buttons refer in the „SCROLLING MODE“ to its scaled up or scaled down range of values of the y-axis. Each time when selecting these two buttons the „SCROLLING MODE“ starts again from the beginning. Pressing the OK or ← button causes that the graphic holds on; and pressing the OK or → again the graph continues to scroll on. When the mode is stopped (the value range will be displayed) one can change the y-axis value range with the ↑ (scaled up) and ↓ (scaled down) buttons. The offset values will only be scrolled to the end of a display

<sup>5</sup>UTC: Universal Time Coordinated is the standardized world time which does not include daylight saving time change

and again with the OK or → button the scrolling will continue.



When the ← button is selected the displayed graph moves half of a display to the left if the „SCROLLING MODE“ has not been stopped beforehand. Even here the value range of the y-axis can be changed or the graph can be shifted a few more steps to the left. In order to continue the scrolling mode one has to press the OK or → button. If you select the ESC button then you come back to the main menu of the graphical program.



### 9.3.2 Front Display - Root Menu

The root menu is shown when the receiver has completed initialization after power-up. With the four arrow buttons and the buttons „OK“, „ESC“, „F1“ and „F2“ the navigation and setting of parameters can be managed. Main menu can be reached by holding „ESC“ for a few seconds. The main menu reflect some of the main parameters of the time server. First line shows the name of the device and the status of the reference clock. The text "NORMAL MODE" might be replaced by "NOT SYNC". If a existing antenna connection is interrupted or not working properly, the text "ANTENNA FAULTY" is displayed instead.

With an integrated time code receiver it might be possible, that the message "NO DATA" appears on the display - in this case the correct value can be set in the time-code parameter submenu.

Current time and date of the timeserver with the name of the time zone (NTP uses UTC time zone) will be monitored in the bottom line. If the "SIMULATION MODE" option is enabled an "\*" will be shown behind the time.

**The multicolor LEDs will reflect the current state of the device:**

#### „Ref. Time“

green: the reference clock produce valid time.

red: the reference clock produce no valid time (e.g. not synchronized)

#### „Time Service“

green: NTP has been synchronized to reference clock.

red: NTP is not synchronous to reference clock or sync to „local clock“

#### „Network“

green: all watched network ports has been "link up" detected

red: at least one of the watched network ports (look at „Setup Device Parameter / Check Network Linkup“) is not connected

#### „Alarm“

off: no error at moment

red: general error – more information will be shown on display.

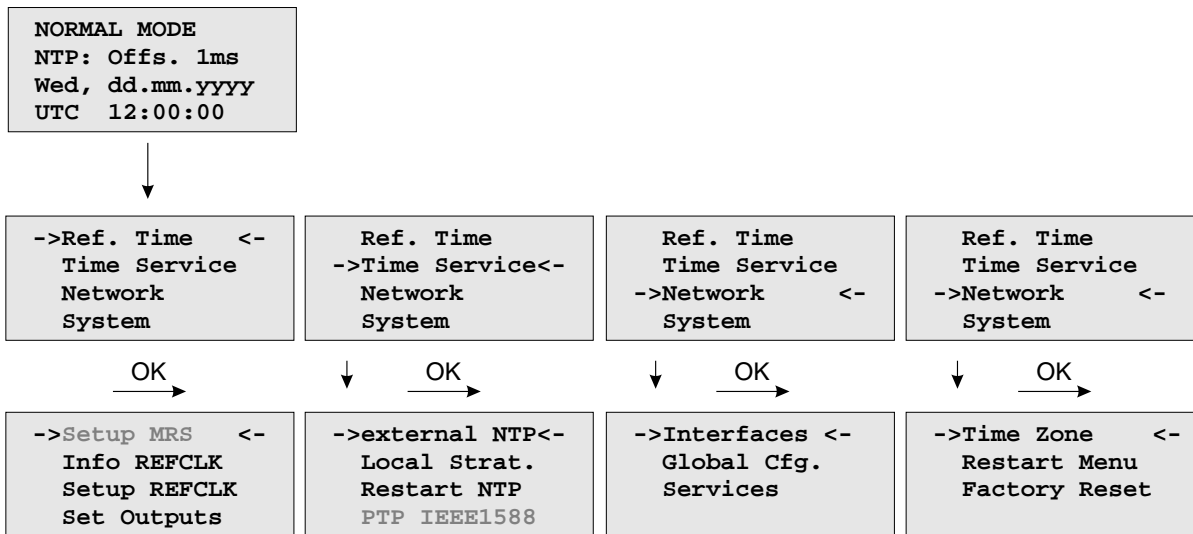
If the symbol „F1“ will be shown in the upper right corner a help page can be displayed when pressing the „F1“ button. When pressing „F1“ from main menu a short description for menu navigation will be displayed:

Use → and ← to  
select different  
main menus. Use  
↑ and ↓ to enter.

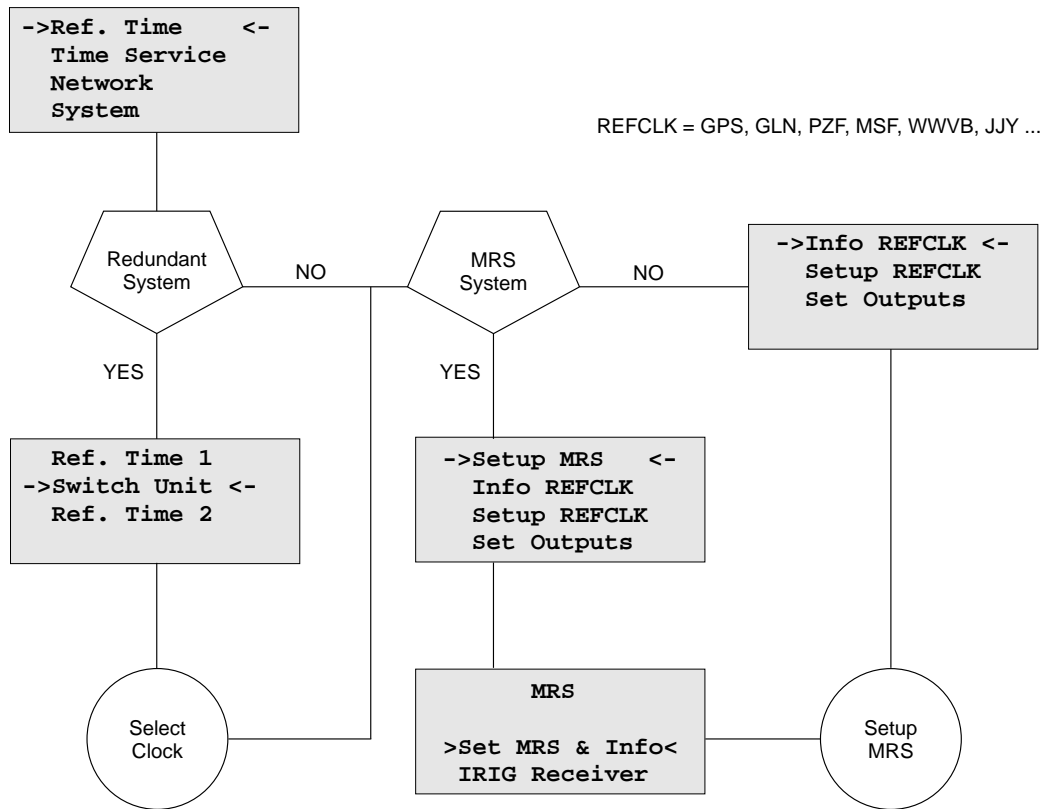
When pressing the „OK“ button from main menu the version of the LANTIME software, the NTP and the LINUX kernel version will be displayed.

ELX800      VX.XXx  
SN: 000000000000  
NTP: X.X.Xx@X.X  
Krn.: X.X.XX.X

The following main menus will be displayed when pressing the arrow buttons:

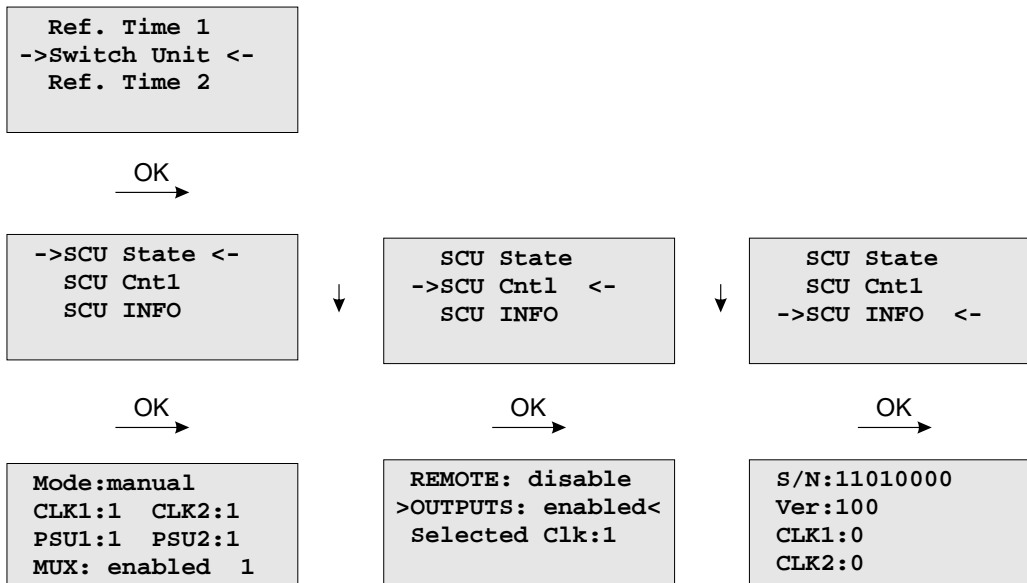


### 9.3.3 Menu: Reference Time



The Reference Clock menu and all its sub menus will manage all status information and parameters of the reference clock. To enter the following sub menus press the "OK" button.

## 9.3.3.1 Optional Menu Switch Unit



With this menu you can check all important status information about the switch card unit. The example above shows a perfect mode of operation. Both power supplies (PSU1, PSU2) are connected - the two receivers are working in "normal operation mode" (CLK1, CLK2). If the second clock is not connected or in free running mode, the display shows "CLK2:0". If there is no power connected on PSU1, you can see the status "PSU1:0" on the display of the LANTIME.

With the submenu **SCU Cntl** you can configure the following parameters:

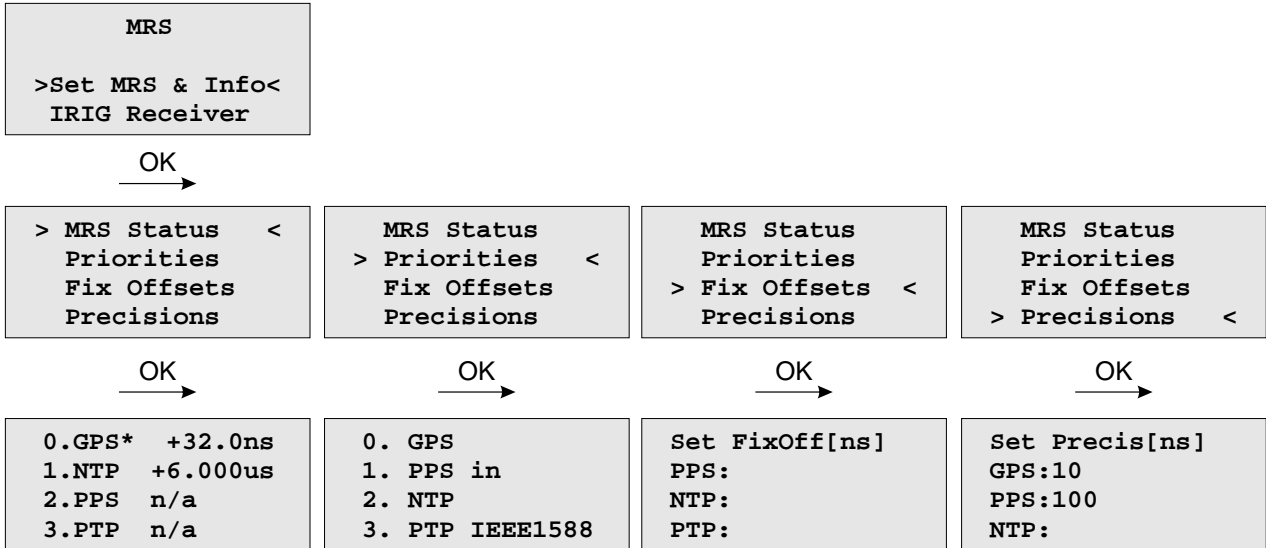
**REMOTE:** disabled/enabled  
disable or enable remote control of the SCU

**OUTPUTS:** enabled/disabled  
disable or enable outputs of the SCU

**Selected Clk:** Clk:1, Clk:2  
The reference clock can be selected with the function keys or from a connected workstation - for this the mechanical switch in front of the SCU card must be locked in position "Auto". Otherwise (position "Manual") the selected clock can only be changed by using the switch of the SCU.

### 9.3.3.2 Menu Option Setup MRS

The internal reference clock of the integrated clock module with the high precision oscillator (OCXO HQ) can be disciplined by different time sources. Possible time sources are GPS receiver, external Pulse Per Second (PPS), IRIG 10MHz Frequency, IRIG Time Code, external NTP server or IEEE1588 Grandmaster (M400, M600, M900). The priorities for the internal controlling can be set up in configuration. The priority will define which reference source will be used next if the highest priority reference source will be no longer available. For each reference source a bias (fixed offset) and a precision value can be defined.



With the OK and arrow buttons you can choose the current status of the MRS. All possible reference clocks will be shown with the number of priority, the name of the reference clock and the current offset to the internal reference clock (OCXO). The current master will be signed with an "\*" behind the name of the reference clock.

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.

The "Fixed Offsets" can be set up in the next sub menu, if you know the constant offset (bias) of an external reference source. 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.

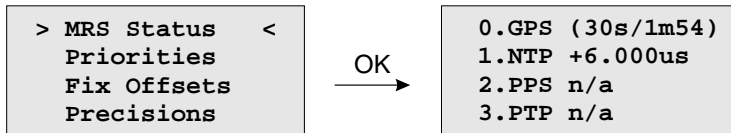
This precision value will determine the hold over time when switching to the next reference clock if the current master is not available anymore. If the precision is 0 the next reference clock will be switched at once. If the precision value is greater than 0 the time for switching to the next reference (hold over time) will be calculated by the following formula:

$$(\text{precision of next reference}) / (\text{precision of current master}) * \text{constant [s]}$$

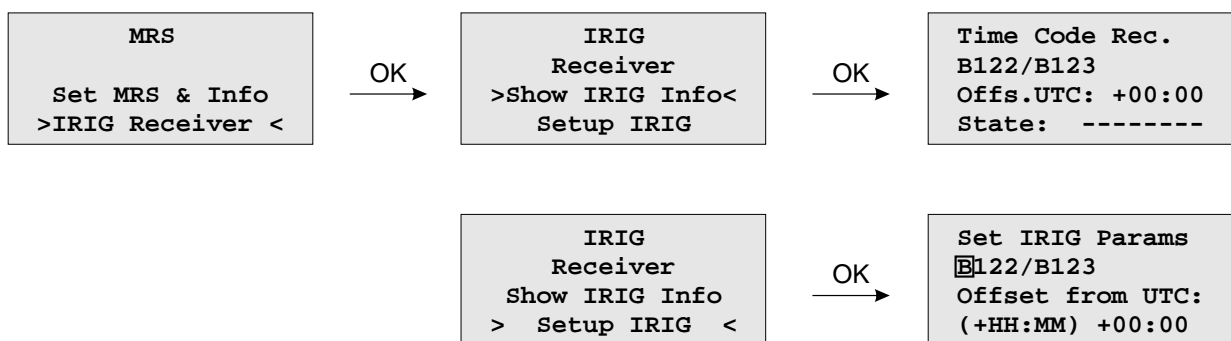
The parameter „constant“ depends on the quality of the internal oscillator.

**Example:**

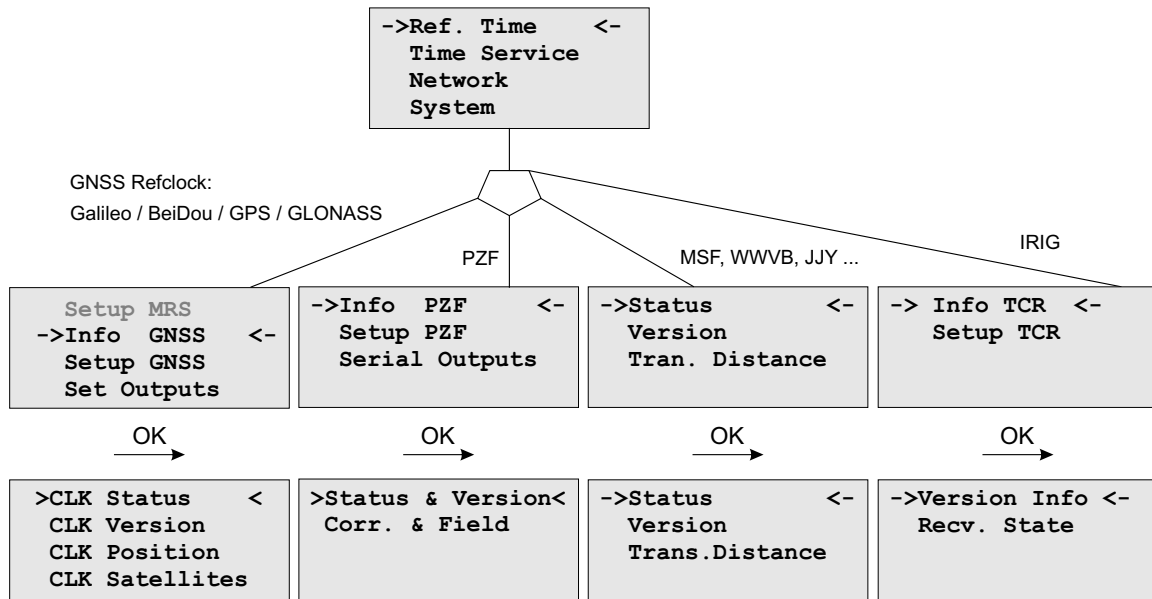
The GPS receiver with an precision of 10ns is the current master. If this master is no longer available it will switch to the next reference source of the priority order – in this case the PPS input with a precision of 100us. With the formula  $((100\text{ns}/10\text{ns}) * 11.4)$  we get hold over time of 114 seconds/1.9 min. 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.

**9.3.3.3 Menu Option MRS - Setup Time Code Receiver**

With this menu, the parameters for the time code input signals can be displayed and adjusted.



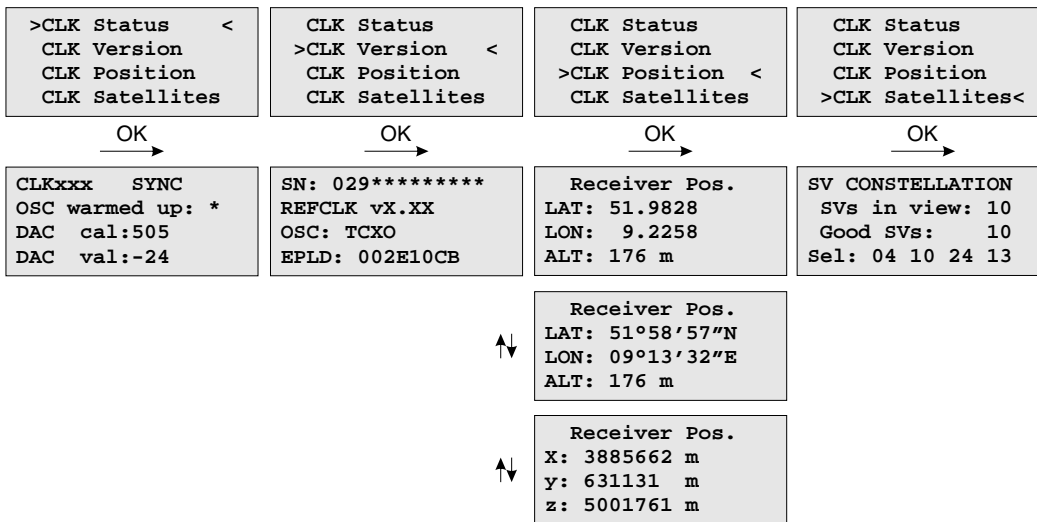
9.3.3.4 Menu: Info Receiver



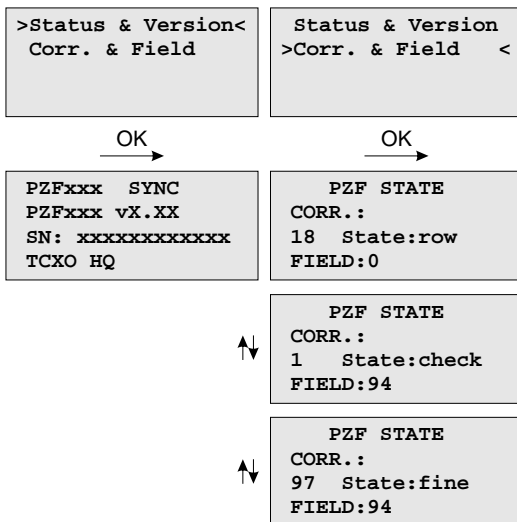
In this menu all relevant information about the reference clock, the internal oscillator and in case of a GNSS receiver, the visible and good satellites will be shown in the display.

### 9.3.3.5 Receiver Status and Version

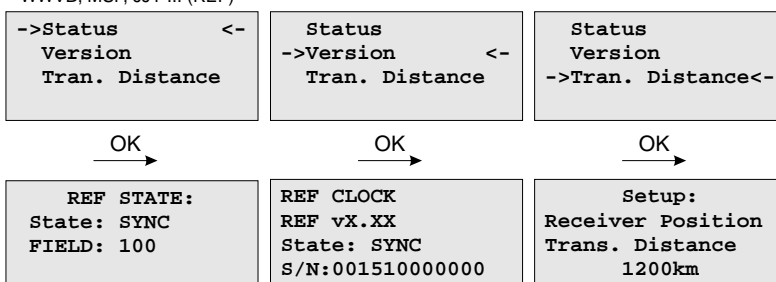
GPS / GLONASS (CLK)



PZF



WWVB, MSF, JYJ ... (REF)

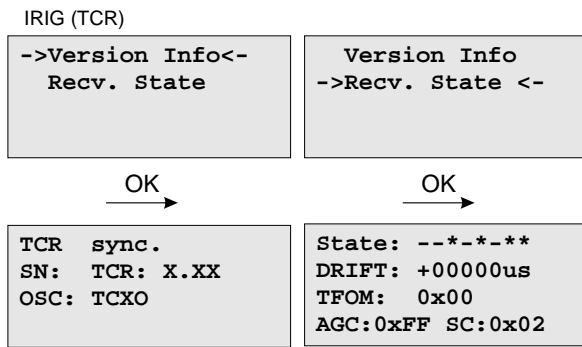


This first menu will monitor the current state („sync“ or „not sync“). The next line will reflect the firmware version, the serial number of the internal GPS and the type of the integrated oscillator.

### 9.3.3.6 Menu: IRIG Receiver State

The first line of the display shows the system state with 8 options – described in the next paragraph. The second line will display the drift in [us] of the internal oscillator and the TFOM value (Time Figure Of Merit: the quality of the IRIG-signal, only used with IEEE 1344) and the current system configuration is shown on the third line. On the fourth line the AGC (Automatic Gain Control of the input signal) value in hexadecimal will be shown.





### IRIG Receiver State: Bit 7 ... 0

Bit 7: Invalid UTC parameter  
 Bit 6: TCAP exceeded, jitter out of range  
 Bit 5: Lock on  
 Bit 4: Telegramm error  
 Bit 3: Data available  
 Bit 2: Invalid sysconf  
 Bit 1: Pulses enabled  
 Bit 0: Warmed up

**Invalid UTC parameter:** This bit is set to one if the checksum of the 'Offset from UTC' parameter, which must be used if no IEEE1344 extensions are available, is invalid. User must enter new 'Offset from UTC' data to clear this bit. Please note that the IRIG-receiver never leaves freewheeling mode if IEEE1344 is disabled and the UTC-Parameter are invalid!

**TCAP exceeded, jitter out of range:** If the jitter between two consecutive IRIG-telegrams exceeds +/- 100us the receiver switches into freewheeling mode and the 'TCAP exceeded' Bit is set. 'TCAP exceeded' is cleared if the measured jitter is below +/- 100us.

**Lock on:** 'Lock On' is set whenever the receiver is in synchronous mode and the internal oscillator correction value has settled.

**Telegram error:** This bit is set if the consistency check of two consecutive IRIG-telegrams fails. The IRIG-receiver switches into free wheling mode if 'telegram error' is set.

**Data available:** 'data available' is set if the receiver can read the timecode.

**Invalid sysconf:** If 'invalid sysconf' is set the checksum of the system configuration data is invalid. In this case the default mode 'IEEE1344 disabled' is selected. User must cycle the system or enter a new system configuration in the IRIG-parameter menu.

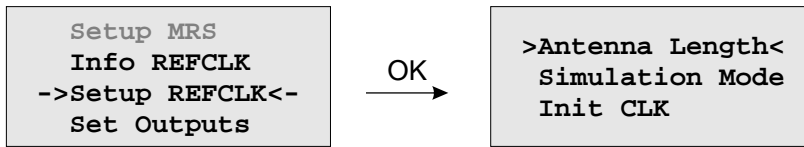
**Pulses enabled:** The pulse per second (PPS) signal which increases the NTP's accuracy is turned when 'lock on' is set the first time. The 'pulses enabled' bit is set if the PPS signal is enabled.

### IRIG system configuration Bit 2 ... 0

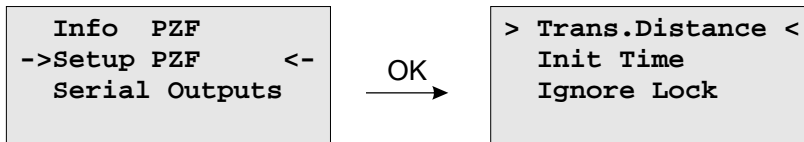
Bit 7 ... 4: reserved  
 Bit 3: ignore Day Of Year enabled  
 Bit 2: ignore TFOM  
 Bit 1: ignore SYNC  
 Bit 0: IEEE 1344 enabled

## 9.3.3.7 Menu: Setup Meinberg Receiver

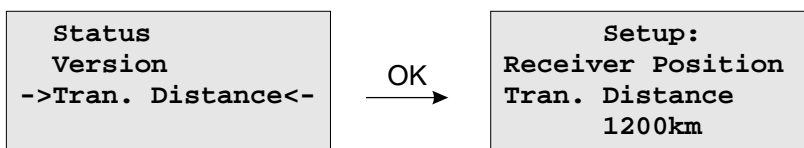
GPS / GLONASS (CLK)



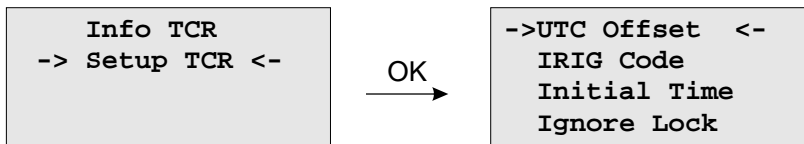
PZF



WWVB, MSF, JJY ...



IRIG



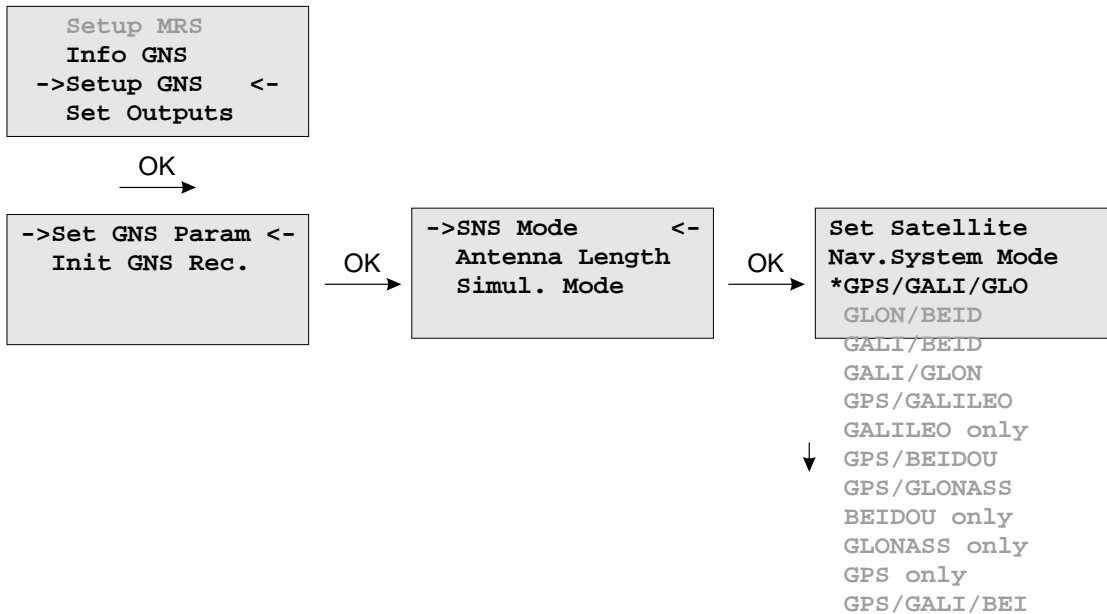
In the Reference Time -> Setup Clock menu the receiver clock parameters can be configured. The antenna cable length of satellite based receivers must be entered here. The GPS and GLONASS reference clocks can be run in simulation mode.

Meinberg's PZF correlation receivers can be operated in simulation mode as well. In addition to that, the distance to the transmitter must be set in the setup menu.

For our long wave receivers (WWVB, MSF, JJY ...) there is only the setting for "Transmitter Distance" available - in the Submenu *Reference Time* -> *Info Refclock*. The setup for our IRIG time code receivers includes the settings for the UTC offset and the corresponding time code. The time code receiver can also operate in simulation mode with **IGNORE LOCK**. With **Initial Time** and **Init Clock** (GPS, GLONASS), the time and date for the simulation mode is set.

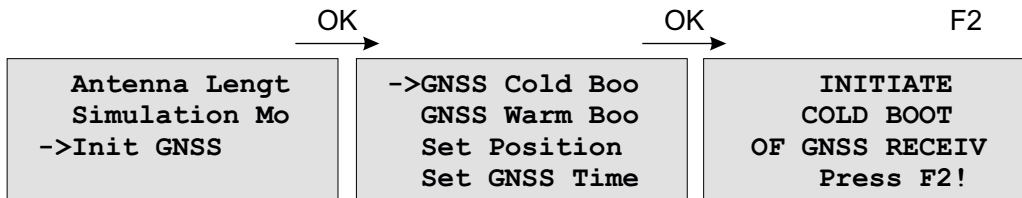
### 9.3.3.8 SNS Mode - Satellite Navigation System Mode

If you are using a GNS receiver (GNS or GNS-UC with Up Converter), this drop-down menu allows you to select one or more satellite systems to be used simultaneously. The following combinations are available:



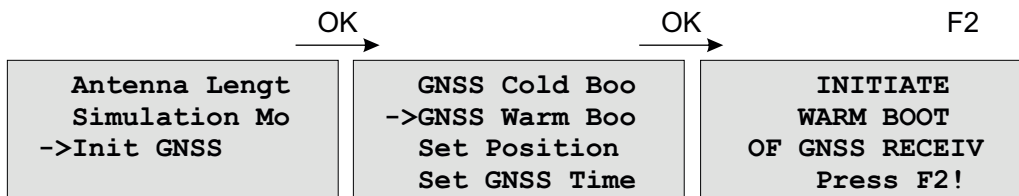
### 9.3.3.9 Initiate Cold Boot

This menu lets the user initialize all GNSS data, i.e. all saved satellite data will be cleared. The user has to acknowledge this menu again before the initialisation starts. The system starts operating in the COLD BOOT mode and seeks for a satellite to read its actual parameters.



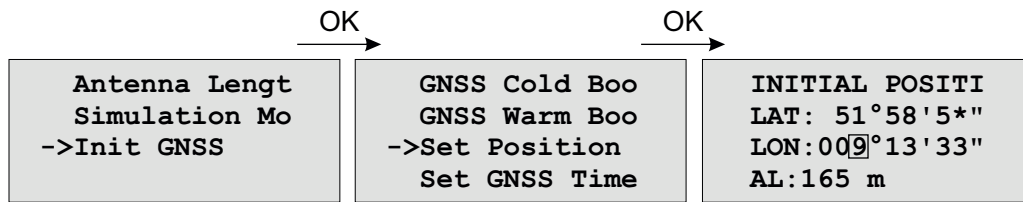
### 9.3.3.10 Initiate Warm Boot

This menu lets the user force the receiver into the Warm 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.



### 9.3.3.11 Init Receiver Position

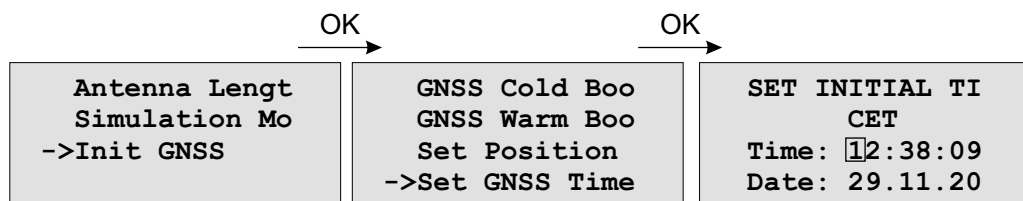
When the receiver is primarily installed at a new location far away from the last position saved in the receiver's memory the satellites in view and their doppler will differ so much from those expected due to the wrong position that the GNSS receiver has to scan for satellites in Warm Boot mode. Making the new approximately known position available to the receiver can avoid Warm Boot and speed up installation.



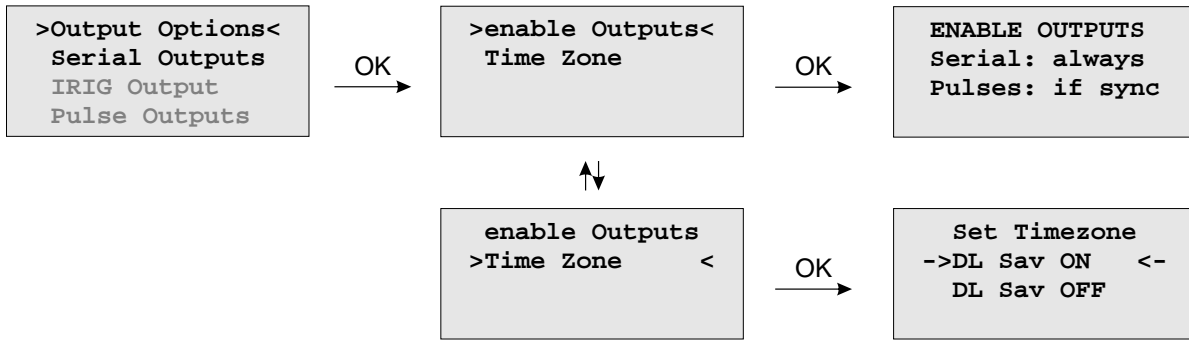
### 9.3.3.12 Init Receiver Time

If the receiver's on-board real time clock keeps a wrong time the receiver is unable to compute the satellites' correct elevation angles and Doppler. This submenu enables the user to change the receiver's system time for initialisation. After the receiver has locked, its real time clock will be adjusted using the information from the satellites.

When the antenna is disconnected it is possible to set the system with any time. Note that the NTP will not synchronize to GNSS losing its reception or if the deviation to the system time is larger than 1024 seconds. In this case the menu **Simulation Mode** has to be active. After setting the clock manually the system time will be set and the NTP will be restarted.



### 9.3.3.13 Menu: Output Options



#### Enable Outputs:

The submenu *Output Options* -> *Enable Outputs* lets the user configure at which time after power up the serial ports and pulse/frequency outputs are to be enabled. Outputs which are shown to be enabled 'always' will be enabled immediately after power-up. Outputs which are shown to be enabled 'if Sync' will be enabled after the receiver has decoded the incoming signals and has checked or corrected its on-board clock. The default setting for all outputs is 'if Sync'.

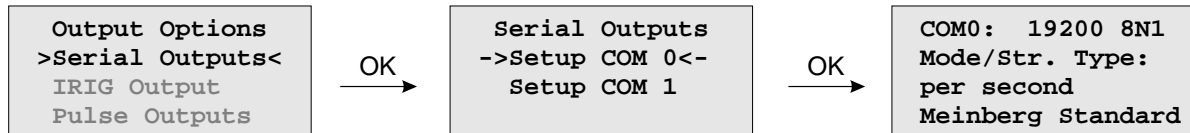
#### Time Zone:

See Chapter "Set Time Zone of Serial Outputs".

### 9.3.3.14 Menu: Serial Outputs

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

**Baudrate:** 300 to 19200  
**Dataformat:** 7E1, 7E2, 7N2, 7O1, 7O2, 8E1, 8E2, 8N1, 8N2, 8O1



COM0 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 timestring.

Defaultsettings COM0:	Speed	Framing	Mode	Signal Type
	19200 baud	8N1	per second	Meinberg Standard

This topic is used to select one of several different types of serial time strings or the capture string for each serial port.

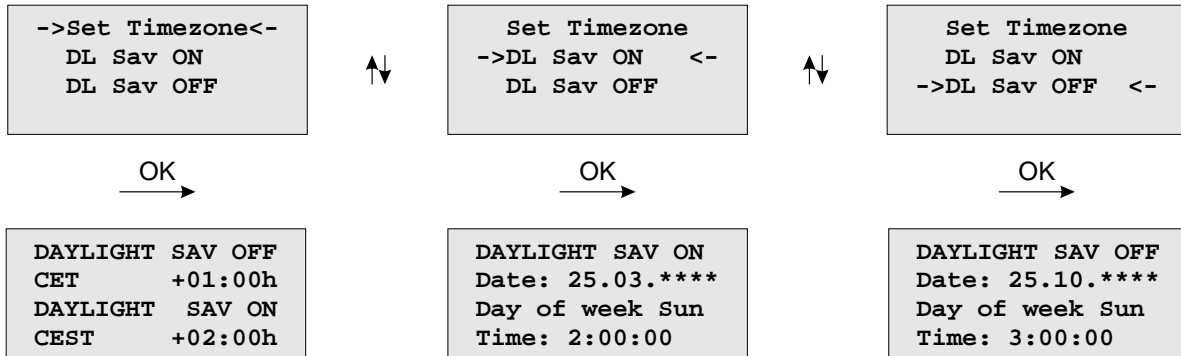
The following time strings can be selected. All time strings are described in the appendix at the end of this documentation.

- Meinberg Standard
- SAT
- NMEA RMC (Rev. 2.2)
- Uni Erlangen
- Computime
- Sysplex 1
- Meinberg Capture
- SPA
- RACAL
- Meinberg GPS
- NMEA GGA (Rev. 2.2)
- NMEA RMC GGA (Rev. 2.2)
- NMEA ZDA (Rev. 2.2)
- ION
- 6021
- IRIG-J

### 9.3.3.15 Setup Output Time Zone

The time zone of the internal receiver can be set up. These parameters will affect the serial output lines and the timecode (IRIG) outputs. The internal time zone of the timeserver and the time of NTP will always be UTC. The time monitored in the main menu will be the time of the NTP.

The menu *Set Timezone* lets the user enter the names of the local time zone with daylight saving disabled and enabled, together with the zones time offsets from UTC. These parameters are used to convert UTC to local time, e.g. CET = UTC + 1h and CEST = UTC + 2h for central Europe. The values of daylight saving are configurable using the Time Zone setup menu.



Beginning and ending of daylight saving may either be defined by exact dates for a single year or using an algorithm which allows the receiver to re-compute the effective dates year by year. The figure shows how to enter parameters for the automatic mode. If the number of the year is displayed as wildcards '\*\*\*\*', a day-of-week must be specified. Then, starting from the configured date, daylight saving changes the first day which matches the configured day-of-week. In the figure October 25th is a Saturday, so the next Sunday is October 26th.

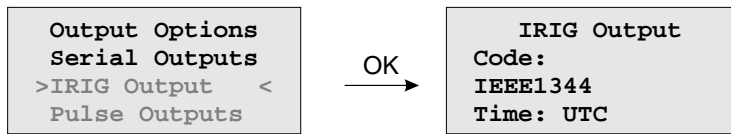
All changeover rules for the daylight saving like "the first/the second/the second to last/the last Sunday/-Monday etc. in the x-th month," can be described by the used format "first specified day-of-week after a defined date".

If the number of the year is not displayed as wildcards the complete date exactly determines the day daylight saving has to change, so the day-of-week does not need to be specified.

If no changeover in daylight saving is wanted, identical dates and times must be entered in both of the submenus (DAYLIGHT SAV ON/OFF). After this a restart should be done.

### 9.3.3.16 Menu: Setup Time Code

The IRIG Time Code is an optional output.



This menu lets the user select the Timecodes to be generated by internal reference clock. Most IRIG-Codes do not carry any time zone information, hence UTC is selected for output by default. If desired, the clocks local time can be output by selecting "TIME: Local".

The following codes can be selected:

- IRIG B002+B122
- IRIG B006+B126
- IRIG B007+B127
- AFNOR NF S87-500
- C37.M8
- IEEE1344

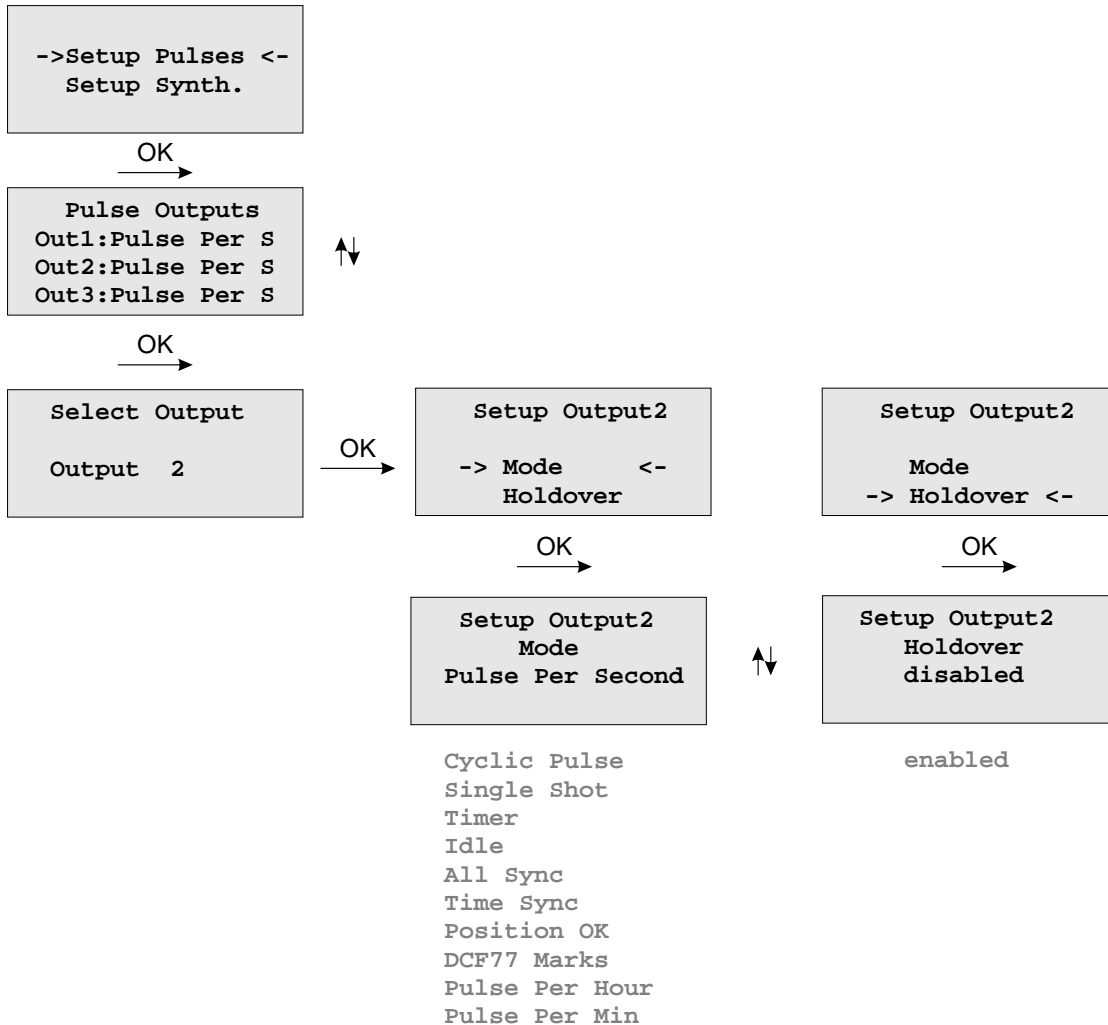
Refer to chapter **Timecode** for details.



### 9.3.3.17 Option: Setup Progr. Pulses

#### Timer Mode

This mode simulates a programmable day assigned timer. Three turn-off and turn-on times are programmable for each output. If you want to program a switchover, change the turn-on time "On" and the corresponding turn-off time "Off". A turn-on time later than the turn-off time would cause a switch program running over midnight. For example a program "On"10.45.00, "Off" 9.30.00 would cause an active output from 10.45 to 9.30 (the next day!). If one or more of the three switching times are unused just enter the same time into the values "On" and "Off". In this case the switch time does not affect the output.



As already mentioned, the outputs home position is selected by "active: high or low".

#### Cyclic Pulse mode - generating of periodically repeated pulses

The value of "Time" determines the time between two consecutive pulses. This cycle time must be entered as hours, minutes and seconds. The pulse train is synchronized at 0:00 o'clock local time, so the first pulse of a day always occurs at midnight. A cycle time of 2 seconds for example, would cause pulses at 0:00:00, 0:00:02, 0:00:04 etc. Basically it is possible to enter any cycle time between 0 and 24 hours, however usually a cycle times that cause a constant distance between all consecutive pulses make sense.

For example: a cycle time of 1 hour 45 minutes would cause a pulse every 6300 seconds (starting from 0 o'clock). The appearing distance between the last pulse of a day and the first pulse of the next day (0:00:00 o'clock) would be only 4500 sec. The value in entry field "Cycle" turns red, when entering a time that causes this asymmetry.

#### DCF77 Marks

In "DCF77 Marks" mode the selected output simulates the telegram as transmitted by german time code transmitter DCF77. The generated time code is related to the local time zone. If you want DCF simulation to be disabled when the clock is in free running mode, you can enter the delay (given in minutes) for deactivat-

ing the DCF-Simulation with the "Timeout" value. DCF Simulation is never suspended, if the delay value is zero.

#### **Single Shot Modus**

Selecting Single Shot generates a single pulse of defined length once per day. You can enter the time when the pulse is generated with the "Time" value. The value "Length" determines the pulse length. The pulse length can vary from 10 msec to 10 sec in steps of 10 msec.

#### **Pulses Per Second, Per Min, Per Hour Modes**

These modes generate pulses of defined length once per second, once per minute or once per hour. "Length" determines the pulse length (10 msec...10 sec).

#### **Position OK, Time Sync and All Sync**

Three different modes are selectable for output of the clocks synchronization state. The Mode 'Position OK' activates the output when the receiver has sufficient satellites in view to calculate its position. In "Time Sync" mode the respective output is activated when the clocks internal timebase is synchronized to the GPS timing. The "All Sync" Mode performs a logical AND operation of the both states previously mentioned, i.e. the output is activated if the position can be calculated AND the internal timebase is synchronized to the GPS timing

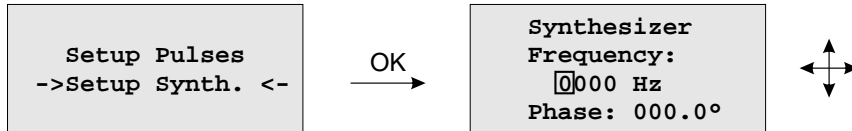
#### **Idle Mode**

Selecting "Idle" deactivates the output.

#### **Holdover**

If "enabled" is selected the operation of the output remains. Otherwise ("disabled") the operation of the output will be switched off when synchronization is lost.

### 9.3.3.18 Option: Synthesizer Frequency Output

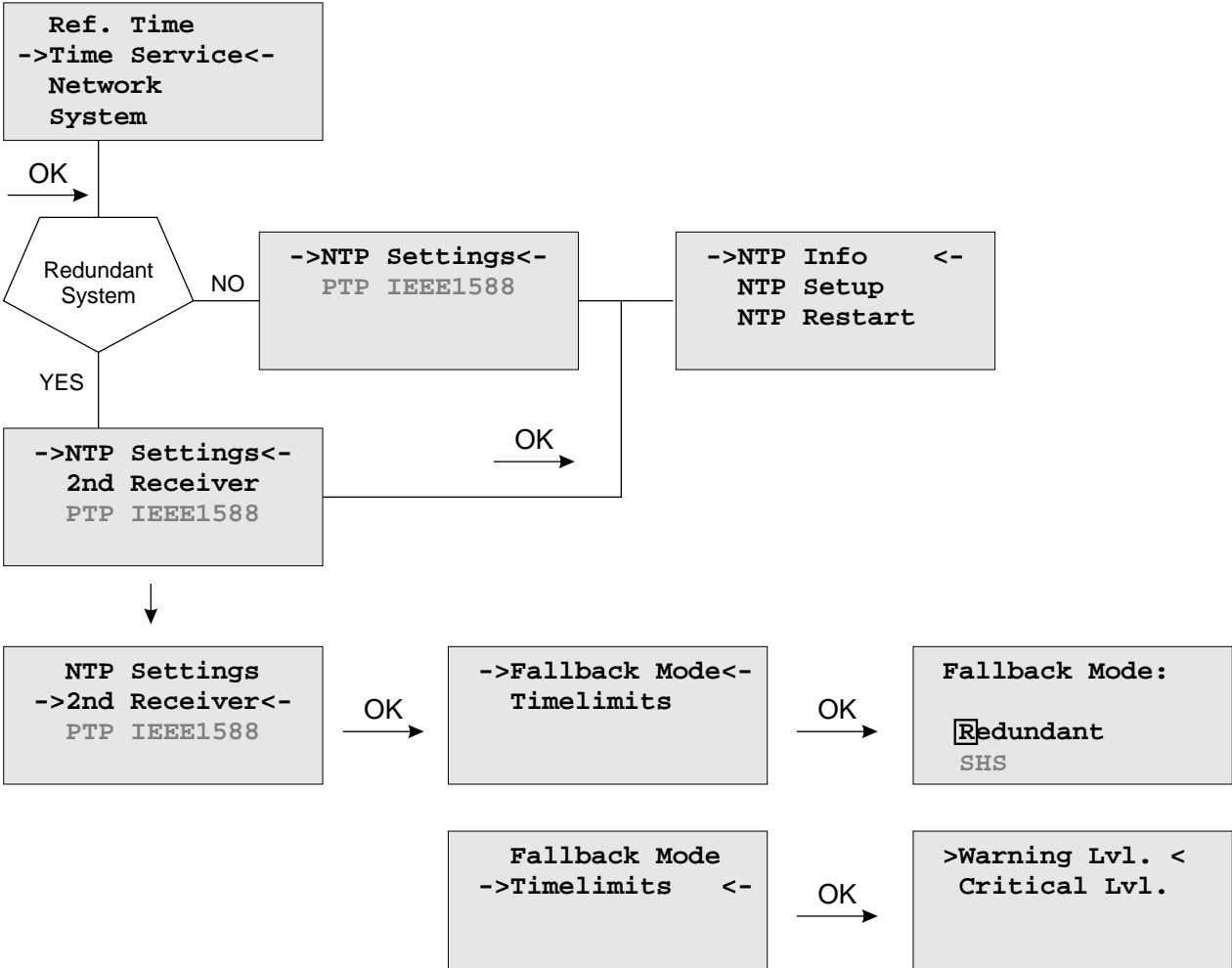


This setup menu lets the user edit the frequency and phase to be generated by the on-board synthesizer. Frequencies from 1/8 Hz up to 10 MHz can be entered using four digits and a range. The range can be selected if the „UP“ or „DOWN“ key is pressed while the cursor is positioned on the frequency's units string. If the least significant range has been selected valid fractions of the frequency are .0, .1 (displayed as 1/8), .3 (displayed as 1/3), .5 and .6 (displayed as 2/3). Selection of 1/3 or 2/3 means real 1/3 or 2/3 Hz, not 0.33 or 0.66. If frequency is set to 0 the synthesizer is disabled.

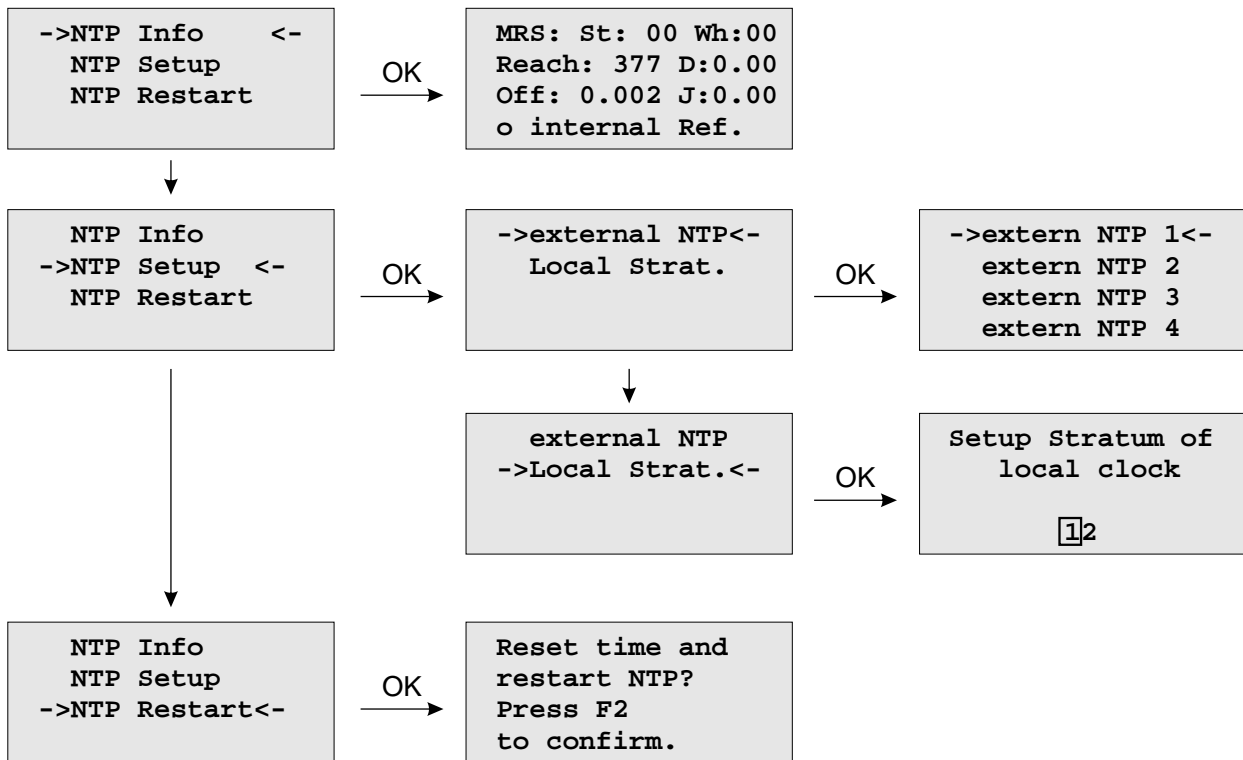
The last line of the display lets the user enter the phase of the generated frequency from  $-360^\circ$  to  $+360^\circ$  with a resolution of  $0.1^\circ$ . Increasing the phase lets the signal come out later. Phase affects frequencies less than 10.00 kHz only, if a higher frequency is selected a message "(phase ignored)" informs the user that the phase value is ignored.

### 9.3.4 Menu: Time Service

The NTP configuration page is used to set up the additional NTP parameters needed for a more specific configuration of the NTP subsystem. The optional available PTP adjustments can be done with this menu.



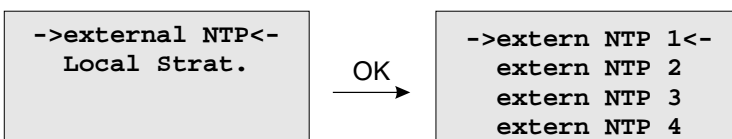
### 9.3.4.1 Menu NTP



### 9.3.4.2 Menu: external NTP

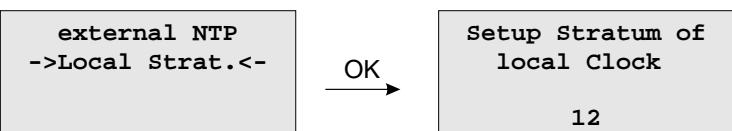
Additional external NTP servers can be set up to provide a high grade of redundancy for the internal reference clock.

The internal reference clock always has priority over the external NTP servers. If the internal reference clock is not synchronized or has failed, the NTP will automatically switch to an external NTP server. With this menu item some external NTP server can be configured.



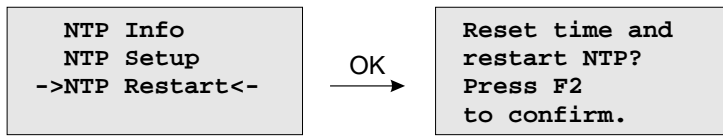
### 9.3.4.3 Menu: Stratum of local clock

The local clock is only chosen as the NTP time reference after the reference clock lost its synchronisation. The stratum level of the 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 anymore when the reference clock is out of order. The field "Stratum of local clock" is used to change the stratum level of the local clock, default value is 12.

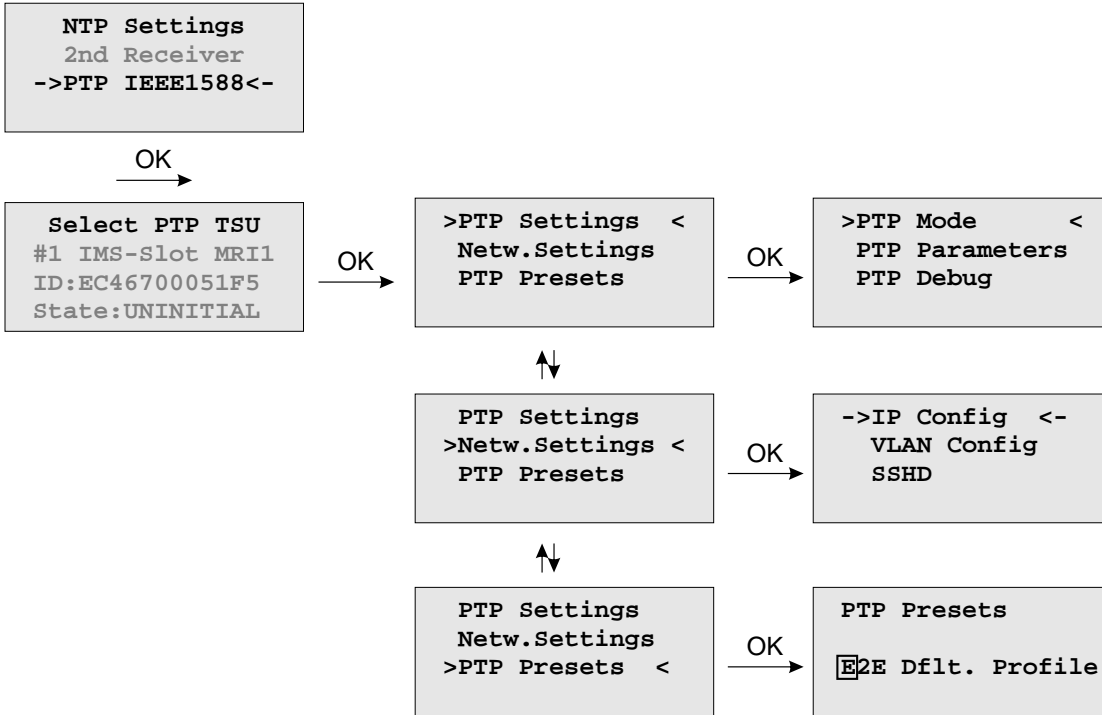


### 9.3.4.4 Menu: Restart NTP

The system time is setup, together with the reference time and the NTP service is rebooting.

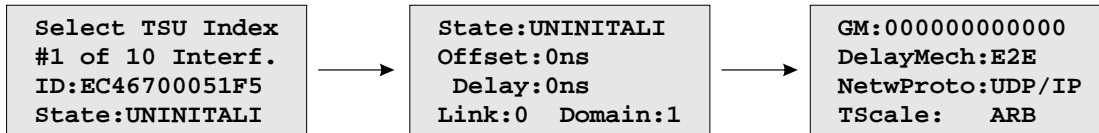


9.3.4.5 Option: Menu PTPv2 - IEEE 1588-2008



The menu for PTP IEEE 1588 configuration is located in the "Time Service" main menu. A device with more than one PTPv2 cards (also called TSU - Time Stamp Units) lists all cards in the sub menu which follows. With ↓ and ↑ buttons one can select among different PTP cards available in the system. A slot number, MAC address and the current state of the selected TSU will be displayed.

### 9.3.4.6 Menu TSU Info



The page "TSU Info" gives an overview of the state of the most important PTP parameters from the time stamp unit which is connected to the PTP0 interface. The appearance of this page is depending on the mode of the PTP engine. There are different states of a TSU possible. For example, if the unit is configured as a PTP Grandmaster clock, then this page shows the "Master" state. On the other hand in MRS (Multi Reference Source) devices, the PTP mode "Slave" is displayed here.

The full list of **TSU States** is as follows:

- uninitialized:* The port is booting up, the software daemon has not yet started, the IP address is not yet assigned.
- initializing:* In this state the port initializes its data sets, hardware, and communication facilities.
- faulty:* Not defined in LANTIME systems.
- disabled:* PTP service has been disabled on this port, either by user configuration or because the module is in a standby mode.
- listening:* The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.
- preMaster:* A short transitional state while the port is becoming a master.
- master:* The port is a current master.
- passive:* The port is in passive mode, meaning there is another master clock active in the PTP domain. The port can enter master state when it wins the BMCA (Best Master Clock Algorithm) due to a failure/service degradation of the current master.
- uncalibrated:* One or more master ports have been detected in the same domain. The TSU is waiting to calculate the path delay to a Grandmaster.
- slave:* The port has successfully subscribed to a master and receives all expected messages. It also successfully measured the path delay using delay request messages.

#### Values **Offset** and **Delay**

"Master" state: 0 ns since they refer to its internal clock.

"Slave" state: they show the offset to the Grandmaster and the mean network delay between the master and a slave.

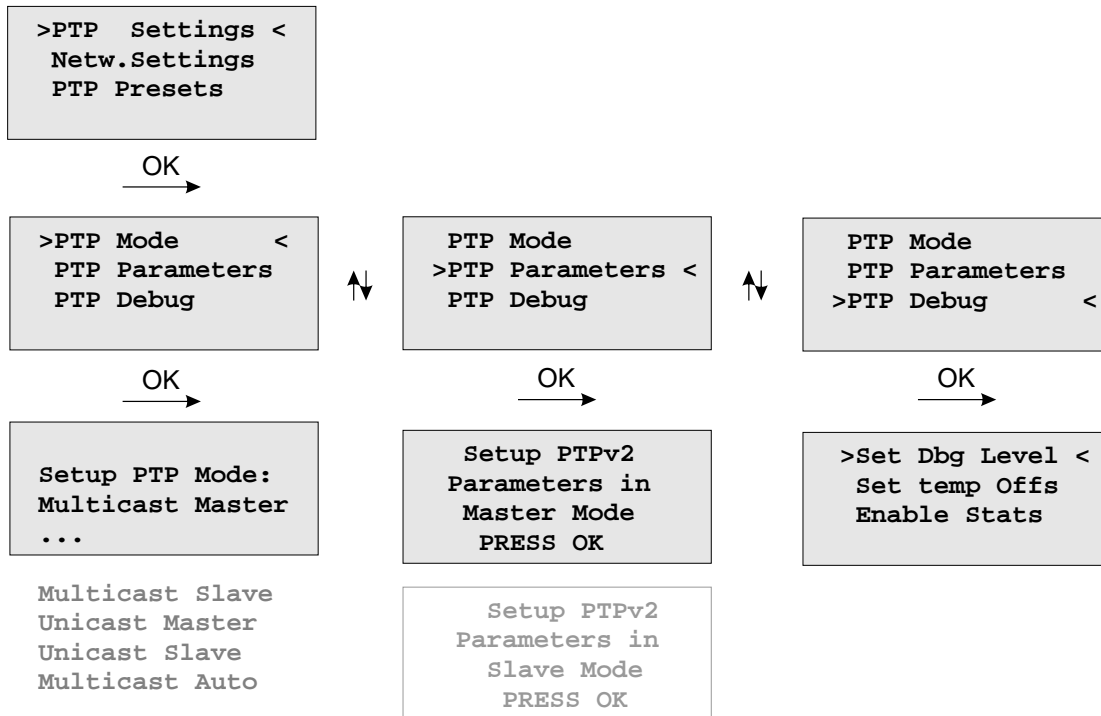
**Link:** status 0: The queried port is down, check the link LED. If faulty, replace the network card.  
status 1: The port of interest is in normal operation.



- Domain:** A PTP domain is a logical group of PTP devices within a physical network that belong to the same domain number. Slave devices that shall sync to a certain master within a network must have been configured with a unique domain number which is the as same on the master.
- GM:** A MAC address of the current Grandmaster.
- DelayMech:** two options possible:  
E2E (End-to-end) where delay measurement messages are sent from the slave to the master (the two end nodes).  
  
P2P (Peer-to-peer): where each device (a peer) in the network exchanges peer-delay measurement messages. This way each device can keep track of the delays between itself and its immediately connected neighbors. P2P mechanism can be used in 1588 PTP-capable networks only.
- NetwProto:** two options possible:  
ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet frame including MAC addresses of a destination and a source.  
  
UDP-UDP/IPv4 (Layer 3): User Data Protocol one of the main protocols used for the Internet.

### 9.3.4.7 Menu TSU Setup

With this menu, all PTP parameters can be configured for the selected interface:

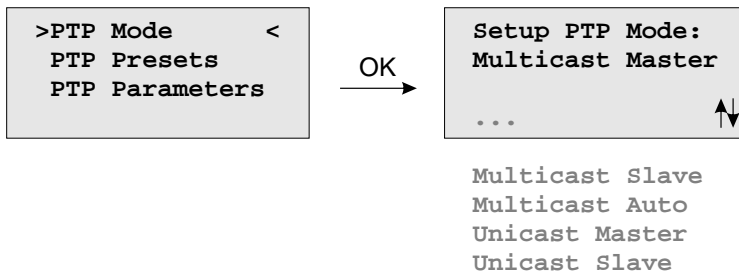


The **Set Dbg Level** menu is for maintenance and debugging purposes only, therefore leave it unchanged unless advised by a technician. The Level of debugging can be increased from 0 (default) to 3 with additional data being logged at each increased debugging level.

**Set temp Offs** is an offset value set temporarily, mainly for a debugging purpose. With the next warm boot the value is set back to 0.

**Enable Stats** option is also mainly for debugging. Per default it is disabled.

### 9.3.4.8 Menu PTP Mode



The number of different PTP operation modes depends on the feature set of the purchased unit.

Supported modes on a GPS-only or GPS/GLONASS-only system:

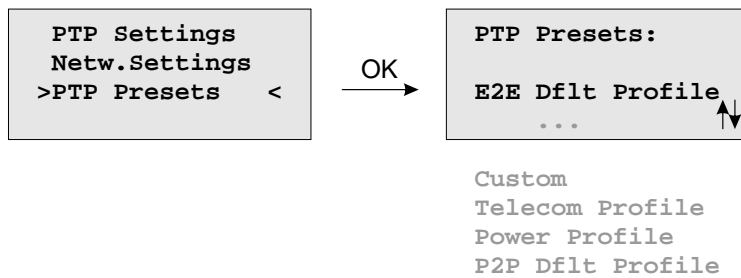
- PTPv2 Multicast Master
- PTPv2 Unicast Master

Supported Modes on a MRS system:

- PTPv2 Multicast Slave
- PTPv2 Multicast Master
- PTPv2 Multicast Auto
- PTPv2 Unicast Slave
- PTPv2 Unicast Master

### 9.3.4.9 Load PTP Presets

Each PTP preset represents a set of PTP configuration parameters that will switch the PTP engine to a dedicated PTP profile. After a preset has been selected, the user still has the opportunity to change all PTP parameters and "fine-tune" them.



**Note:** Whenever a PTP preset is selected, all previously saved PTP parameters will be overwritten!

Six different presets are supported:

#### In Multicast Master / Slave Mode:

##### Delay Request Response Default Profile

- Sync Msg Rate: 1/sec
- Ann Msg Rate: 2 sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"

##### Peer-to-Peer Default Profile

- Sync Msg Rate: 1/sec
- Ann. Msg Rate: 2 sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "P2P"

##### Power Systems Profile

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

##### Telecom ITU-T G.8275.1

- Ann Msg. Rate: 8/sec
- Sync Msg. Rate: 16/sec
- Del Req Rate: 16/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E"
- Network Prot. "Layer 2 (IEEE 802.3)"

---

In Unicast Master / Slave Mode:

---

**Telecom ITU-T G.8265.1**

- Ann Msg. Rate: 1/sec
  - Sync Msg. Rate: 16/sec
  - Del Req Rate: 16/sec
  - Priority 1: 128
  - Priority 2: 128
  - Delay Mech: "E2E"
  - Network Prot. "Layer 3 (UDP/IPv4)"
- 

In Unicast or Multicast Master / Slave Mode:

---

**SMPTE ST 2059-2**

- Ann Msg. Rate: 4/sec
- Sync Msg. Rate: 8/sec
- Del Req Rate: 8/sec
- Priority 1: 128
- Priority 2: 128
- Delay Mech: "E2E" or "P2P"

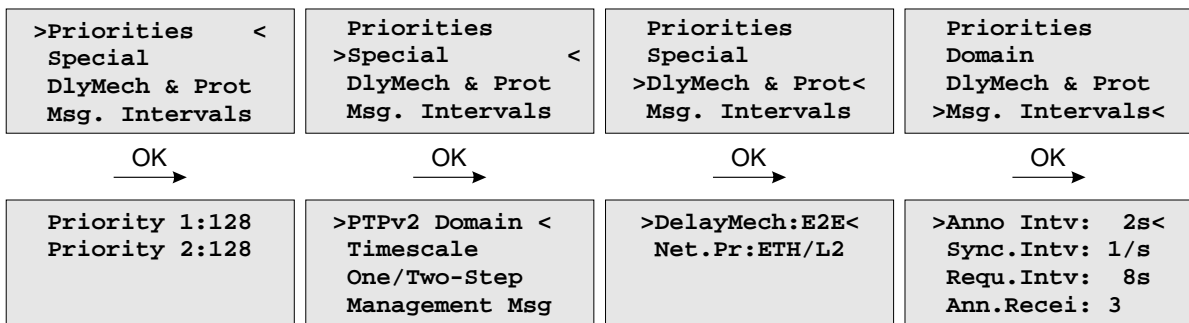
**Custom Profile**

By selecting "Custom" settings all parameters are ready for editing.

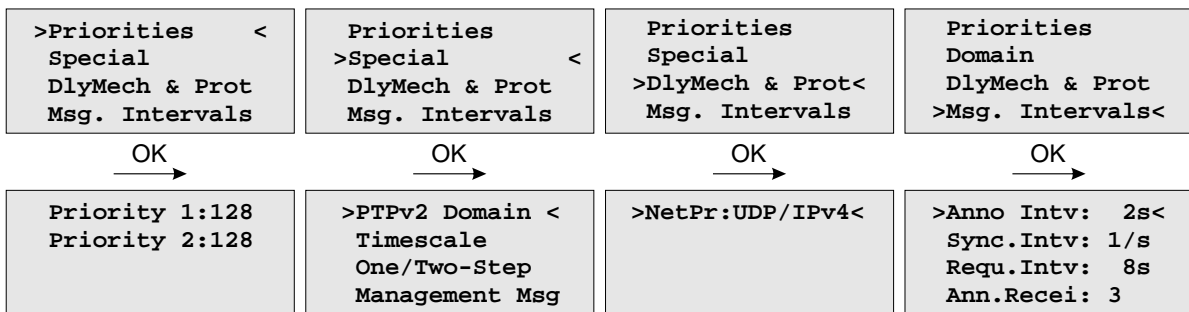
### 9.3.4.10 PTP Parameters

Depending on the selected mode, different sub menus will appear for configuring the PTP parameters.

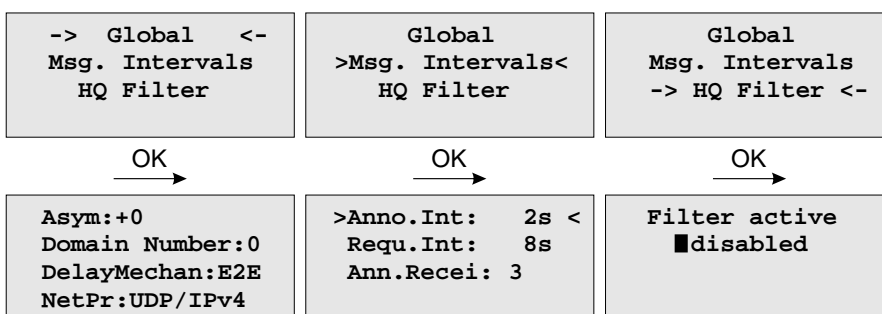
#### MULTICAST MASTER



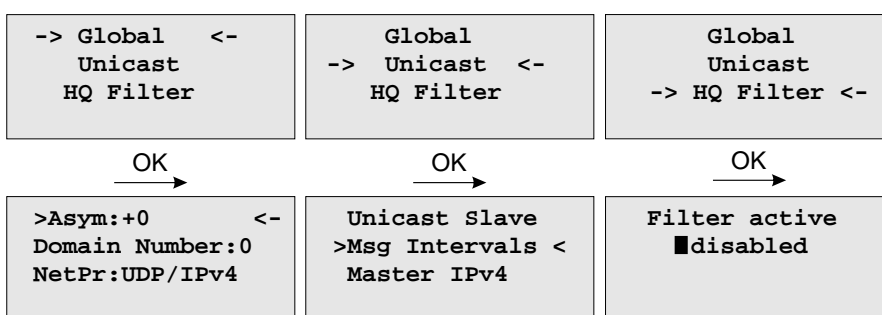
#### UNICAST MASTER



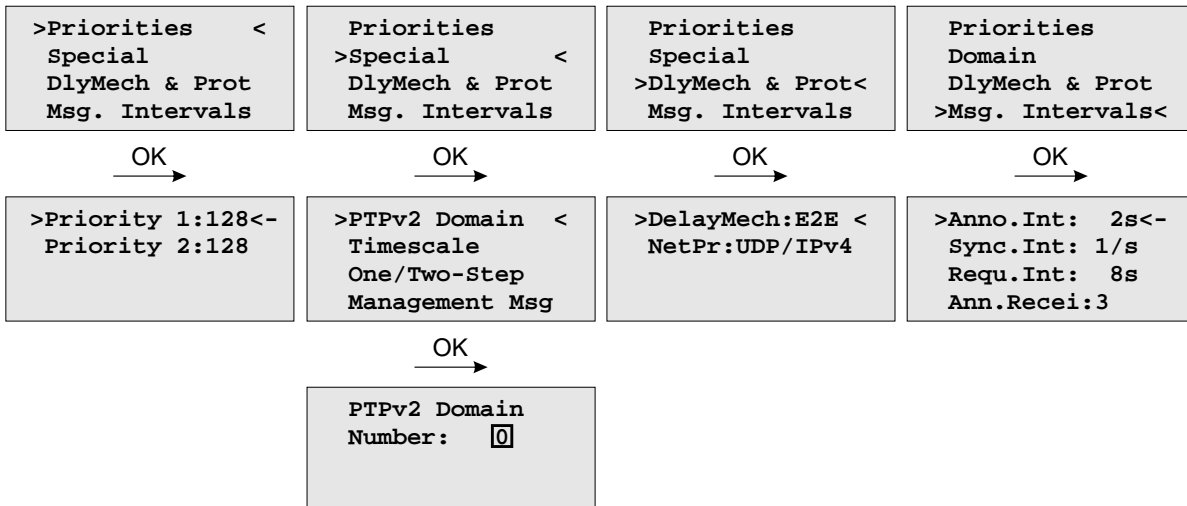
#### MULTICAST SLAVE



#### UNICAST SLAVE



### 9.3.4.11 Multicast Master



In Multicast mode all PTP messages will be sent as Multicast packets where receiving nodes (slave clocks) do not require to know the identity of the time sources in the network. The selection of the active time source (the Grandmaster) follows the so-called "Best Master Clock Algorithm" a mechanism that all participating PTP masters must follow. The multicast communication model requires a minimized configuration of all participating nodes and this advantage is beneficial in smaller networks. In larger networks it is considered inefficient as the content of message is forwarded to all nodes, requiring them to spend network bandwidth and CPU resources.

The following settings can be done in Multicast Master Mode.

**Priority1:** The attribute is used in the execution of the best master clock algorithm (BMCA). Lower values take precedence.

Configurable range: 0..255.

The operation of the BMCA selects clocks from a set with a lower value of priority1 over clocks from a set with a greater value of priority1.

**Priority2:** The attribute is used in the execution of the BMCA. Lower values take precedence.

Configurable range: 0..255.

In the event that the operation of the BMCA fails to order the clocks based on the values of priority1, clockClass, clockAccuracy, and scaledOffsetLogVariance, the priority2 attribute allows the creation of up to 256 priorities to be evaluated before the tiebreaker. The tiebreaker is based on the clockIdentity. The values clockClass, clockAccuracy, and scaledOffsetLogVariance depend on the internal state of the grandmaster and cannot be configured.

**PTPv2 Domain:** A PTP domain is a logical group of PTP devices within a physical network that belong to the same domain number. Slave devices that shall sync to a certain master within a network must have configured a unique domain number which is the same on the master.

**Timescale:** two options possible:

**PTP:** In normal operation, the epoch is the PTP epoch and the timescale is continuous. The unit of measure of time is the SI second. The PTP epoch is 1 January 1970 00:00:00 TAI time source.

**ARB** as arbitrary: In normal operation, the epoch is set by an administrative procedure.

- One / Two Step:** Per default Two Step approach is enabled  
 Two Step approach: The PTP protocol requires the master to periodically send SYNC messages to the slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by sending this time stamp in a separate packet (a so-called FOLLOW-UP message).
- One Step approach: the SYNC message itself is time stamped on- the- fly just before it leaves the network port. Therefore, not FOLLOW-UP message is needed.
- Management Msg:** A protocol within PTP used to query and update the PTP data sets maintained by master clocks. These messages are also used to customize a PTP system and for initialization and fault management. Management messages are used between management nodes and clocks. Per default are enabled.
- DelayMech:** two options possible:  
 E2E (End-to-end) where delay measurement messages are sent from the slave to the master (the two end nodes).
- P2P (Peer-to-peer): where each device (a peer) in the network exchanges peer-delay measurement messages. This way each device can keep track of the delays between itself and its immediately connected neighbors. P2P mechanism can be used in 1588 PTP-capable networks only.
- NetPr:** two options for the network protocol are possible:  
 ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet frame including MAC addresses of a destination and a source.
- UDP-UDP/IPv4/IPv6 (Layer 3): User Data Protocol one of the main protocols used for the Internet.
- Msg. Intervals:** specify the settings for the PTP timing messages.
- Anno. Intv** specifies the time for sending announce messages between masters to select the Grand Master. Available settings are: 16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s with a default value 2 seconds.
- Sync. Intv** specifies the time for sending sync messages from a master to a slave. Available settings are: 128/s, 64/s ... 64s, 128s, with a default value 1 second.
- Requ. Intv** specifies an interval how often delay request messages are sent from a slave to the master. Delay request messages intervals 128/s, 64/s,... 64s, 128s, with a default value 2 seconds.
- Ann. Recei** value specifies the time for announce receipt timeout messages which is 2-10 times the Announce interval, with a default of 3. This is the time for a BMCA to determine a Grand master.



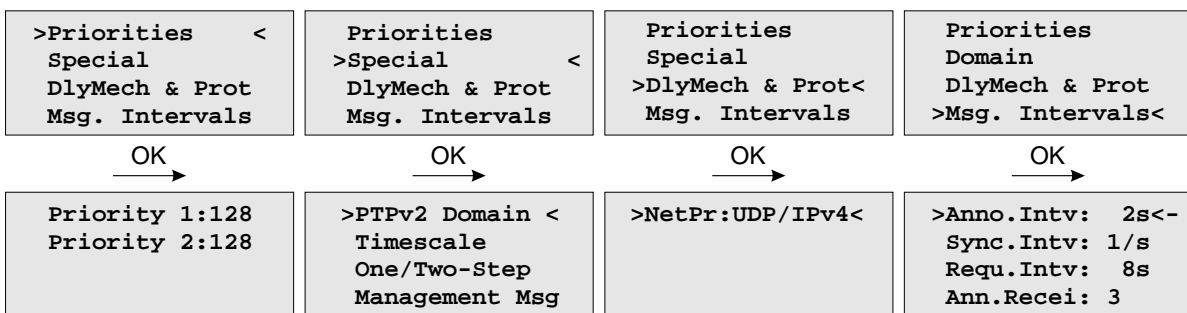
### 9.3.4.12 Unicast Master

Unicast mode is applicable generally in larger networks to reduce the overall traffic or when the network is not set up to support multicast. Sometimes there is only one slave and one master of interest and they just want to be alone with each other to have a private conversation without other PTP capable devices being involved. Whatever the reason IEEE 1588 2008 includes support for unicast operation.

When one or more masters have been identified the slave can use Unicast Negotiation to get Announce and Sync messages sent from the master, and to get Delay Requests answered with Delay Responses.

The PTP message sequences between the master and a slave are repeated until the duration of a negotiated interval expires. For example a slave might ask for 4 Sync messages per second, for a period of 60 seconds. In this case after 60 seconds the master would stop sending Sync messages until another Sync message contract was negotiated.

If unicast mode is selected then an additional sub menu will appear to configure or display unicast specific parameters.



The following settings can be done in Unicast Master Mode:

- Priority1:** The attribute is used in the execution of the best master clock algorithm (BMCA). Lower values take precedence.

Configurable range: 0..255.

The operation of the BMCA selects clocks from a set with a lower value of priority1 over clocks from a set with a greater value of priority1.
- Priority2:** The attribute is used in the execution of the BMCA. Lower values take precedence.

Configurable range: 0..255.

In the event that the operation of the BMCA fails to order the clocks based on the values of priority1, clockClass, clockAccuracy, and scaledOffsetLogVariance, the priority2 attribute allows the creation of up to 256 priorities to be evaluated before the tiebreaker. The tiebreaker is based on the clockIdentity. The values clockClass, clockAccuracy, and scaledOffsetLogVariance depend on the internal state of the grandmaster and cannot be configured.
- PTPv2 Domain:** A PTP domain is a logical group of PTP devices within a physical network that belong to the same domain number. Slave devices that shall sync to a certain master within a network must have configured a unique domain number which is the same on the master.
- Timescale:** two options possible:  
**PTP:** In normal operation, the epoch is the PTP epoch and the timescale is continuous. The unit of measure of time is the SI second. The PTP epoch is 1 January 1970 00:00:00 TAI time source.  
**ARB** as arbitrary: In normal operation, the epoch is set by an administrative procedure.

**One / Two Step:** Two Step approach: The PTP protocol requires the master to periodically send SYNC messages to the slave devices. The hardware time stamping approach of PTP requires that the master records the exact time when such a SYNC packet is going on the network wire and needs to communicate this time stamp to the slaves. This can be achieved by sending this time stamp in a separate packet (a so-called FOLLOW-UP message).

One Step approach: the SYNC message itself is time stamped on-the-fly just before it leaves the network port. Therefore, not FOLLOW-UP message is needed.

Per default Two Step approach is enabled.

**Management Msg:** A protocol within PTP used to query and update the PTP data sets maintained by master clocks. These messages are also used to customize a PTP system and for initialization and fault management. Management messages are used between management nodes and clocks.

Per default are enabled.

**DelayMech:** in unicast mode only one option possible:  
E2E (End-to-end) where delay measurement messages are sent from the slave to the master (the two end nodes).

**NetPr:** in unicast mode only one option for the network protocol possible:  
UDP-UDP / IPv4 / IPv6 (Layer 3): User Data Protocol is one of the main protocols used for the Internet.

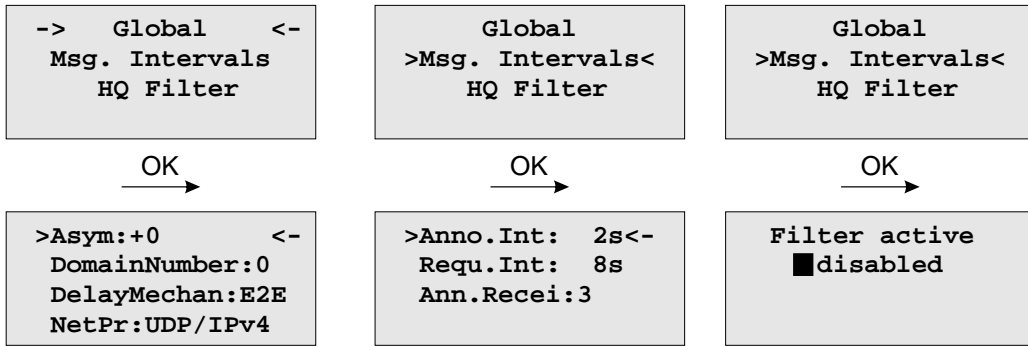
**Msg. Intervals:** specify the settings for the PTP timing messages.  
**Anno. Intv** specifies the time for sending announce messages between masters to select the Grand Master. Available settings are: 16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s with a default value 2 seconds.

**Sync. Intv** specifies the time for sending sync messages from a master to a slave. Available settings are: 128/s, 64/s ... 64s, 128s, with a default value 1 second.

**Requ. Intv** specifies an interval how often delay request messages are sent from a slave to the master. Delay request messages intervals 128/s, 64/s,... 64s, 128s, with a default value 2 seconds.

**Ann. Recei** value specifies the time for announce receipt timeout messages which is 2-10 times the Announce interval, with a default of 3. This is the time for a BMCA to determine a Grand master.

### 9.3.4.13 Multicast Slave (MRS only)

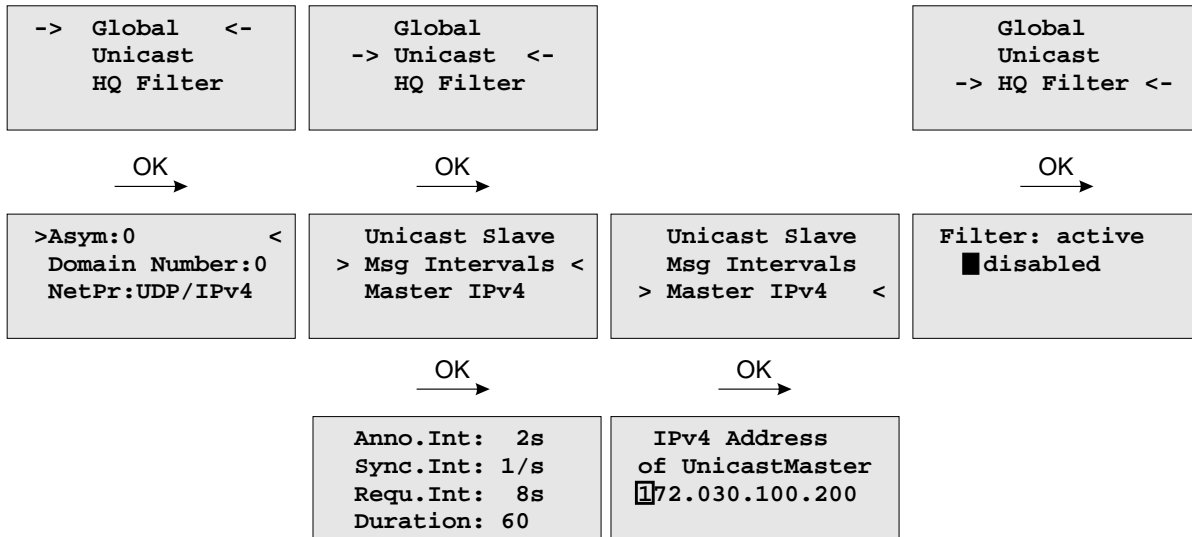


The following settings can be done in Multicast Slave Mode:

- Asym:** or Default Asymmetry is an initial calibration value (in ns) and can be entered here if a certain asymmetry offset in the network path is known before the PTP unit starts. This occurs in SDH networks for example.
- Max.Path Delay:** If a measured path delay exceeds the value of this parameter (in ns), then the PTP unit is able to detect a change in the asymmetry offset and can take this into account for its delay measurements.
- Note:** Keep defaults settings here (0 ns for both parameters) unless some problems with the client synchronization accuracy are observed and only if the asymmetry offset can be measured beforehand.
- PTPv2 Domain:** A PTP domain is a logical group of PTP devices within a physical network that belong to the same domain number. Slave devices that shall sync to a certain master within a network must have configured a unique domain number which is the same on the master.
- DelayMech:** two options possible:  
 E2E (End-to-end) where delay measurement messages are sent from the slave to the master (the two end nodes).  
 P2P (Peer-to-peer): where each device (a peer) in the network exchanges peer-delay measurement messages. This way each device can keep track of the delays between itself and its immediately connected neighbors (for example a switch or a router). P2P mechanism can be used in 1588 PTP capable networks only.
- NetPr:** two options for the network protocol possible:  
 ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet frame including MAC addresses of a destination and a source.  
 UDP-UDP/IPv4/IPv6 (Layer 3): User Data Protocol one of the main protocols used for the Internet.

- Msg. Intervals:** specify the settings for the PTP timing messages.
- Anno. Intv** specifies the time for sending announce messages between masters to select the Grand Master. Available settings are: 16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s with a default value 2 seconds.
- Sync. Intv** specifies the time for sending sync messages from a master to a slave. Available settings are: 128/s, 64/s ... 64s, 128s, with a default value 1 second.
- Requ. Intv** specifies an interval how often delay request messages are sent from a slave to the master. Delay request messages intervals 128/s, 64/s,... 64s, 128s, with a default value 2 seconds.
- Ann. Recei** value specifies the time for announce receipt timeout messages which is 2-10 times the Announce interval, with a default of 3. This is the time for a BMCA to determine a Grand master.
- HQ Filter:** In heavy loaded networks when using non-PTP compliant switches, the "HQ Filter" can be activated to reduce the jitter. Detailed information about the usage and the configuration of the HQ filter can be found in the "PTPv2 Configuration Guide" in chapter [PTP Option](#). The Default setting is with HQ Filter disabled.

### 9.3.4.14 Unicast Slave (MRS only)



The following settings can be done in Unicast Slave Mode:

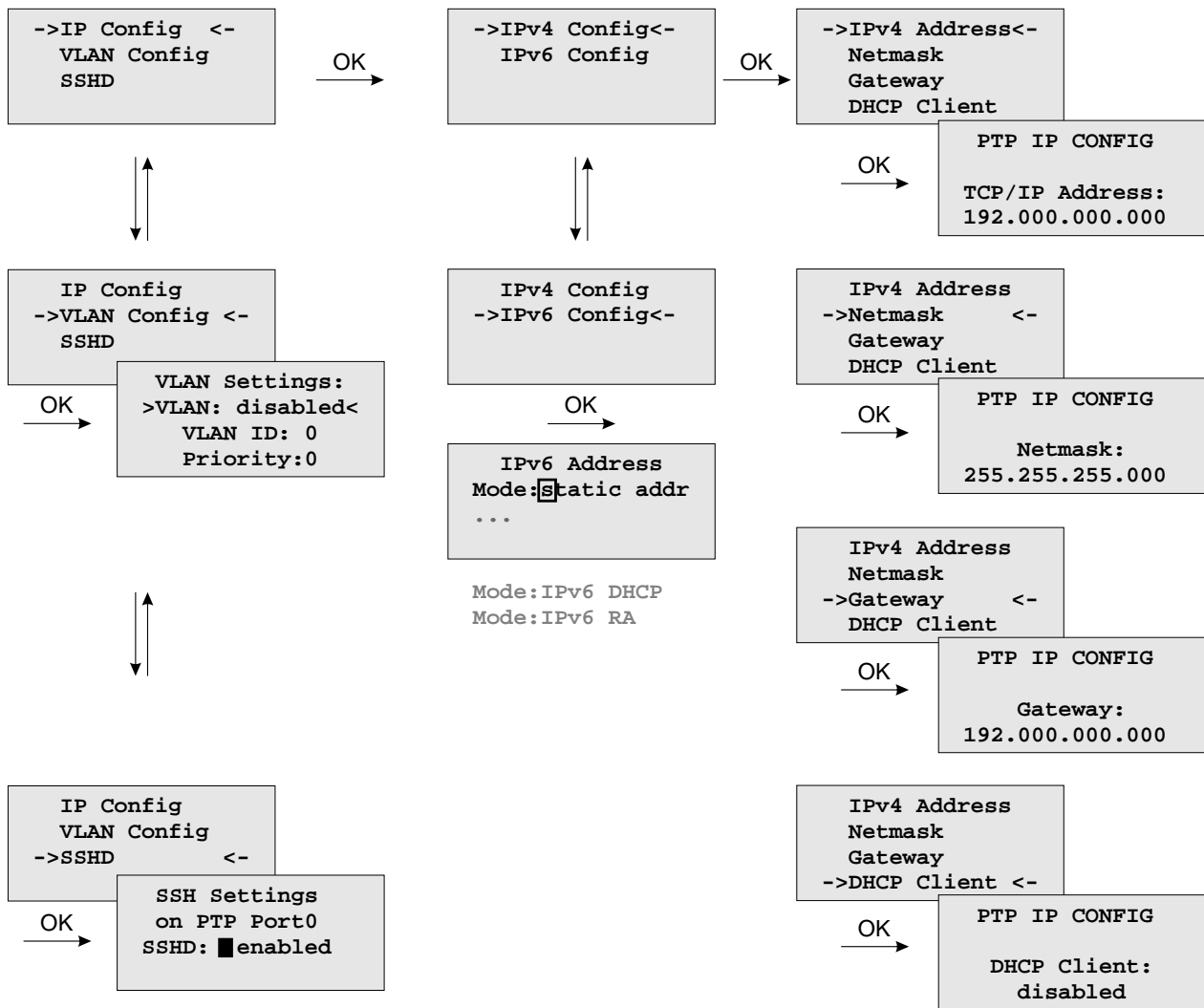
- Asym:** or Default Asymmetry is an initial calibration value (in ns) and can be entered here if a certain asymmetry offset in the network path is known before the PTP unit starts. This occurs in SDH networks for example.
- Max. Path Delay:** If a measured path delay exceeds the value of this parameter (in ns), then the PTP unit is able to detect a change in the asymmetry offset and can take this into account for its delay measurements.
- Note:** Keep defaults settings here (0 ns for both parameters) unless some problems with the client synchronization accuracy are observed and only if the asymmetry offset can be measured beforehand.
- PTPv2 Domain:** A PTP domain is a logical group of PTP devices within a physical network that belong to the same domain number. Slave devices that shall sync to a certain master within a network must have configured a unique domain number which is the same on the master.
- NetPr:** one setting possible:  
UDP-UDP/IPv4 (Layer 3): User Data Protocol one of the main protocols used for the Internet.
- Msg Intervals:** specify the settings for the PTP timing messages.  
**Anno. Intv** specifies the time interval of announce messages between master servers to select the Grand Master. Note: This value should be the same as for the master. Available settings are: 1, 2, 4, 8 or 16 seconds, with a default value of 2 seconds.  
**Sync. Intv** specifies the time interval of sync messages that a slave requests from a master. Available settings are 0.5, 1, or 2 seconds, with a default value of 1 second.  
**Requ. Intv** specifies an interval how often delay request messages are sent from a slave to the master. Delay request messages intervals of 1, 2, 4, 8, 16 or 32 seconds, with a default value of 8 seconds.

The **Duration** parameter is used to set a timeout for the grandmaster that sends out the sync packages until the timeout expires. A slave sends a new signaling message to refresh the request before the end of the Duration timeout. Thus it is receiving the requested sync packages continuously. The duration parameter will handle all message types and should be in the range between 10-300 s.

- Master IPv4:** The correct IP address of the Master's PTP port must be entered in this field.
- HQ Filter:** In heavy loaded networks when using non-PTP compliant switches, the "HQ Filter" can be activated to reduce the jitter. Detailed information about the usage and the configuration of the HQ filter can be found in the "PTPv2 Configuration Guide" in chapter [PTP Option](#). The Default setting is with HQ Filter disabled.

### 9.3.4.15 Menu PTP Network Settings

Configuration for the PTP network port



IP configuration for the PTPx interface. It can be selected if either a static IP address shall be used or if a dynamic IP address via DHCP should be assigned.

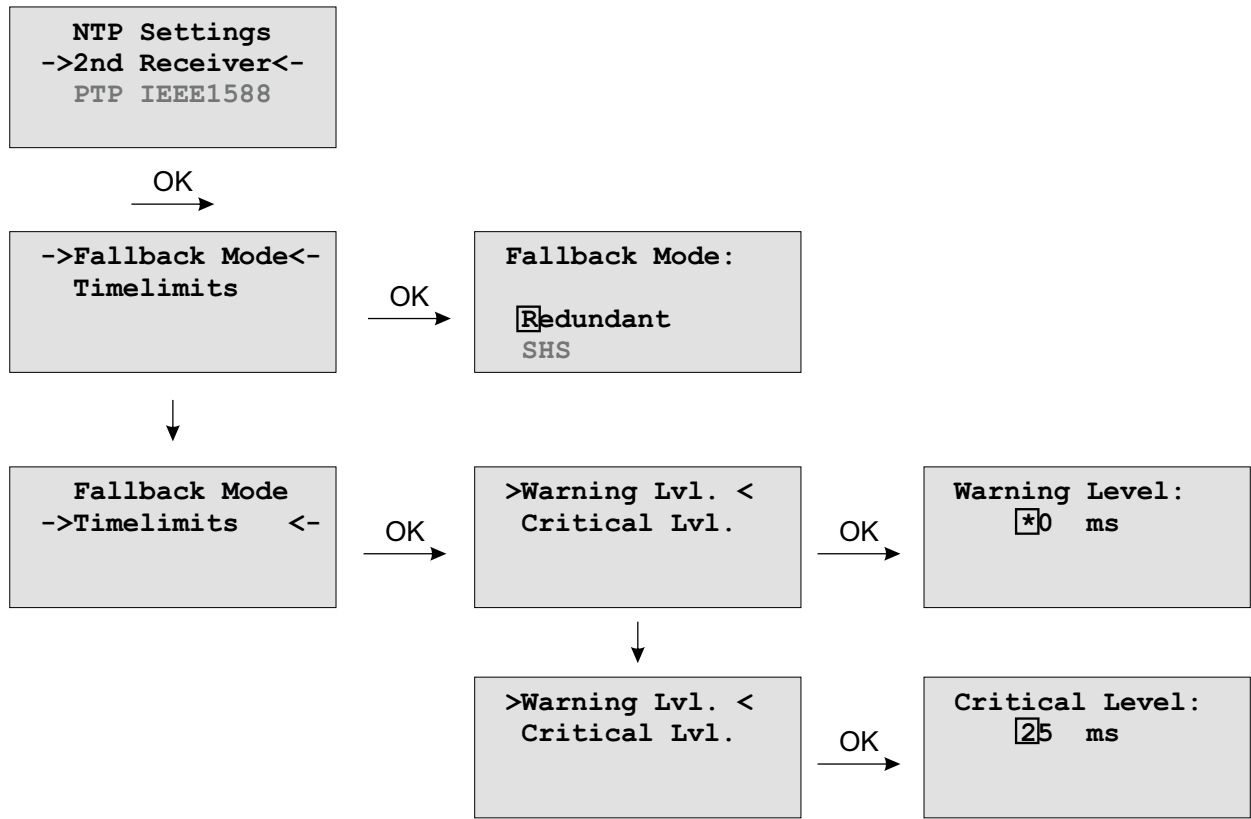
#### VLAN Config:

Configuration of Virtual LAN (IEEE 802.1Q) settings for the PTPx interface:

- VLAN ID: A 12-bit value (0..4096) specifying the VLAN to which the network port belongs.
- VLAN Priority: The priority indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data,...)

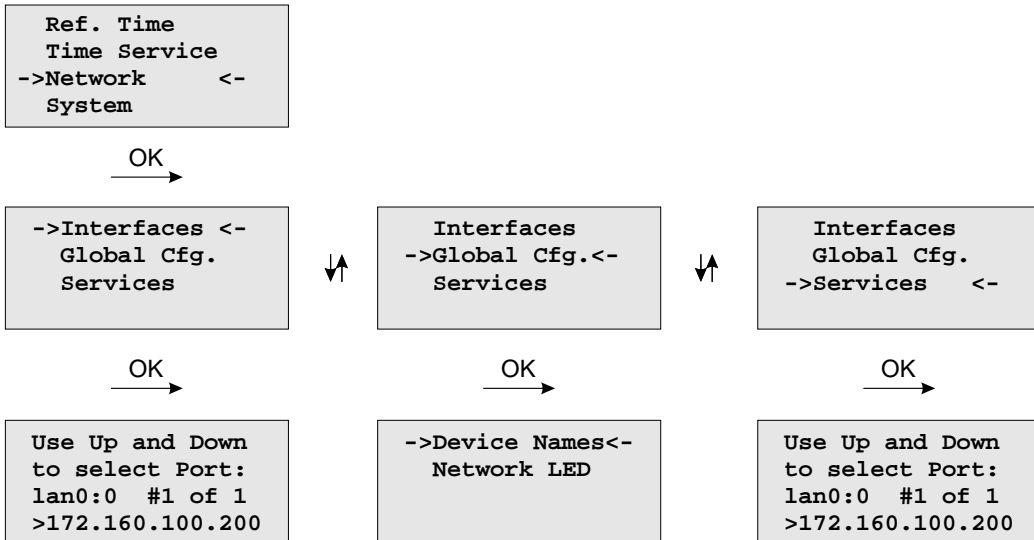
### 9.3.4.16 Optional Menu: 2nd Receiver

With the submenu *2ndreceiver* you can select the Fallback mode (Redundant or SHS) and you also can adjust the time limits for the "Warning level" and the "Critical Level" here.





### 9.3.5 Menu: Network

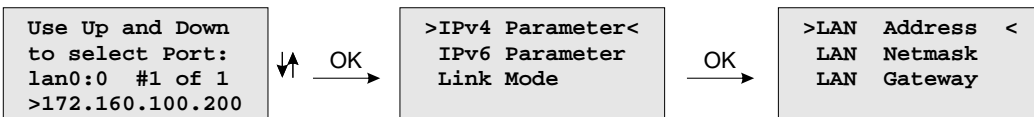


In this submenu the network configuration parameters related to the network interfaces can be changed. The submenus can be selected with the arrow keys and the “OK” button:

As soon as an IP address is configured, additional network configuration can be done via network connection with TELNET, SSH or the WEB interface. Ask your network administrator for network specific parameters. Every change of the network parameters will restart the NTP. All network specific parameters will be saved on the flash disk (/mnt/flash/config/global\_configuration) and will be reloaded after reboot. It is highly recommended not to edit this file manually but to configure the parameters via the several configuration interfaces (HTTP, CLI or SNMP). If this file is not present, an empty file will be created. See Appendix for the default settings of this file.

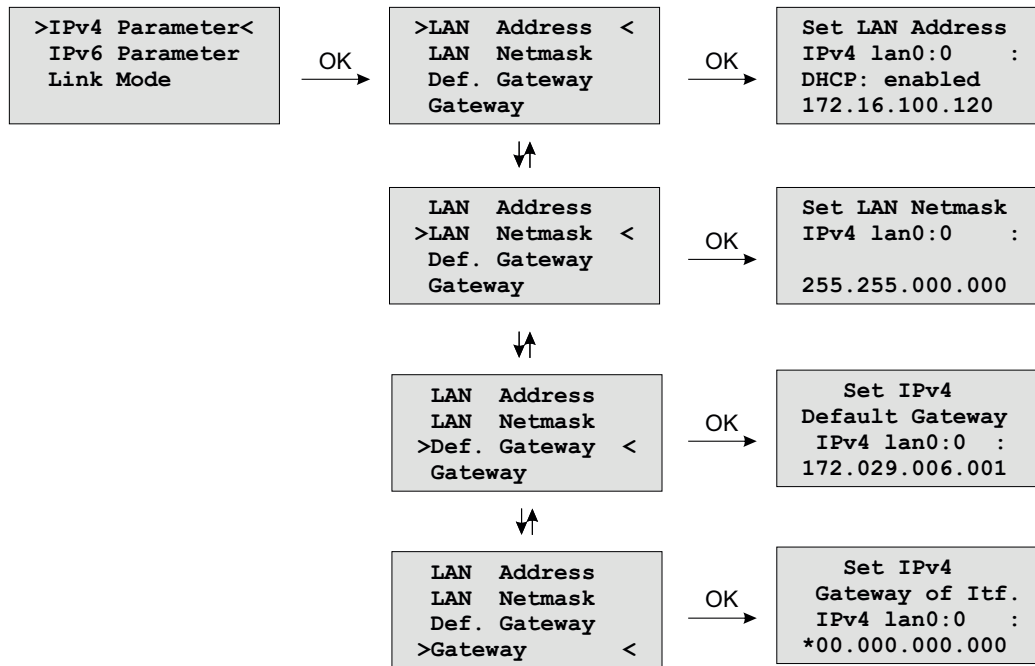
#### 9.3.5.1 Menu: Setup Network Interfaces

In the network configuration parameters related to the network interfaces can be changed. The following submenus can be selected with the arrow keys and the “OK” button:



When configured an IP address once additionally network configuration can be done via network connection with TELNET, SSH or the WEB interface. Ask your network administrator for network specific parameters. Every change of the network parameters will restart the NTP. All network specific parameters will be saved on the flash disk (/mnt/flash/config/global\_configuration) and will be reloaded after reboot.

## 9.3.5.2 Menu: Setup IPv4 LAN Parameter



There is a separate configuration submenu for every physical network interface. If there is no DHCP client mode activated a static IP address for each interface can be entered. 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: 172.160.100.200**

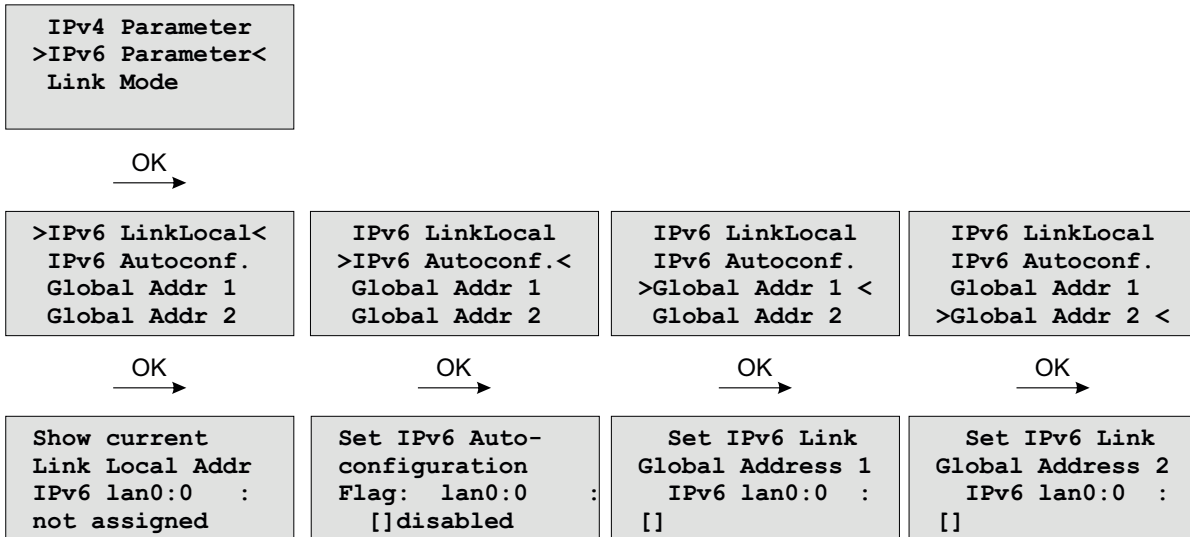
Additionally you can specify the IPv4 netmask and your default gateway address.

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". Using DHCP is the default factory setting.

If the DHCP client has been activated, the automatically obtained parameters are shown in the appropriate fields (IPv4 Address, Netmask, Default Gateway).

### 9.3.5.3 Menu: Setup IPv6 Parameter

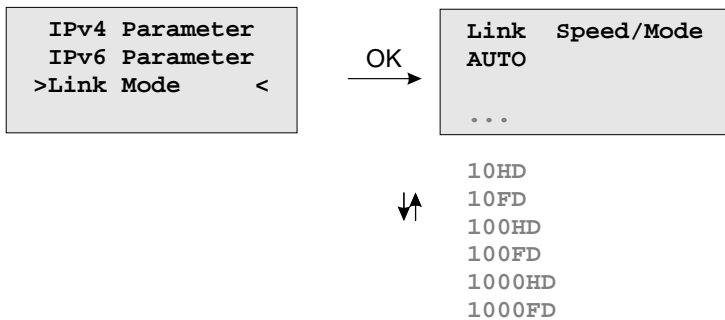


The IPV6 parameter can be configured via the front panel display for the first ethernet port (ETH0) only. Additionally IPV6 configuration can be done via network connection with TELNET, SSH or the WEB interface.

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

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.

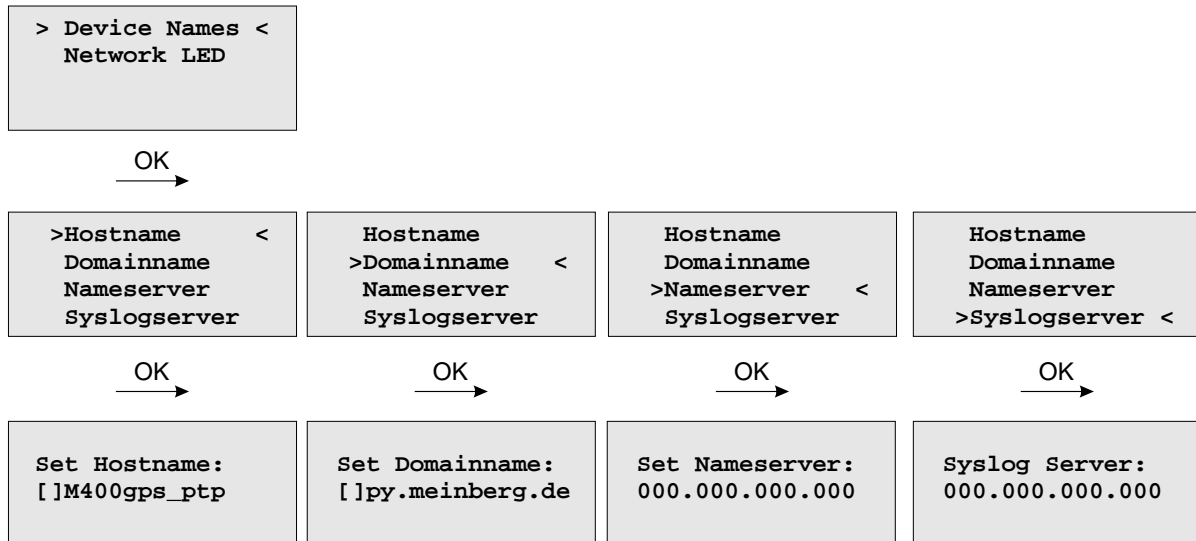
### 9.3.5.4 Menu: Link Mode



With the Link Mode submenu the parameters for link speed and duplex mode of the first ethernet interface (ETH0) can be configured. There are 5 modes available: Autosensing, 10 Mbit/Half Duplex, 100 Mbit/Half-Duplex, 1000 Mbit/Half-Duplex (Gigabit Support), 10MBit/Full-Duplex, 100 Mbit/Full-Duplex and 1000 Mbit/Full-Duplex (Gigabit Support).

The interfaces are configured with „Autosensing“ by default.

## 9.3.5.5 Menu: Global Configuration



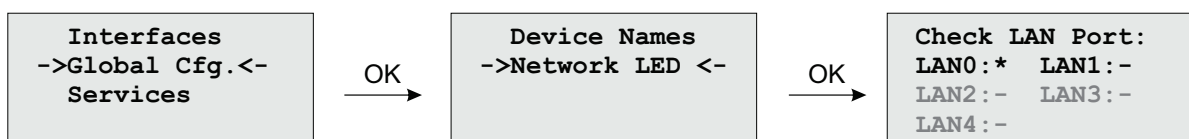
In this sub menu you can change the global network settings like host and domain name, nameserver and syslog server. Further name- or syslog servers can be set up via HTTP interface or CLI Setup. In the nameserver and syslog server fields you have to enter an IPv4 address.

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 SYSLOG daemon can be told to do so by using the command “syslogd -r” when starting the daemon.

If you enter nothing in the SYSLOG server fields or specify 0 .0.0.0 as the SYSLOG servers addresses, the remote SYSLOG service is not used on your LANTIME.

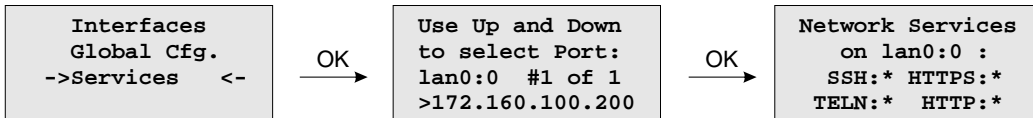
Please be aware of the fact that all SYSLOG entries of the timeserver are stored in „/var/log/messages“ and will be deleted when you power off or reboot the timeserver. A daily CRON job is checking for the size of the LANTIME SYSLOG and deletes it automatically if the log size is exceeding a certain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

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



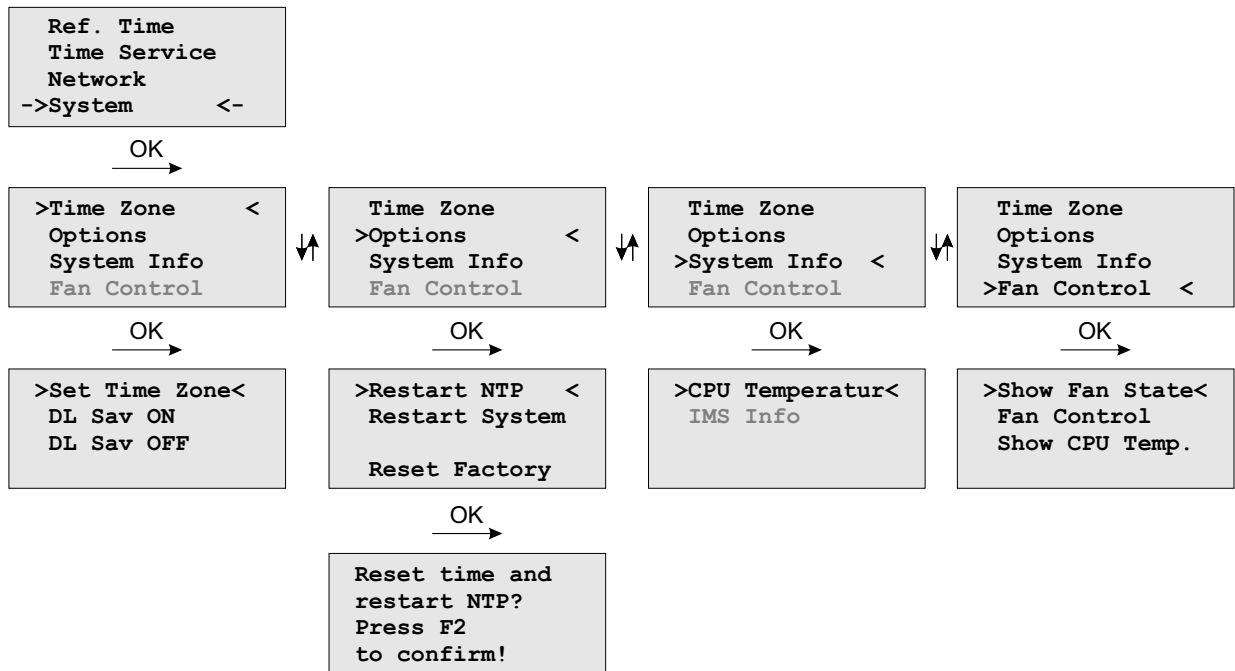
The submenu „Netw. LED“ will monitor the network ports, which will be checked continuously if the network port is „LINKED UP“. If one of these ports has no link up, the network LED on the front panel will change to red. An „L“ for „LED“ indicates if the port is checked. Please navigate through the list of ports with the LEFT/RIGHT buttons and change the setting with the UP/DOWN buttons.

### 9.3.5.6 Menu: Network Services



The possible network protocols and access methods can be configured. After pressing the OK button you can enable/disable SSH, TELNET, SNMP, FTP, IPV6, HTTP, HTTPS and NETBIOS by using the UP/DOWN Keys and navigate through the list with the LEFT/RIGHT keys. After you saved your settings with the "OK" button, all these subsystems are stopped and eventually restarted (only if they are enabled, of course).

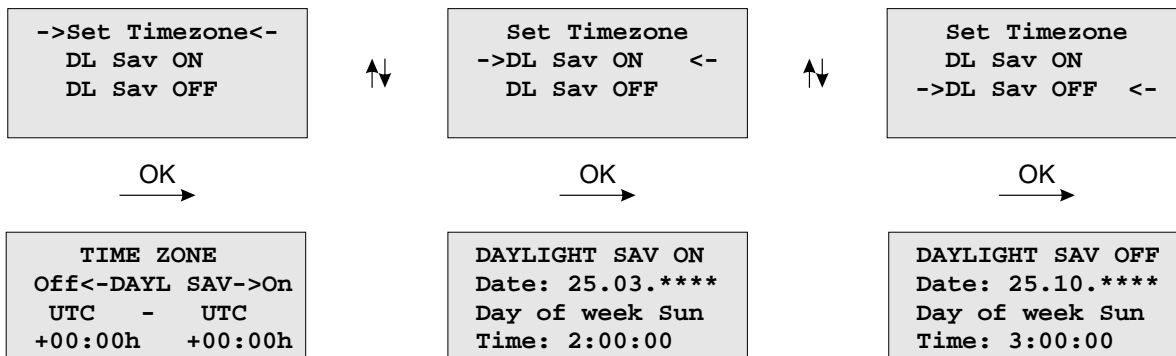
## 9.3.6 Menu: System



In this submenu system specific parameters can be configured.

### 9.3.6.1 Menu: Set Time Zone of Display

The time zone of the time that is shown on the front panel display can be set up here. The internal time zone of the timeserver and the time of NTP will always be UTC. These parameters will not affect the serial output lines and the timecode (IRIG) outputs. These parameters have to be configured in another menu - (**Reference Time->Setup Outputs**).



This menu lets the user enter the names of the local time zone with daylight saving disabled and enabled, together with the zones' time offsets from UTC. These parameters are used to convert UTC to local time, e.g. MEZ = UTC + 1h and MESZ = UTC + 2h for central Europe. The range of date daylight saving comes in effect can be entered using the next two pages of the setup menu.

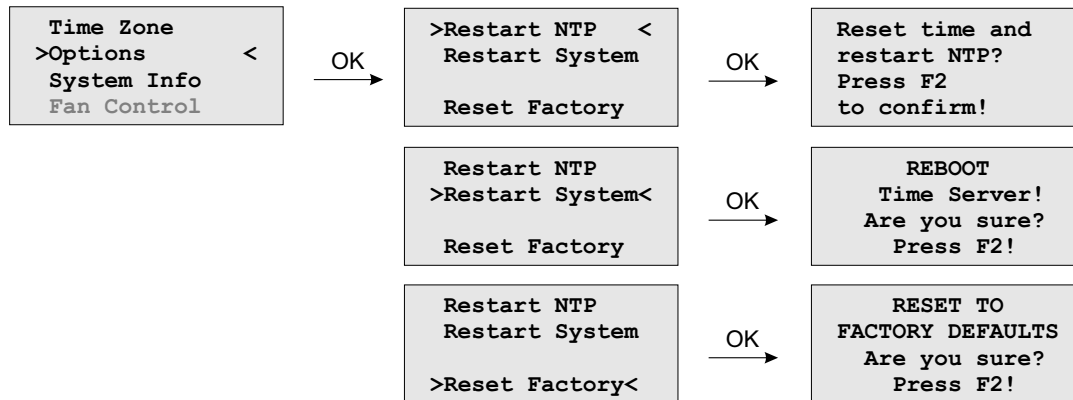
Beginning and ending of daylight saving may either be defined by exact dates for a single year or using an algorithm which allows the receiver to re-compute the effective dates year by year. The figures below show how to enter parameters in both cases. If the number of the year is displayed as wildcards ('\*'), a day-of-week must be specified. Then, starting from the configured date, daylight saving changes the first day which matches the configured day-of-week. In the figure below October 25th, 2008 is a Saturday, so the next Sunday is October 26th, 2008.

All changeover rules for the daylight saving like "the first/the second/the second to last/the last Sunday/Monday etc. in the x-th month," can be described by the used format "first specified day-of-week after a defined date".

If the number of the year is not displayed as wildcards the complete date exactly determines the day daylight saving has to change (October 26th, 2008 in the figures below), so the day-of-week does not need to be specified and therefore is displayed as wildcards.

If no changeover in daylight saving is wanted, identical dates and times must be entered in both of the submenus (DAYLIGHT SAV ON/OFF).

## 9.3.6.2 Menu Options

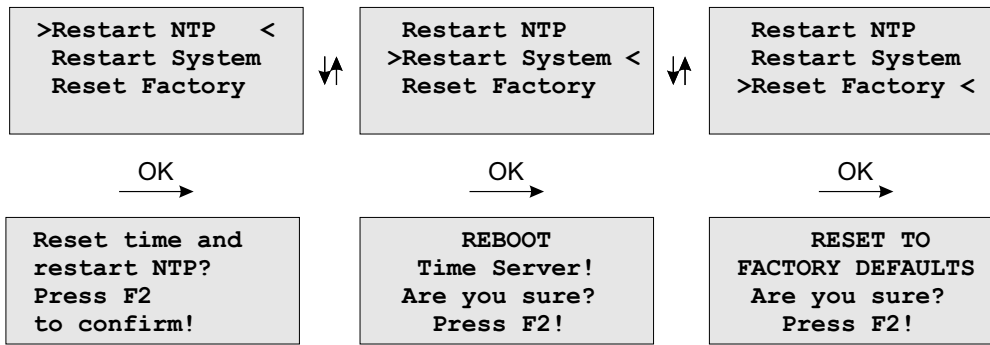


In menu option you can make the following settings or request setting information:

- Time Zone:** The converted time (offset to UTC) for the configured time zone, which is shown in the display. This has no effect on the time strings that are outputted via the serial interfaces.
- You can make this setting via the menu "Ref. Time -> Set Outputs -> Time Zone".
- Options:** In this sub menu you can reset the system to the state of delivery by using "Reset Factory". The network settings remain unchanged.
- With "Restart NTP" you can restart the NTP service and with "Restart System" the LINUX operating system of the CPU.
- System Info:** With "System Info" you can request the current operating temperature of the CPU. If the LANTIME is used in an IMS System, information about the system configuration, like the allocation of single slots, can be displayed in this menu section.
- Fan Control:** If an active cooling is installed, the cooling status can be displayed via this menu item and via "Fan Control" you can set the mode of the active cooling:
- Auto:** (temperature independent - the threshold value can be adjusted via the webinterface - menu "System -> Fan Control".
- FAN ON:** The cooling is permanently active.
- FAN OFF:** The cooling is permanently off.



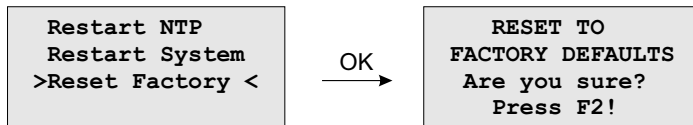
### 9.3.6.3 Menu: Restart System



If the time of the reference clock has changed (e.g. while testing with different times) the system time has to be set with the time of the reference clock and the NTP has to be restarted.

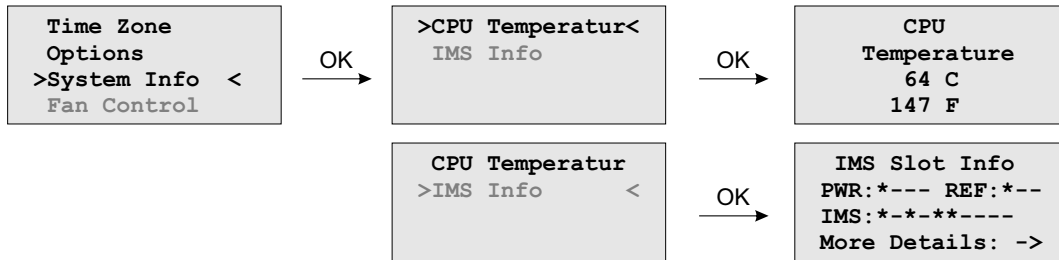
The command **Reboot System** reboots the Linux operating system – the built-in reference clock will not be restarted.

### 9.3.6.4 Menu Factory Reset



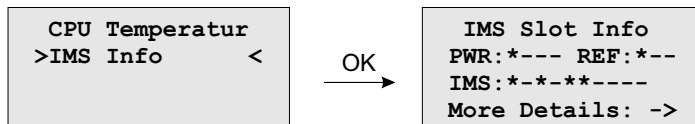
When **Reset to factory defaults** is called and confirmed, all network parameters and system parameters are reset to factory settings.

### 9.3.6.5 Menu System Info



In the "System Info" submenu, the CPU temperature can be queried. In IMS systems a detailed overview of the system configuration can be shown.

### 9.3.6.6 Option: Menu IMS Slot Info



Note: This display menu is visible only in case of an IMS system. Here a detailed overview of the modules, used in the selected slots, are given.

The example above shows the configuration of a LANTIME M3000:

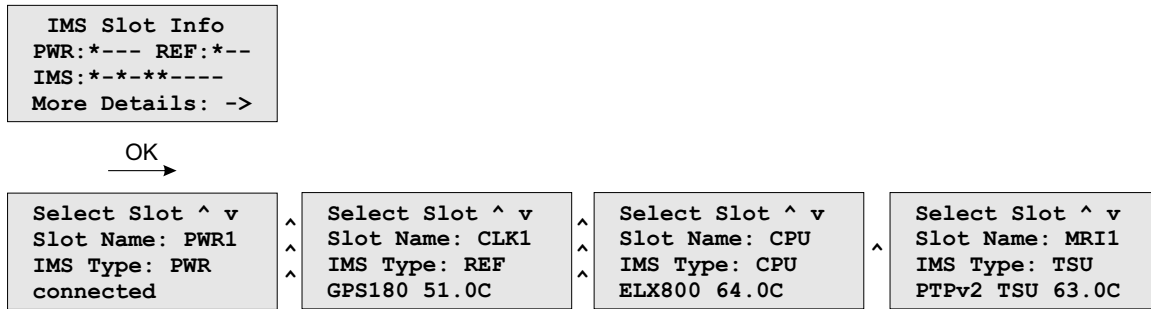
PWR:\*— This string means PWR 1 is occupied and active.

REF:\*— CLK 1 is occupied, CLK 2 and RSC (SCU slot) are empty.

IMS:\*-\*-\*— Indicates that the IMS slots MRI 1, ESI 1 and IO 1 and IO2 are occupied and active.

More Details: ->With the OK button you can open the submenu "Select Slot"

### 9.3.6.7 Option: IMS Menu Select Slots



This menu shows which module is inserted into the selected slot.

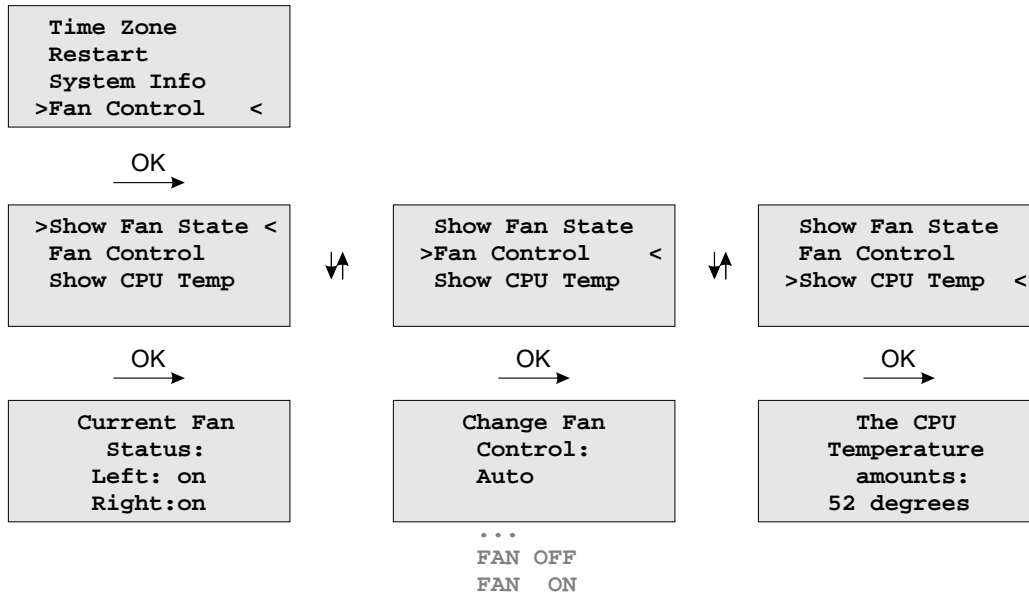
**Displayed values are:**

Slot Name: In this example, PWR 1, CLK1, CPU, MRI1, IO1 and IO2

IMS Type: PWR (power supply), REF (receiver), CPU (processor unit), LIU (Telecom outputs) ...

On the bottom line, the current operating temperature (degrees/celsius) is displayed.

## 9.3.6.8 Option: Fan Control



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:

- FAN ON**     the ventilators are always running
- FAN OFF**    the ventilators are off
- Auto**        the ventilation runs from the temperature, which is specified by the "Temperature Threshold" parameter (see "The Web Interface").  
The default value is +55 degrees celsius. If the temperature of the device is less than 7 degrees (Celsius) as the specified value, the fan control turns off automatically.

### 9.3.7 USB Stick Menu

LANTIME NTP servers provide an USB interface for connecting an USB storage device. The USB stick can be used in combination with the LANTIME or the LAN-CPU for various tasks:

- Transfer configuration parameters between different LANTIMEs
- Keypad locking for secure using the keypad of the LCD
- Transfer of log files
- Install Software Updates
- Upload and download secure certificates (SSL, SSH) and passwords



When connecting the USB stick the LC-Display will – after a few seconds – signal that the USB stick has been detected and allows you to enter the USB menu with the "OK" button.

```
USB Memory Stick
(OK to confirm)
```

The desired menu function can be chosen by using ↑ and ↓ keys and it will be activated with the "OK" button. You can leave this menu with removing the USB storage or with the "ESC" button.

#### Menu "Install Firmware"

If a firmware update file is stored on the USB stick, the menu item "Install [Firmware Version]" appears on the display. Now you can install the update package on the LANTIME by pressing the OK button. The file format is *firmware-6.24.020-x86.rel*. However, only the version is shown in the display, in this example *6.24.020-x86*.

```
USB Stick Menu
(OK to confirm)
Install
7.xx.xxx-x86
```

#### Note:

After uploading the new firmware to the LANTIME the new version has to be activated via the web interface (menu "System → Firmware/Software Update") or the CLI (Command Line Interface).

**Menu "Save as Startup"**

If this menu item is confirmed with the OK key, the firmware configuration of the LANTIME currently marked as "Start configuration" is saved on the USB stick.

```
USB Stick Menu
(OK to confirm)
Save as Startup
```

**Please Note:**

Even if you are currently making changes to a LANTIME, you can only save the configuration on the USB stick which you have confirmed via the web interface as "Startup configuration". This has the advantage that you can save your "old" configuration even if you make extensive changes to the settings of your system.

**Menu "Backup Configuration to USB Stick"**

With this submenu you can copy the configuration file from your LANTIME to the USB storage device. The stored configuration you can then find on your USB stick under */Lantime/Config/USB\_Backup/xxxxxxxxxxx* (xxx... = the 12-digit serial number of your LANTIME).

**Note:**

The configuration copied to the USB stick is always the currently stored "Start-up configuration" of the system.

```
USB Stick Menu
(OK to confirm)
Backup Config.
to USB Stick
```

If the backup is to be imported on other LANTIMES, the directory must be renamed:  
*/Lantime/Config/USB\_Backup/ANY\_SN*

**Menu "Write Diagnostic File to USB Stick"**

```
USB Stick Menu
(OK to confirm)
Write Diag. File
to USB Stick
```

This submenu is an easy way to get the contents of the LANTIMES diagnostic files. After you push the OK button, the system will copy a file archive to your USB device: */Lantime/Diag/ltdiag.tgz*

### Keypad locking

The USB stick can be used for locking the function buttons of the LANTIME LC Display. Activating this feature the user cannot use the buttons without connecting the USB stick to the LANTIME. The access authorisation has been realized with a password file on the USB stick `/Lantime/keypad_lock`. This password file will be compared with `/mnt/flash/config/keypad_lock`. So it is possible to manage different LANTIME with one USB stick.

The keypad locking will be activated with a submenu from the USB stick:

```

USB Stick Menu
(OK to confirm)
  Lock
  Front Panel
    
```

When activating this submenu the file `/mnt/flash/config/keypad_lock` will be copied to the internal flash. When de-activating the keypad locking this file will be removed from the internal flash.

```

USB Stick Menu
(OK to confirm)
  Unlock
  Front Panel
    
```

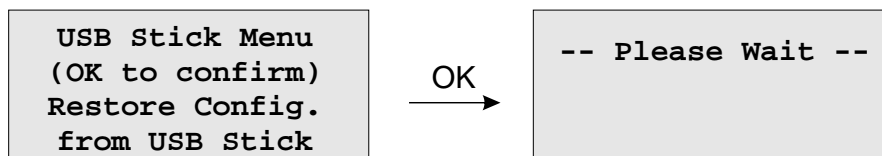
**Note:**

Make sure, that you never loose the "Keypad\_Lock" file or the USB storage device! If you have problems, please contact Meinberg Radio clocks: [Mail to techsupport@meinberg.de](mailto:techsupport@meinberg.de) .

### Menu Restore Configuration

This command is for restoring the LANTIME configuration. The Timeserver restarts after this procedure.

1. A USB stick is required, on which a backup file is stored
2. The backup will only be imported, if a directory with the appropriate SN is available (or "ANY\_SN")
3. After "Restore" the config is not bootable yet. To activate this, you must first execute the 'saveconfig' command via a CLI (console program) or use the web interface and press the "Save as Startup Configuration" button.



## 9.4 Via Serial Connection

### Initial Start of Operation: LANTIME Configuration Wizard

After the boot-phase of the device, you have to establish a serial connection with the LAN-CPU. Via the terminal connection it is possible to configure parameters with a command line interface. Use a NULL-Modem cable or a CAB-CONSOLE-RJ45 cable to connect your PC or Laptop. You can use for example the standard Hyperterminal program, shipped with your Windows operating system. Configure your terminal program with 38400 Baud, 8 Databits, no parity and 1 Stopbit. The terminal emulation has to be set to VT100. After connecting the LANTIME the login message appears (press RETURN for initial connection):

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:

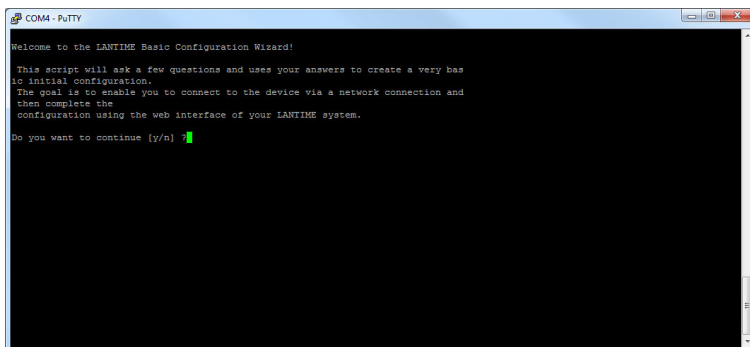
Login: **root**

Password: **timeserver**

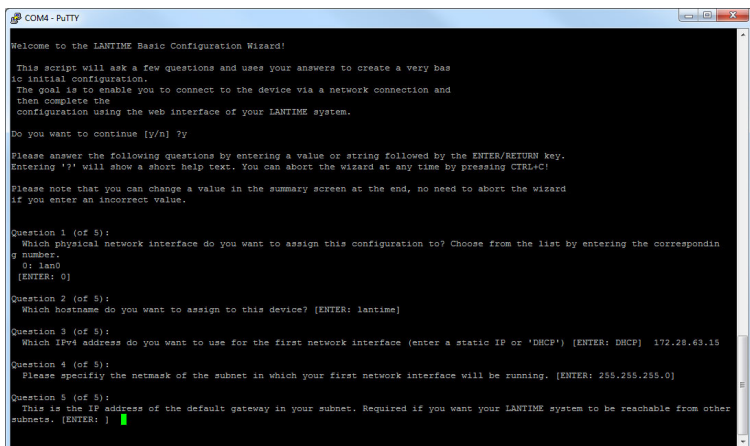
(It may be the case to press a RETURN button again).

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:



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



At the end please confirm your configuration.

After the lantime has been assigned to a correct IP address, all other settings can be done via the extensive and powerful web interface (see chapter [Via Web GUI](#)).

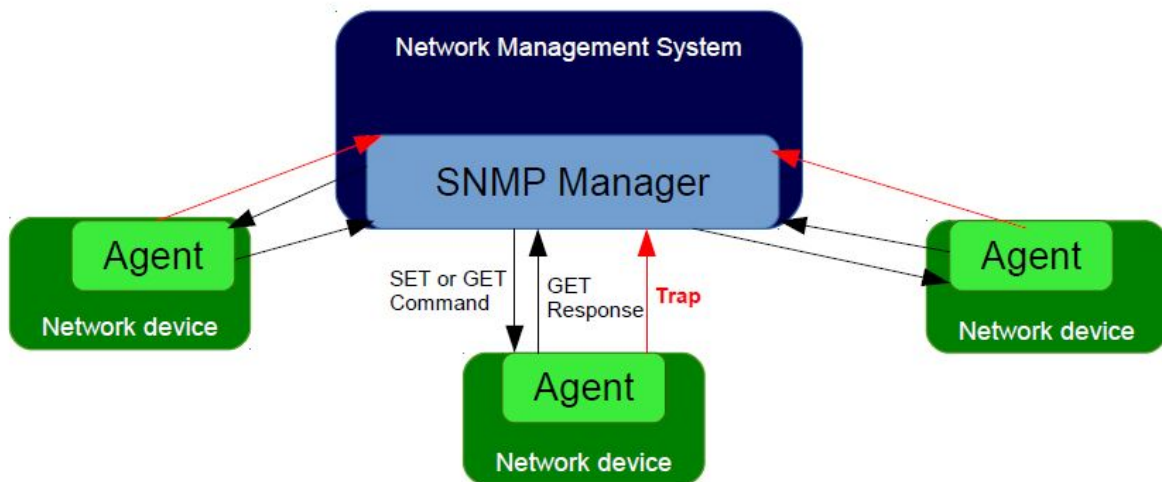


## 9.5 Via SNMP

### 9.5.1 The Simple Network Management Protocol

Most network connected devices support a number of management options including the Simple Network Management Protocol, or SNMP. SNMP is a network protocol which allows a single network management system to monitor a large number of devices on the network.

The way it works is each network element has an Agent which communicates with the Manager via SNMP. Each Agent has a corresponding Management Information Base, or MIB. The MIBs organize data elements in a tree structure. It is written in a standard, highly structured language so that the MIBs from all of the devices on the network can be compiled into the same Manager.



MIB elements are called Object Identifiers or OIDs. They consist of configuration variables, status variables, tree structure labels and notifications. The OIDs can be read or changed using SNMP SET and GET commands. There are also recursive commands which allow the Manager to ask for all of the OIDs in a branch (subtree), or even the whole tree. This process is referred to as "walking the MIB". Event Notifications, commonly referred to as traps, are a special type of OID. A trap can be configured so that when the status of the device changes a message is immediately sent from the Agent to the Manager.

## 9.5.2 MIB Objects of a LANTIME

An LTOS operating systems running on Meinberg LANTIME servers supports all SNMP versions (v1,v2c and v3) with a full functionality. The LANTIME propriatery OIDs are structured into subtrees, which define a particular system component or a mode of operation. The main subtree with OIDs referring to the LANTIME status of different modes is called LantimeNGStatus, NG standing for New Generation of LANTIME features in the LANTIME firmware. The LantimeNGStatus consists of eight subtrees, where Refclock, NTP, PTP, SystemHardware, Cluster and Misc are the most important to monitor.

### 9.5.2.1 Refclock subtree

Here is a short list of OIDs from the NGStatus subtree with corresponding descriptions:

#### mbgLiNgRefclockState

This OID describes a current state of a LANTIME refclock (hardware clock module) referring to GNSS or any other time source signal in MRS (Multi Reference Source) model.

Status	Description
0:	<p><u>refclock is not available:</u> See the possible troubleshooting:</p> <ol style="list-style-type: none"> <li>1. Refclock module cannot be accessed.</li> <li>2. Check if it is damaged and replace it if necessary.</li> </ol>
1:	<p><u>synchronized:</u> The reflock of your system is correctly synchronized to the selected time source (GPS or MRS). In an MRS system, a refclock can be synchronized to a reference time source from the priority list. See an example in the next figure.</p> <p>The MRS system above synchronizes first to GPS, but if the GPS signal is unavailable, the refclock switches to the next time source from the priority list (PTP in our case). The switch happens only after a trust time of the unavailable time source (GPS signal) has run out. This is to prevent hopping from one time source to another in short time periods. If GPS becomes available again, the refclock switches back to GPS, without waiting for the PTP trust time in this case, since GPS itself a higher precision than PTP.</p>
2:	<p><u>not synchronized:</u> Obviously the refclock is not synchronized to its time source. Here is the possible troubleshooting:</p> <ol style="list-style-type: none"> <li>A) Check if the GPS antenna is connected and reference time received. More about how to mount and position Meinberg GPS antenna correctly learn here.</li> <li>B) If GPS is the current time source, check number of satellites in view. There should be at least four to provide sync information.</li> <li>C) Start "warm boot" to refresh current satellite position. This is useful especially if the physical position of your LANTIME has been displaced by more than 100 km from its previous location and therefore obsolete satellite data are still stored in the system.</li> <li>D) Start "cold boot" to update a satellite almanac.</li> <li>E) If nothing from above helps, the GPS clock module needs to be changed.</li> </ol>

It is recommended configuring your network management software to check this status regularly, if possible every 60 s.

**mbgLtNgRefclockLeapSecondDate**

This OID conveys information about the next Leap Second Date. If the upcoming Leap Second Date has not been announced yet, the OID holds information about the previous leap second event.

Here is short summary of the leap seconds. There are two different timescales we usually talk about in the sync environment: GPS, which stands for Global Positioning System time and UTC (Universal Time Co-ordinated), formerly known as GMT (Greenwich Mean Time). They differ from each other by number of leap seconds introduced since beginning of GPS time on 6-Jan-1980. In the moment of writing the UTC is 16 seconds behind the GPS time, which is due to the uneven rotation of the Earth.

```
Since the introduction of a new leap second influences the time in the whole system being synchronized, we suggest to check this status regularly, e.g. 1/hour.
```

Next in a row of OIDs are those referring to NTP status. They can be found in the “mbgLtNgNtp” subtree.

### 9.5.2.2 NTP subtree

Here is a short list of OIDs from the NGStatus subtree with corresponding descriptions:

#### mbgLiNgNtpCurrentState

This is one of the most important OID in this subtree to check regularly. It informs about the NTP service of your LANTIME. There are three states possible:

Status	Description
0:	<p><u>not available</u>: See the possible troubleshooting:</p> <p>A) Check if NTP service is actually enabled at a given LAN interface. To check it, log in to a webinterface. Factory default credentials: root/timeserver. Go to menus: "Network → Network Services" and activate the service of the corresponding interface. See Figure 3 for details.</p> <p>B) Check if it is damaged and replace it if necessary.</p>
1:	<p><u>not synchronized</u>: In case of "not synchronized" the NTP service is not yet synchronized to a reference clock. Possible causes for this state are as follows:</p> <p>A) NTP daemon is still in its initialization phase for which it needs approx. 3-5 min. Therefore wait a while and see if the status changes.</p> <p>B) If a refclock is not sync, the same is indicated in the NTP status. In such case NTP daemon is switched to synchronize to its local clock and its stratum value changes to 12. Please check the possible troubleshooting for a refclock status as described above.</p>
2:	<p><u>synchronized</u>: The NTP service is in normal operation. The LANTIME is now working properly.</p>

It is recommended to check NTP status regularly, but not more than every 64 s.

### 9.5.2.3 Hardware subtree

#### mbgLtNgSysPsStatus

If a LANTIME has a redundant power supply (RPS) unit, it is important to check the status of both RPS modules regularly. This PowerSupplyStatus OID can be found in the System Hardware subtree. The following states are available:

Status	Description
0:	<u>notAvailable</u> : The queried power supply unit is not recognized by a system. Check to see if it is damaged, and replace it if necessary.
1:	<u>down</u> : The power supply unit of interest is not in service. Check to see if it is damaged, and replace it if necessary.
2:	<u>up</u> : The queried power supply module is in operation.

It is recommended to check this OID every 60 s.

### 9.5.2.4 Misc subtree

#### mbgLtNgEthPortLinkState

In the mbgLtNgMisc subtree one can find an EthPortLinkState OID which identifies the status of each physical Ethernet port of a LANTIME. Available values:

Status	Description
0:	<u>notAvailable</u> : The queried port is down, check the link LED. If faulty, replace the network card.
1:	<u>up</u> : The port of interest is in normal operation.

It is recommended to check this OID every 60 s.

### 9.5.2.5 PTP subtree

If your LANTIME has IEEE 1588 PTPv2 functionality, the corresponding PTP OIDs can be found in the “mbgLtNgPtp” subtree. These are the most important OIDs to monitor:

#### mbgLiNgPtpPortState

The following PTP Port States are possible:

Status	Description
0:	<u>uninitialized</u> : The port is booting up, the software daemon has not yet started, the IP address is not yet assigned.
1:	<u>initializing</u> : In this state the port initializes its data sets, hardware, and communication facilities.
2:	<u>faulty</u> : Not defined in a LANTIME.
3:	<u>disabled</u> : PTP service has been disabled on this port, either by user configuration or because the module is in a standby mode.
4:	<u>listening</u> : The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.
5:	<u>preMaster</u> : A short transitional state while the port is becoming a master.
6:	<u>master</u> : The port is a current master.
7:	<u>passive</u> : The port is in passive mode, meaning there is another master clock active in the PTP domain. The port can enter master state when it wins the BMCA due to a failure/service degradation of the current master.
8:	<u>uncalibrated</u> : One or more master ports have been detected in the domain.
9:	<u>slave</u> : The port has successfully subscribed to a master and receives all expected messages. It also successfully measured the path delay using delay request messages.

It is recommended to monitor the PtpPortState OID every 3 s

### 9.5.3 SNMP Traps

**SNMP Trap Name:** mbgLtNgTrapNTPNotSync  
**OID:** .1.3.6.1.4.1.5597.30.3.0.1  
**Severity:** Warning or critical  
**Short explanation:** the trap is sent when NTP is not synchronized  
**Reference to other chapters:** [Troubleshooting and Alarming](#) → [NTP Messages](#) → [NTP Not Sync](#)  
**Cleared By:** mbgLtNgTrapNTPSync

**SNMP Trap Name:** mbgLtNgTrapNTPStopped  
**OID:** .1.3.6.1.4.1.5597.30.3.0.2  
**Severity:** Critical  
**Short explanation:** trap to be sent when NTP is stopped  
**Reference to other chapters:** [Troubleshooting and Alarming](#) → [NTP Messages](#) → [NTP Stopped](#)  
**Cleared By:** MbgLtNgTrapNTPSync or mbgLtNgTrapNTPNotSync

**SNMP Trap Name:** mbgLtNgTrapServerBoot  
**OID:** .1.3.6.1.4.1.5597.30.3.0.3  
**Severity:** Info  
**Short explanation:** trap to be sent when time server has finished boot sequence  
**Reference to other chapters:** no further information  
**Cleared By:** -

**SNMP Trap Name:** mbgLtNgTrapReceiverNotResponding  
**OID:** .1.3.6.1.4.1.5597.30.3.0.4  
**Severity:** Critical  
**Short explanation:** trap to be sent when receiver is not responding  
**Reference to other chapters:** [Troubleshooting and Alarming](#) → [Reference Clock](#) → [CLK Not Rspnding](#)  
**Cleared By:** MbgLtNgTrapReceiverNotSync or mbgLtNgTrapReceiverSync

**SNMP Trap Name:** mbgLtNgTrapReceiverNotSync  
**OID:** .1.3.6.1.4.1.5597.30.3.0.5  
**Severity:** Error  
**Short explanation:** trap to be sent when receiver is not synchronised  
**Reference to other chapters:** [Troubleshooting and Alarming](#) → [Reference Clock](#) → [CLK Not Sync](#)  
**Cleared By:** mbgLtNgTrapReceiverSync

**SNMP Trap Name:** mbgLtNgTrapAntennaFaulty  
**OID:** .1.3.6.1.4.1.5597.30.3.0.6  
**Severity:** Critical  
**Short explanation:** trap to be sent when connection to antenna is broken  
**Reference to other chapters:** [Troubleshooting and Alarming](#) → [Reference Clock](#) → [Antenna Faulty](#)  
**Cleared By:** mbgLtNgTrapAntennaReconnect

**SNMP Trap Name:** mbgLtNgTrapAntennaReconnect  
**OID:** .1.3.6.1.4.1.5597.30.3.0.7  
**Severity:** Clearing event  
**Short explanation:** trap to be sent when antenna has been reconnected  
**Reference to other chapters:** no further information  
**Cleared By:** -

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapConfigChanged
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.8
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when timeserver reloaded its configuration
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapLeapSecondAnnounced
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.9
<b>Severity:</b>	Info Warning
<b>Short explanation:</b>	trap to be sent when a leap second has been announced
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">Ref. Clock</a> → <a href="#">Leap Second Announced</a> <a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">NTP</a> → <a href="#">Leap Second Handling</a>
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapSHSTimeLimitError
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.10
<b>Severity:</b>	Critical
<b>Short explanation:</b>	trap to be sent when SHS timelimit exceeded
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">Ref. Clock</a> → <a href="#">SHS Time Limit Warning</a> <a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Introduction</a> <a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Security</a> → <a href="#">SHS Mode</a> <a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Security</a> → <a href="#">SHS Time Limit</a>
<b>Cleared By:</b>	mbgLtNgTrapSHSTimeLimitOk

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapSecondaryRecNotSync
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.11
<b>Severity:</b>	Warning
<b>Short explanation:</b>	trap to be sent when secondary receiver is not synchronised
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">Ref. Clock</a> → <a href="#">CLK Not Sync</a>
<b>Cleared By:</b>	mbgLtNgTrapSecondaryRecSync

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPowerSupplyFailure
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.12
<b>Severity:</b>	Critical
<b>Short explanation:</b>	trap to be sent when one of the redundant power supplies fails
<b>Reference to other chapters:</b>	<a href="#">Important Safety Information</a> → <a href="#">Security during Installation</a> <a href="#">Important Safety Information</a> → <a href="#">Safety during Operation</a>
<b>Cleared By:</b>	mbgLtNgTrapPowerSupplyUp

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapAntennaShortCircuit
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.13
<b>Severity:</b>	Critical
<b>Short explanation:</b>	trap to be sent when a connected antenna fails due to a short circuit
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">Ref. Clock</a> → <a href="#">Antenna Short Circuit</a>
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapReceiverSync
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.14
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when receiver is synchronised
<b>Reference to other chapters:</b>	<a href="#">Antenna and Receiver Information</a> → <a href="#">Reference Time Sources</a>
<b>Cleared By:</b>	-

---



SNMP Trap Name:	mbgLtNgTrapNTPClientAlarm
OID:	.1.3.6.1.4.1.5597.30.3.0.15
Severity:	Error
Short explanation:	trap to be sent when an NTP Client Monitoring alarm occurs, e.g. when a monitored client is not reachable
Reference to other chapters:	check the network configuration in LTOS 6 Managm./Mon. → Network
Cleared By:	-
SNMP Trap Name:	mbgLtNgTrapPowerSupplyUp
OID:	.1.3.6.1.4.1.5597.30.3.0.16
Severity:	Info
Short explanation:	trap to be sent when a power supply returned to a healthy state
Reference to other chapters:	no further information
Cleared By:	-
SNMP Trap Name:	mbgLtNgTrapNetworkDown
OID:	.1.3.6.1.4.1.5597.30.3.0.17
Severity:	Critical
Short explanation:	trap to be sent when a monitored network port is down
Reference to other chapters:	Troubleshooting and Alarming → Network → Network Link Down
Cleared By:	mbgLtNgTrapNetworkUp
SNMP Trap Name:	mbgLtNgTrapNetworkUp
OID:	.1.3.6.1.4.1.5597.30.3.0.18
Severity:	Clearing event
Short explanation:	trap to be sent when a monitored network port is up
Reference to other chapters:	no further information
Cleared By:	-
SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotRespp
OID:	.1.3.6.1.4.1.5597.30.3.0.19
Severity:	Warning or critical
Short explanation:	trap to be sent when secondary receiver is not responding
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → CLK Not Responding
Cleared By:	mbgLtNgTrapSecondaryRecSync
SNMP Trap Name:	mbgLtNgTrapMrsLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.30
Severity:	Warning
Short explanation:	trap to be sent when a reference offset exceeds the configured limit
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Clock → MRS Settings Troubleshooting and Alarming → Ref. Clock → MRS Limit Exceed
Cleared By:	-
SNMP Trap Name:	mbgLtNgTrapMrsRefDisconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.31
Severity:	Critical
Short explanation:	trap to be sent when a reference signal has been lost
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → MRS Reference Disconnected
Cleared By:	mbgLtNgTrapMrsRefReconnect

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapMrsRefReconnect
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.32
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when a reference signal recovered
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapFdmError
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.33
<b>Severity:</b>	Critical
<b>Short explanation:</b>	trap to be sent when the Fdm module generates an alarm
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">FDM</a> → <a href="#">FDM Configuration</a>
<b>Cleared By:</b>	mbgLtNgTrapFDMOk

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapSHSTimeLimitWarning
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.34
<b>Severity:</b>	Warning Critical
<b>Short explanation:</b>	trap to be sent when SHS warning limit exceeded
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Introduction</a> <a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Security</a> → <a href="#">SHS Configuration</a> <a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Security</a> → <a href="#">SHS Mode</a> <a href="#">Troubleshooting and Alarming</a> → <a href="#">Ref. Clock</a> → <a href="#">SHS Time Limit Warning</a>
<b>Cleared By:</b>	mbgLtNgTrapSHSTimeLimitOk

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapSecondaryRecSync
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.35
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when secondary receiver is synchronised
<b>Reference to other chapters:</b>	<a href="#">Antenna and Receiver Information</a> → <a href="#">Reference Time Sources</a>
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapNTPSync
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.36
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when NTP is synchronised
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPtpPortDisconnected
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.37
<b>Severity:</b>	Warning or critical
<b>Short explanation:</b>	trap to be sent when PTP network port got disconnected
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">PTP</a> → <a href="#">PTP Global Status</a>
<b>Cleared By:</b>	mbgLtNgTrapPtpPortConnected

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPtpPortConnected
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.38
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when PTP network port got connected
<b>Reference to other chapters:</b>	no further Information
<b>Cleared By:</b>	-

---

---

**SNMP Trap Name:** mbgLtNgTrapPtpStateChanged  
**OID:** .1.3.6.1.4.1.5597.30.3.0.39  
**Severity:** Info Warning  
**Short explanation:** trap to be sent when PTP state changed (e.g. from 'passive' to 'master')  
**Reference to other chapters:** [LTOS 6 Managm./Mon.](#) → [Web GUI](#) → [PTP](#) → [PTP Global Status](#)  
**Cleared By:** -

---

**SNMP Trap Name:** mbgLtNgTrapPtpError  
**OID:** .1.3.6.1.4.1.5597.30.3.0.40  
**Severity:** Warning Critical  
**Short explanation:** trap to be sent when PTP raised an error  
**Reference to other chapters:** [LTOS 6 Managm./Mon.](#) → [Web GUI](#) → [PTP](#) → [PTP Global Status](#)  
**Cleared By:** -

---

**SNMP Trap Name:** mbgLtNgTrapLowSystemResources  
**OID:** .1.3.6.1.4.1.5597.30.3.0.41  
**Severity:** Clearing event  
**Short explanation:** trap to be sent when system is running on low resources  
**Reference to other chapters:** no further information  
**Cleared By:** mbgLtNgTrapSufficientSystemResources

---

**SNMP Trap Name:** mbgLtNgTrapFanDown  
**OID:** .1.3.6.1.4.1.5597.30.3.0.45  
**Severity:** Critical  
**Short explanation:** trap to be sent when fan goes down  
**Reference to other chapters:** [Troubleshooting and Alarming](#) → [Miscellaneous](#) → [Fan Failure](#)  
**Cleared By:** mbgLtNgTrapFanUp

---

**SNMP Trap Name:** mbgLtNgTrapFanUp  
**OID:** .1.3.6.1.4.1.5597.30.3.0.46  
**Severity:** Clearing event  
**Short explanation:** trap to be sent when fan comes up  
**Reference to other chapters:** no further information  
**Cleared By:** -

---

**SNMP Trap Name:** mbgLtNgTrapCertificateExpired  
**OID:** .1.3.6.1.4.1.5597.30.3.0.47  
**Severity:** Info or warning  
**Short explanation:** trap to be sent when HTTPS certificate expires or will expire  
**Reference to other chapters:** [LTOS 6 Managm./Mon.](#) → [Web GUI](#) → [Security](#) → [HTTPS Certificate](#)  
**Cleared By:** -

---

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapSufficientSystemResources
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.48
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when system has regained sufficient resources
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapOscillatorWarmedUp
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.49
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when oscillator is warmed up
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapOscillatorNotWarmedUp
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.50
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when oscillator is not warmed up
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">Ref. Clock</a> → <a href="#">Oscillator not Adjusted</a>
<b>Cleared By:</b>	mbgLtNgTrapOscillatorWarmedUp

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapMrsRefChanged
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.51
<b>Severity:</b>	Info Warning
<b>Short explanation:</b>	trap to be sent when MRS reference source changed
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapClusterMasterChanged
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.52
<b>Severity:</b>	Warning
<b>Short explanation:</b>	trap to be sent when cluster mode is active and cluster changed
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Network</a> → <a href="#">Network Interf.</a> - <a href="#">Cluster</a>
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapClusterFalsetickerDetected
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.53
<b>Severity:</b>	Warning
<b>Short explanation:</b>	trap to be sent when cluster mode is active and a cluster member is detected as falseticker
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Network</a> → <a href="#">Network Interf.</a> - <a href="#">Cluster</a>
<b>Cleared By:</b>	mbgLtNgTrapClusterFalsetickerCleared

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapClusterFalsetickerCleared
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.54
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when cluster mode is active and a cluster member is no longer a falseticker
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapSHSTimeLimitOk
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.55
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when SHS timelimit error has been acknowledged or time difference drops below warning limit
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">Introduction</a>
<b>Cleared By:</b>	-
<b>SNMP Trap Name:</b>	mbgLtNgTrapIMSError
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.56
<b>Severity:</b>	Critical
<b>Short explanation:</b>	trap to be sent when an IMS module is not responsive anymore has got temperature issues, etc.
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">Miscellaneous</a> → <a href="#">IMS Error</a>
<b>Cleared By:</b>	mbgLtNgTrapIMSOk
<b>SNMP Trap Name:</b>	mbgLtNgTrapIMSOk
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.57
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when an IMS module returns to healthy state
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-
<b>SNMP Trap Name:</b>	mbgLtNgTrapFDMOk
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.58
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when an FDM module returns to healthy state
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managm./Mon.</a> → <a href="#">Web GUI</a> → <a href="#">FDM</a> → <a href="#">FDM Configuration</a>
<b>Cleared By:</b>	-
<b>SNMP Trap Name:</b>	mbgLtNgTrapNTPOffsetLimitExceeded
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.59
<b>Severity:</b>	Error
<b>Short explanation:</b>	trap to be sent when monitoring an NTP client and its offset limit is exceeded
<b>Reference to other chapters:</b>	<a href="#">Troubleshooting and Alarming</a> → <a href="#">NTP</a> → <a href="#">NTP Offset Limit Exceeded</a>
<b>Cleared By:</b>	-
<b>SNMP Trap Name:</b>	mbgLtNgTrapNTPOffsetLimitOk
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.60
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when monitoring an NTP client and its offset limit is back again in a valid range
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	mbgLtNgTrapNTPOffsetLimitExceeded
<b>SNMP Trap Name:</b>	mbgLtNgTrapXheRubError
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.61
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when external rubidium announces OK
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapXheRubError
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.62
<b>Severity:</b>	Error
<b>Short explanation:</b>	trap to be sent when external rubidium announces error
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPowerConsumptionExceeded
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.63
<b>Severity:</b>	Warning
<b>Short explanation:</b>	trap to be sent when device consumes too much power
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	mbgLtNgTrapPowerConsumptionOk

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPowerConsumptionOk
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.64
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when device has got enough power
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPowerRedundancyNotAvail
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.65
<b>Severity:</b>	Warning
<b>Short explanation:</b>	trap to be sent when there currently is no power supply backup avail
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	mbgLtNgTrapPowerRedundancyAvail

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapPowerRedundancyAvail
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.66
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when there is at least one power supply as backup
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapTrustedSourceError
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.67
<b>Severity:</b>	Warning
<b>Short explanation:</b>	trap to be sent when a MRS source's time deviation exceeds a configured limit
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	mbgLtNgTrapTrustedSourceOk

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapTrustedSourceOk
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.68
<b>Severity:</b>	Clearing Event
<b>Short explanation:</b>	trap to be sent when a MRS source's time deviation returns to its configured bounds
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapNormalOperation
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.77
<b>Severity:</b>	Clearing event
<b>Short explanation:</b>	trap to be sent when the system returned to a healthy state
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapHeartbeat
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.88
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent periodically to indicate that time server is still alive
<b>Reference to other chapters:</b>	<a href="#">LTOS 6 Managem./Mon. → Notifications → Miscellaneous - Enable Heartbeat</a>
<b>Cleared By:</b>	-

---

<b>SNMP Trap Name:</b>	mbgLtNgTrapTestNotification
<b>OID:</b>	.1.3.6.1.4.1.5597.30.3.0.99
<b>Severity:</b>	Info
<b>Short explanation:</b>	trap to be sent when a test notification has been requested
<b>Reference to other chapters:</b>	no further information
<b>Cleared By:</b>	-

---

# 10 Troubleshooting and Alarming

## 10.1 NTP Messages

### Error and System message / Explanation

#### *NTP Not Sync /*

The NTP service of a LANTIME is not sync.

### Troubleshooting / Additional information

- For LANTIMEs with built-in reference clock, please check the status of the clock on the main page. If the reference clock is not synchronized, please refer to the troubleshooting information for "CLK Not Sync".
- For LANTIMEs, which are to be synchronized by external NTP servers, make sure that the external NTP servers are reachable.
- For MRS devices, check whether MRS reference time sources are configured in the Web interface (→ Clock → MRS settings) and corresponding signals are available (→ Clock → MRS status).
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

#### *NTP Stopped /*

The NTP service stopped

- Info: After every configuration change relevant to the NTP, the NTP service is stopped and restarted. In this case, a message 'NTP Stopped' is written into the system log of the LANTIME.
- Contact the Meinberg TechSupport and provide a LANTIME diagnostic file, if 'NTP Stopped' is permanently displayed as NTP status in the front panel or in the web interface.

#### *NTP Offset Limit Exceeded /*

LANTIME generates this message if the internal time offset between LANTIME system time and the reference clock is higher than the configured threshold value.

- Check the configured threshold value in the Web Interface: "NTP → Special Settings → Max. Internal Offset (ms.)"
- Note: After restarting the LANTIME it takes several minutes, depending on the reference time source, until the internal offset is  $< \pm 1$  ms.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.



## 10.2 Ref. Clock Messages

### Error and System message / Explanation

#### *CLK Not Responding /*

The LANTIME can no longer communicate with its internal reference clock.

#### *CLK Not Sync /*

Performance and system resources issue of the NTP

### Troubleshooting / Additional information

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file.

LANTIME with GNSS reference clock (GPS/GLN/GNS):

- Check the antenna position:
- If the GPS reference clock is connected to a GPS antenna distributor GPSAV4 (<https://www.meinbergglobal.com/english/products/gps-antenna-distributor.htm>), make sure that the "Clock 1" port of the GPSAV4 is attached, since the GPSAV4 and the antenna are supplied by power via this port.

LANTIME with a longwave receiver (DCF77-PZF/WWVB/MSF/JJY):

- Check the antenna position

LANTIME with TCR reference clock (IRIG):

- Check whether the timecode input port at the back of the LANTIME is correctly connected to an IRIG source. In the Web interface, check whether the correct IRIG input code has been configured (Clock → IRIG Settings → Input Timecode). The input timecode is the IRIG code provided to the LANTIME by the IRIG source.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

**Antenna Faulty /**

GNSS reference clock (GPS/GLN/GNS):  
The antenna has not been detected.

- Check the connections between the antenna and a LANTIME.
- Check the output voltage at the LANTIME antenna connector.
- To do this, disconnect the antenna cable from the LANTIME antenna port. The following voltage value should
- be measured between the inner and outer conductor:
  - GPS Receiver → 15-18 V DC
  - GLN Receiver → 5V DC
  - GNS Receiver → 5V DC
- If the voltage is 0V DC, please contact the Meinberg TechSupport:
- If the measured voltage at the antenna port of the LANTIME is correct, reconnect the antenna cable and
- check the voltage at the other end of the antenna cable.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

Longwave receiver (DCF77-PZF/WWVB/MSF/JJY):  
Either the antenna or any other input signal has not been detected.

- Check the connections between the antenna and a LANTIME.
- Check the status of the received antenna signal in the main page of the web interface. The displayed field strength value should be  $> 40$ . If this is not the case, please check how the antenna is positioned.
- Check the output voltage at the LANTIME antenna connector.
- To do this, disconnect the antenna cable from the LANTIME antenna port. The following voltage value should be measured between the inner and outer conductor: Long Wave Receiver → 5 V DC
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

### Antenna Short Circuit /

Short circuit at the antenna connection.

- Disconnect the antenna cable from the LANTIME antenna connector.
- Perform a powercycle of the device
- If the LANTIME does not show the error message after the start-up, connect the antenna again. Otherwise contact the Meinberg TechSupport and provide a LANTIME diagnostic file.

### GPS Warm Boot /

In warm boot mode, the GPS reference clock performs the position determination. To complete this process successfully, at least 4 satellites should be received. After successful position determination, the position will be stored in the battery-buffered memory of the clock. Thus the position determination does not to be carried out again after a restart.

- If the LANTIME can not complete the GPS warm boot process, check the number of "good satellites" that can be viewed in the web interface: "Clock → GPS (GNSS Clock → Receiver Information → Number of good satellites".
- If the number of good satellites is permanently below 4 and the LANTIME can not complete the position determination, then refer to the troubleshooting case for "CLK Not Sync".
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

### GPS Cold Boot /

In GPS Cold Boot mode, the GPS reference clock tries to download the GPS almanac, which contains the satellite track data for all satellites. To complete this process, at least 1 satellite should be received. The process takes at least 12 minutes. After the cold boot is completed, the clock automatically switches to the GPS warm boot to determine the position.

The GPS almanac is stored in the battery-buffered memory of the clock.

- If the LANTIME can not complete the GPS Cold Boot operation after more than 30 minutes, check the number of "good satellites" in the web interface: "Clock → GPS (GNSS Clock → Receiver Information → Number of good satellites".
- If the number of good satellites is 0, then refer to the troubleshooting case for "CLK Not Sync".
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

**SHS Time Limit Warning /**

LANTIME systems with two built-in reference clocks send out this message as soon as the time difference between both clocks exceeded the pre-configured "Time Limit Warning Level" setting.

- Check the current time difference between the two reference clocks in the main menu of the web interface.
- Check your SHS configuration under "Security → SHS Configuration". Are the configured thresholds possibly too strict?
- Check the status of both reference clocks in the main menu of the web interface. If one of the two clocks is not synchronized, please refer to the troubleshooting case for "CLK Not Sync".
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

**Oscillator not Adjusted /**

The internal oscillator is not (yet) fully disciplined. As soon as this process is finished, the LANTIME sends out a log message "Oscillator Adjusted". The time needed for an oscillator to be disciplined depends on the quality of the incoming signal, the aging and environmental influences on the oscillator.

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

**Leap Second Announced /**

LANTIMEs with a GNSS reference clock (GPS / GLN / GNS) or long wave receiver (DCF77-PZF / WWVB / MSF / JJY) send out the "Leap Second Announced" notification message as soon as they have received the announcement by the reference signal. The GPS satellites announce the upcoming leapsecond usually about half a year in advance. Long wave transmitters usually send the announcement 1 hour in advance.

- This is only an info notification, therefore no further action is required.

**XMR Limit Exceed /**

LANTIME generates this message when the measured time offset of an MRS time source has exceeded the configured threshold value.

- Check the current MRS time source status in the Web Interface under "Clock → GNSS Clock → MRS Status".
- Check the MRS configuration in the Web Interface under "Clock → GNSS Clock → MRS Settings". Are the configured threshold values (check the "Limit" column) configured possibly too strict?
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

**XMR Reference Disconnected /**

LANTIME generates this message if the configured MRS time source is no longer available.

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

## 10.3 Network Messages

**Error and System message / Explanation*****Network Link Down /***

There was no link detected at one of the LANTIME's network interface.

**Troubleshooting / Additional information**

- Check which ports are physically connected and the link should be available.
- Check for compatible network settings on switch and LANTIME.
- Check the settings for link monitoring via the Web Interface: "Network → Physical Network Configuration → Indicate Link on Front Panel LED".
  - The LANTIME monitors a link status for the ports where the "Indicate Link on Front Panel LED" option is activated.
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

## 10.4 Miscellaneous Messages

### Error and System message / Explanation

#### *Fan Failure* /

The LANTIME has detected a fault on a fan module, or a fan module has been removed during system operation.

### Troubleshooting / Additional information

- If the fan module has not been intentionally removed, contact the Meinberg TechSupport and provide a LANTIME diagnostic file.

#### *IMS Error* /

Either the LANTIME has detected an error on an IMS module or an IMS module has been plugged out of the LANTIME IMS system during the operation.

### Troubleshooting / Additional information

- If the IMS module has not been intentionally removed, contact the Meinberg TechSupport and provide a LANTIME diagnostic file.

*CPU No Response* (This error message can only appear on a display) /

The display does not receive any information from the installed LANTIME CPU unit.

### Troubleshooting / Additional information

- Check whether the LANTIME is still available over the network (try to ping, SSH, HTTP / HTTPS)
- Does a power cycle solve this problem?
- If the LANTIME is still accessible via HTTP / HTTPS, please download a diagnostic file via the web interface and send it to the Meinberg TechSupport. If no connection to the LANTIME is possible, contact the Meinberg TechSupport with the serial number of your LANTIME.

#### *Certificate Expired* /

LANTIME generates this warning 60 days, 30 days, and 15 days before the end period of the installed SSL certificate for HTTPS service.

### Troubleshooting / Additional information

- Check the validity of the installed SSL certificate via the Web Interface: "Security → HTTPS Certificate → Show SSL Certificate".
- Upload a new SSL certificate using the LANTIME Web Interface in the Security Page dialogue.: "Security → HTTPS Certificate → Upload SSL Certificate".
- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

**Low System Resource /**

LANTIME generates this warning:

directory "/var" < 1MB free

directory "/var" > 90% usage

RAM Mem free < 6MB

**Troubleshooting / Additional information**

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance for solving the problem.

# 11 Support Information

In this chapter you will learn about different levels of support at the Meinberg Company. In general, the Basic Customer Support level is included in the price you pay for your Meinberg product and demands no additional costs. It includes free e-mail, phone support and free lifetime firmware updates for the lifetime of your product, i.e. for as long as you choose to use it.

Depending on the product this level also includes a 2 or 3 year hardware warranty. You can extend the hardware warranty period after the standard warranty of your Meinberg product ends.

The chapter includes:

- Basic Customer Support
- Support Ticket System
- How to download a Diagnostic File
- Self-Help Online Tools
- NTP and IEEE 1588-PTP online tutorials
- The Meinberg Academy introduction and offerings
- Meinberg Newsletter



## 11.1 Basic Customer Support

Contact Meinberg via e-mail or phone.

Technical Support	
E-Mail	<a href="mailto:techsupport@meinberg.de">techsupport@meinberg.de</a>
Service hotline	+49 (0) 5281 / 9309-888
Service hours hotline	Mon – Thu 8:00 – 17:00, Fri 8:00 – 16:00 (CET/CEST) Not available on Sat/Sun and German Public Holidays

Office (Sales/Purchase)	
E-Mail	<a href="mailto:info@meinberg.de">info@meinberg.de</a>
Service hotline	+49 (0) 5281 / 9309-888
Service hours hotline	Mon – Thu 7:30 – 17:00, Fri 07:30 – 15:00 (CET/CEST) Not available on Sat/Sun and German Public Holidays

### MEINBERG Remote Support

In order to assist you with configuration, installation, monitoring and diagnostics of your Meinberg products, you can download a remote support software that allows Meinberg technical support to remote control your computer.

By following this link:

<https://www.meinbergglobal.com/english/support/remote.htm>

you can find all necessary information and to download the support.

### LANTIME Firmware Updates

To check if an update is available for your LANTIME, please visit;

<https://www.meinbergglobal.com/english/sw/firmware.htm>

and fill out the form. Available firmware updates will be provided by e-mail (LANTIME firmware V5 or older versions) or with a direct download link (LANTIME firmware V6 or newer).

## 11.2 Support Ticket System

Meinberg assists you quickly and directly on questions regarding the initial setup of your devices, troubleshooting or if you want to update the hard- or software. We offer free support for the whole lifetime of your Meinberg product.

- Send a mail to [techsupport@meinberg.de](mailto:techsupport@meinberg.de) with a description of your issue.
- A support ticket will automatically be opened.
- Our support engineers will contact you as soon as possible.
- It is always helpful for our engineers to receive a diagnostic file when you send a ticket.
- The diagnostic file includes all status data of a LANTIME system logged since the last reboot and can be downloaded from all LANTIME timeservers. The file format of the diagnostic file is a tgz-archive. → See chapter [How to download a Diagnostic File](#) how to generate this file at your LANTIME system.

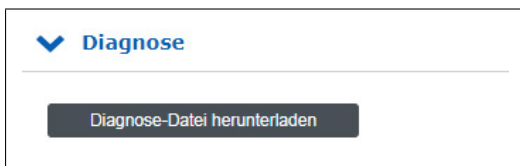
## 11.3 How to download a Diagnostic File

In most support cases the first action is to ask the customer to download the diagnostic file, because it is very helpful at identifying the current state of the LANTIME and finding possible errors. Therefore we recommend that you attach your Diagnostic File when sending a ticket to our support.

The diagnostic file includes all status data of a LANTIME system logged since the last reboot. It can be downloaded from all LANTIME timeservers or you can save the file on a USB stick connected to the device. The file format of the diagnostic file is a tgz-archive. The archive contains all the important configuration and logfiles.

### 11.3.1 Download via Web GUI

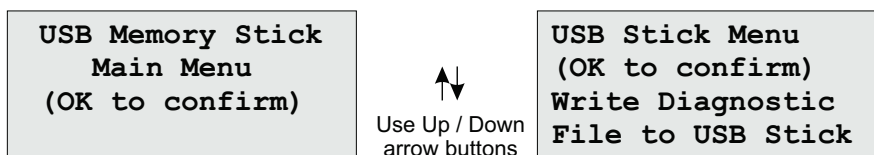
- Connect to the Web GUI by putting the IP address into the address field of the web browser.
- Open the „System“ page and the submenu "Diagnostics".
- Press the "Download Diagnostic File" button.



- The file will take some time to be created as its size is several MBs. After the file has been created it will be automatically sent to your web browser. Then save the file to your local hard disk.
- The diagnostic file is named "*lt\_diag\_SERIALNUMBER.tgz*" and the file format is a tgz archive. You can open the tgz archive e.g. with 7Zip (<https://www.7-zip.org/>).

### 11.3.2 Download via USB Stick

- The USB stick have to be formatted in a linux compatible file system like FAT. Connect a USB stick to the USB port of the LANTIME:
- The USB Memory Stick Menu opens automatically. Press „OK“ to confirm.
- You can use the up and down arrows to move through the menu.
- Use the „Write diagnostic File to USB stick“ option to write the current diagnostic file to the USB stick.
- You can find the Diagnostic File by opening the LANTIME folder and continue on to the Diag folder.



## 11.4 Self-Help Online Tools

Here is the list of some informative websites where you can query different information about the Meinberg Systems.

1. Meinberg Homepage - general:  
<https://www.meinbergglobal.com/>
2. NTP Download - at Meinberg:  
<https://www.meinbergglobal.com/english/sw/>
3. NTP Client Download for Windows (NTP-time-server-monitor):  
<https://www.meinbergglobal.com/english/sw/ntp-server-monitor.htm>
4. LANTIME firmware update request online form:  
<https://www.meinbergglobal.com/english/sw/firmware.htm>
5. Download page for Meinberg software, drivers and software:  
<https://www.meinbergglobal.com/english/sw/>
6. All Meinberg manuals (ENG, German versions):  
<https://www.meinbergglobal.com/english/docs/>
7. Meinberg Newsletter and subscription page:  
<https://www.meinbergglobal.com/english/company/news.htm>
8. NTP / IEEE 1588-PTP online tutorials from Meinberg:  
<http://blog.meinbergglobal.com/>
9. FAQs about Meinberg Products:  
<https://www.meinbergglobal.com/english/faq/>
10. Meinberg Knowledgebase:  
<https://kb.meinbergglobal.com>
11. GPS / GNSS Antenna Installation and mounting:  
<https://www.meinbergglobal.com/english/info/gps-antenna-mount.htm>  
<https://www.youtube.com/watch?v=ZTJMKSI8OCY> (YouTube video)
12. NTP support page and documentation:  
<http://support.ntp.org/bin/view/Support/WebHome>

## 11.5 NTP and IEEE 1588-PTP online tutorials

A team of Meinberg engineers are writing online tutorials covering topics on IEEE 1588 PTP, NTP, synchronization setups and configurations used in different industries.

The tutorials can be found at:  
<http://blog.meinbergglobal.com/>

The blog provides you also the opportunity to write a comment or a question to our experts and get their reply.

### Categories:

Configuration Guidelines, IEEE 1588, Industry Applications, NTP and Security.

## 11.6 The Meinberg Academy introduction and offerings

Meinberg Sync Academy (MSA) is an institution within the Meinberg Company which takes care for education and expert knowledge dissemination in the field of time and frequency synchronization. The academy offers tutorials and courses on the latest synchronization technologies such as NTP, IEEE 1588-PTP, synchronization networks for different industries: telecom, power, broadcasting, professional audio/video, finance, IT and . The MSA courses include both, theoretical lectures and practical hands-on labs.

If you are planning or re-designing synchronization for your networks and you need additional knowledge, see our agenda for the upcoming courses.

Homepage: <https://www.meinbergglobal.com/english/support/meinberg-sync-academy.htm>

Courses: Meinberg Product Training, NTP Complete, PTP Complete  
Customized Trainings and Online Trainings.

Contact Phone: +49 (0) 5281 93093-0

E-Mail: [info@meinberg.de](mailto:info@meinberg.de)

## 11.7 Meinberg Newsletter

Meinberg publishes regularly up-to-date information, technical news, firmware updates and security advisory by the Meinberg Newsletter in both the English and German language.

Subscribe to the newsletter here:

<https://www.meinbergglobal.com/english/contact/newslett.htm>

# 12 Appendix

## 12.1 LANTIME CPU - Central Processing Unit

### Booting the Single Board Computer

The LINUX operating system is loaded from a packed file on the flash disk of the single board computer to a RAM disk. All files of the flash disk are stored in the RAM disk after booting. Because of that it is guaranteed that the file system is in a defined condition after restart. This boot process takes approx. two minutes. During this time the following message appears on the display:

```
MEINBERG LANTIME
is booting ...
please wait ...
.....
```

After starting up the LINUX system the network function is initiated and the program for communication with the reference clock and the NTPD (NTP daemon) is started. After that NTPD starts synchronization with the reference clockss (usual the hardware clock of the single board computer and the used receiver). Until synchronization is finished the following message is displayed:

```
CLK: Not Sync
NTP: Sync to OSC
Wed, dd.mm.yyyy
UTC 12:00:00
```

For the synchronization of the NTPD, e.g. with a GPS creceiver, it is necessary that the GPS receiver is synchronous with the GPS time. In this case the following message is shown on the display:

```
NORMAL OPERATION
NTP: Offs. 2ms
Wed, dd.mm.yyyy
UTC 12:00:00
```

The second line shows the user that the NTPD is synchronized with the GPS with an offset of -50us. Because of the internal time of the NTP which is adjusted by a software PLL (phase locked loop) it takes a certain time to optimise this offset. The NTPD tries to keep the offset below +-128 ms; if the offset becomes too large the system time is set with the GPS time. Typically values for the offset are +-5 ms after the NTPD has already synchronized.

### 12.1.1 Technical Specifications LAN CPU

CPU Module Type C05F1:

<b>Processor:</b>	AMD Geode™ LX 800 (500 MHz, 128 KB L2 cache, 3.6 W)
<b>Main Memory:</b>	onboard 256 MByte
<b>Flashdisk:</b>	1 GB
<b>Network Connector:</b>	10/100 MBIT with RJ45-Jack
<b>Power Requirements:</b>	5 V +- 5 %, @ 1 A
<b>Frontpanel:</b>	3U / 4TE (128 mm high x 20,3 mm wide)
<b>Ambient Temperature:</b>	0 ... 50 °C
<b>Storage Temperature:</b>	-20 ... 70 °C
<b>Humidity:</b>	85 % max.

## 12.2 Description of Time String Formats

### 12.2.1 Format of the Meinberg Standard Time String

The Meinberg Standard Time String is a sequence of 32 ASCII characters starting with the <STX> (start-of-text) character and ending with the <ETX> (end-of-text) character. The format is as follows:

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

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<STX>	Start-of-Text, ASCII code 02h sent with one-bit accuracy at the change of each second		
dd.mm.yy	The date:		
	<i>dd</i>	Day of Month	(01–31)
	<i>mm</i>	Month	(01–12)
	<i>yy</i>	Year of the Century	(00–99)
w	The day of the week		(1–7, 1 = Monday)
hh.mm.ss	The time:		
	<i>hh</i>	Hours	(00–23)
	<i>mm</i>	Minutes	(00–59)
	<i>ss</i>	Seconds	(00–59, or 60 during leap second)
uv	Clock status characters (depending on clock type):		
	u:	'#'	GPS: Clock is in free-run mode (no exact synchronization) PZF: Time frame not synchronized DCF77: Clock has not synchronized since last reset
		' '	(space, 20h) GPS: Clock is synchronized (base accuracy is reached) PZF: Time frame is synchronized DCF77: Clock has synchronized since last reset
	v:	'*'	GPS: Receiver has not checked its position PZF/DCF77: Clock currently running off XTAL
		' '	(space, 20h) GPS: Receiver has determined its position PZF/DCF77: Clock is synchronized with transmitter
x	time zone indicator:		
		'U'	UTC Universal Time Coordinated, formerly GMT
		' '	CET European Standard Time, daylight saving disabled
		'S'	(CEST) European Summertime, daylight saving enabled
y	Announcement of clock jump during last hour before jump enters effect:		
		'!	Announcement of start or end of Daylight Saving Time
		'A'	Announcement of leap second insertion
		' '	(Space, 20h) nothing announced
<ETX>	End-of-Text, ASCII code 03h		

### 12.2.2 Format of the Meinberg GPS Time String

The Meinberg GPS Time String is a sequence of 36 ASCII characters starting with the <STX> (start-of-text) character and ending with the <ETX> (end-of-text) character. Unlike the Meinberg Standard Time String, the Meinberg GPS Time String does not carry any local time zone or UTC data; it simply carries the direct GPS

time without any conversion into UTC. The format is as follows:

<STX>D:*dd.mm.yy*;T:w;U:*hh.mm.ss*;uvGy;lll<ETX>

The letters printed in *italics* are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<STX>	Start-of-Text, ASCII code 02h
<i>dd.mm.yy</i>	The date: <i>dd</i> Day of Month (01–31) <i>mm</i> Month (01–12) <i>yy</i> Year of the Century (00–99)
<i>w</i>	the day of the week (1–7, 1 = Monday)
<i>hh.mm.ss</i>	the current time: <i>hh</i> Hours (00–23) <i>mm</i> Minutes (00–59) <i>ss</i> Seconds (00–59, or 60 while leap second)
<i>uv</i>	Clock status characters: <i>u</i> : '# ' Clock is in free-run mode (no exact synchronization) (Space, 20h) ' ' Clock is synchronized (base accuracy is achieved)  <i>v</i> : '* ' Receiver has not checked its position (Space, 20h) ' ' Receiver has determined its position
<i>G</i>	'GPS time' time zone indicator
<i>y</i>	Announcement of clock jump during last hour before jump enters effect: before discontinuity comes in effect: 'A' Announcement of leap second insertion ' ' (Space, 20h) nothing announced
<i>lll</i>	Number of leap seconds between UTC and GPS Time (UTC = GPS time + number of leap seconds)
<ETX>	End-of-Text, ASCII code 03h



### 12.2.3 Format of the Meinberg Capture String

The Meinberg Capture String is a sequence of 31 ASCII characters terminated by a <CR>/<LF> (Carriage Return/Line Feed) combination. The format is as follows:

`CHxdd.mm.yy_hh:mm:ss.ffffff<CR><LF>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

`x`            0 or 1 corresponding on the number of the capture input  
`_`            Space, ASCII code 20h

`dd.mm.yy` Capture date:

<i>dd</i>	Day of Month	(01–31)
<i>mm</i>	Month	(01–12)
<i>yy</i>	Year of the Century	(00–99)

`hh:mm:ss.ffffff` Capture time:

<i>hh</i>	Hours	(00–23)
<i>mm</i>	Minutes	(00–59)
<i>ss</i>	Seconds	(00–59, or 60 while leap second)
<i>ffffff</i>	Fractions of Second, 7 Digits	

<CR>        Carriage Return, ASCII code 0Dh

<LF>        Line Feed, ASCII code 0Ah

## 12.2.4 Format of the SAT Time String

The SAT Time String is a sequence of 29 ASCII characters starting with the <STX> (start-of-text) character and ending with the <ETX> (end-of-text) character. The format is as follows:

*<STX>dd.mm.yy/w/hh:mm:ssxxxuv<ETX>*

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

<STX>	Start-of-Text, ASCII code 02h sent with one-bit accuracy at the change of each second
dd.mm.yy	The date: <i>dd</i> Day of Month (01–31) <i>mm</i> Month (01–12) <i>yy</i> Year of the Century (00–99)
w	The day of the week (1 = Monday)
hh:mm:ss	The time: <i>hh</i> Hours (00–23) <i>mm</i> Minutes (00–59) <i>ss</i> Seconds (00–59, or 60 during leap second)
xxxx	Time zone indicator: 'UTC' Universal Time Coordinated, formerly GMT 'CET' European Standard Time, daylight saving disabled 'CEST' European Summertime, daylight saving enabled
u	Clock status characters: '#' Clock has not synchronized since last reset '' (Space, 20h) Clock has synchronized since last reset
v	Announcement of clock jump during last hour before jump enters effect: '!' Announcement of start or end of Daylight Saving Time '' (Space, 20h) nothing announced
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah
<ETX>	End-of-Text, ASCII code 03h

## 12.2.5 Format of the Uni Erlangen String (NTP)

The Uni Erlangen String (NTP) of a GPS clock is a sequence of 66 ASCII characters starting with the <STX> (start-of-text) character and ending with the <ETX> (end-of-text) character. The format is as follows:

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

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

<STX>	Start-of-Text, ASCII code 02h sent with one-bit accuracy at the change of each second
dd.mm.yy	The date: <i>dd</i> Day of Month (01–31) <i>mm</i> Month (01–12) <i>yy</i> Year of Century (00–99)
w	Day of the week (1–7, 1 = Monday)
hh.mm.ss	The time: <i>hh</i> Hours (00–23) <i>mm</i> Minutes (00–59) <i>ss</i> Seconds (00–59, or 60 during leap second)
v	-/+ sign of the offset of local timezone relative to UTC
oo:oo	Offset of local time zone relative to UTC in hours and minutes
ac	Clock status characters: a: '#' Clock has not synchronized since reset ' ' (Space, 20h) Clock has synchronized since reset  c: '*' GPS receiver has not checked its position ' ' (Space, 20h) GPS receiver has determined its position
d	Time zone indicator: 'S' CEST European Summertime, Daylight Saving Time enabled ' ' CET European Standard Time, Daylight Saving Time disabled
f	Announcement of clock jump during last hour before jump enters effect: '!' Announcement of start or end of Daylight Saving Time ' ' (Space, 20h) nothing announced
g	Announcement of clock jump during last hour before jump enters effect: 'A' Announcement of leap second insertion ' ' (Space, 20h) nothing announced
i	Leap second insertion 'L' Leap second is currently to be inserted (only active in 60th second) ' ' (Space, 20h) No leap second to be inserted
bbb.bbbb	Geographical latitude of receiver position in degrees Leading characters padded by Space characters (20h)
n	Latitudinal hemisphere, with the following characters possible: 'N' North of Equator

	'S'	South of Equator
lll.llll		Geographical longitude of receiver position in degrees Leading characters padded by Space characters (20h)
e		Longitudinal hemisphere, with the following characters possible: 'E' East of Greenwich Meridian 'W' West of Greenwich Meridian
hhhh		Altitude above WGS84 ellipsoid in meters Leading characters padded by Space characters (20h)
<ETX>		End-of-Text, ASCII code 03h

### 12.2.6 Format of the NMEA 0183 String (RMC)

The NMEA 0183 RMC String is a sequence of 65 ASCII characters starting with the string '\$GPRMC' and ending with the characters <CR> (Carriage Return) and <LF> (Line Feed). The format is as follows:

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

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

- \$            Start character, ASCII code 24h  
sent with one-bit accuracy at the change of each second
  
- GP            Talker ID, in this case "GP" for GPS
  
- RMC            Message type ID, in this case "RMC"
  
- hhmmss.ss    The time:
  - hh*        Hours                    (00–23)
  - mm*        Minutes                    (00–59)
  - ss*        Seconds                    (00–59, or 60 while leap second)
  - ff*        Fractions of Seconds (1/10 ; 1/100)
  
- A            Status (A = Time Data Valid, V = Time Data not Valid)
  
- bbbb.bb      Geographical latitude of receiver position in degrees  
Leading characters padded by Space characters (20h)
  
- n            Latitudinal hemisphere, with the following characters possible:
  - 'N'        North of Equator
  - 'S'        South of Equator
  
- lllll.ll      Geographical longitude of receiver position in degrees  
Leading characters padded by Space characters (20h)
  
- e            Longitudinal hemisphere, with following characters possible:
  - 'E'        East of Greenwich Meridian
  - 'W'        West of Greenwich Meridian
  
- 0.0,0.0      Speed over the ground in knots and track angle in degrees.  
With a Meinberg GPS clock, these values are always 0.0,  
With GNS clocks, the values are calculated by the  
receiver for mobile applications
  
- ddmmyy      The date:
  - dd*        Day of Month                (01–31)
  - mm*        Month                        (01–12)
  - yy*        Year of  
                                  the Century                (00–99)
  
- a            Magnetic Variation E/W
  
- hh            Checksum (XOR of all characters except '\$' and '\*')
  
- <CR>        Carriage Return, ASCII code 0Dh
  
- <LF>        Line Feed, ASCII code 0Ah

## 12.2.7 Format of the NMEA 0183 String (GGA)

The NMEA 0193 GGA String is a sequence of characters starting with the string '\$GPGGA' and ending with the characters <CR> (Carriage Return) and <LF> (Line Feed). The format is as follows:

***\$GPGGA,hhmmss.ff,bbbb.bbbbb,n,llll.ll,e,A,vv,hhh.h,aaa.a,M,ggg.g,M,0\*cs<CR><LF>***

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

\$	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second
GP	Talker ID, in this case "GP" for GPS
GGA	Message type ID, in this case "GGA"
hhmmss.ss	The time: <i>hh</i> Hours (00–23) <i>mm</i> Minutes (00–59) <i>ss</i> Seconds (00–59, or 60 while leap second) <i>ff</i> Fractions of Seconds (1/10 ; 1/100)
bbbb.bbbbb	Geographical latitude of receiver position in degrees Leading characters padded by Space characters (20h)
n	Latitudinal hemisphere, with the following characters possible: 'N' North of Equator 'S' South of Equator
llll.lllll	Geographical longitude of receiver position in degrees Leading characters padded by Space characters (20h)
e	Longitudinal hemisphere, with following characters possible: 'E' East of Greenwich Meridian 'W' West of Greenwich Meridian
A	Position fixed (1 = yes, 0 = no)
w	Number of satellites used (0–12)
hhh.h	HDOP (Horizontal Dilution of Precision)
aaa.h	Mean Sea Level Altitude (MSL Altitude = WGS84 Altitude - Geoid Separation)
M	Units, Meters (Fixed Value)
ggg.g	Geoid Separation (WGS84 Altitude - MSL Altitude)
M	Units, Meters (Fixed Value)
cs	Checksum (XOR of all characters except '\$' and '*')
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

### 12.2.8 Format of the NMEA 0183 String (ZDA)

The NMEA 0183 ZDA String is a sequence of 38 ASCII characters starting with the string '\$GPZDA' and ending with the characters <CR> (Carriage Return) and <LF> (Line Feed). The format is:

**\$GPZDA, *hhmmss.ss, dd, mm, yyyy, HH, II*\*cs<CR><LF>**

ZDA - Time and Date: UTC, day, month, year and local time zone.

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

**\$** Start character, ASCII Code 24h  
sending with one bit accuracy at change of second

***hhmmss.ss*** UTC time:  
 hh Hours (00–23)  
 mm Minutes (00–59)  
 ss Seconds (00–59, or 60 during leap second)

***HH,II*** The local time zone (offset to UTC):  
 HH Hours (00–±13)  
 II Minutes (00–59)

***dd,mm,yy*** The date:  
 dd Day of Month (01–31)  
 mm Month (01–12)  
 yyyy Year (0000–9999)

***cs*** Checksum (XOR of all characters except '\$' and '\*')

**<CR>** Carriage Return, ASCII code 0Dh

**<LF>** Line Feed, ASCII code 0Ah

### 12.2.9 Format of the ABB SPA Time String

The ABB SPA Time String is a sequence of 32 ASCII characters starting with the characters ">900WD" and ending with the <CR> (Carriage Return) character. The format is as follows:

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

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

*yy-mm-tt* The date:

*yy* Year of the Century (00–99)

*mm* Month (01–12)

*dd* Day of Month (01–31)

*\_* Space (ASCII code 20h)

*hh.mm;ss.fff* The time:

*hh* Hours (00–23)

*mm* Minutes (00–59)

*ss* Seconds (00–59, or 60 during leap second)

*fff* Milliseconds (000–999)

*cc* Checksum calculated as XOR sum of the preceding characters.

The resultant 8-bit value is reported as a hex value in the form of two ASCII characters (2 ASCII characters 0..9 or A..F)

<CR> Carriage Return, ASCII Code 0Dh



### 12.2.10 Format of the Computime Time String

The Computime Time String is a sequence of 24 ASCII characters starting with the T character and ending with the <LF> (Line Feed, ASCII code 0Ah) character. The format is as follows:

*T:yy:mm:dd:ww:hh:mm:ss*<CR><LF>

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

T	Start character sent with one-bit accuracy at the change of each second
yy:mm:dd	The date: yy    Year of Century    (00–99) mm    Month            (01–12) dd    Day of Month        (01–31) ww    Day of Week         (01–07, 01 = monday)
hh:mm:ss	The time: hh    Hours                (00–23) mm    Minutes              (00–59) ss    Seconds             (00–59, or 60 during leap second)
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

### 12.2.11 Format of the RACAL Standard Time String

The RACAL Standard Time String is a sequence of 16 ASCII characters started by a X (58h) character and ending with the <CR> (Carriage Return, ASCII code 0Dh) character. The format is as follows:

<X><G><U>*yymmddhhmmss*<CR>

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

<X>	Control character Sent with one-bit accuracy at the change of each second	Code 58h
<G>	Control character	Code 47h
<U>	Control character	Code 55h
<i>yymmdd</i>	Current date: yy      Year of Century      (00–99) mm      Month                    (01–12) dd      Day of Month                (01–31)	
<i>hh:mm:ss</i>	Current time: hh      Hours                        (00–23) mm      Minutes                        (00–59) ss      Seconds                        (00–59, or 60 during leap second)	
<CR>	Carriage Return, ASCII Code 0Dh	

### 12.2.12 Format of the SYSPLEX-1 Time String

The SYSPLEX-1 time string is a sequence of 16 ASCII characters starting with the <SOH> (Start of Header) ASCII control character and ending with the <LF> (Line Feed, ASCII code 0Ah) character.

**Please note:**

To ensure that the time string can be correctly output and displayed through any given terminal program, a singular "C" (not include quotation marks) must be input.

The format is:

<SOH>ddd:hh:mm:ssq<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are part of the time string. The groups of characters as defined below:

<SOH>	Start of Header, ASCII code 01h sent with one-bit accuracy at the change of each second
ddd	Day of Year (001–366)
hh:mm:ss	Current time:
hh	Hours (00–23)
mm	Minutes (00–59)
ss	Seconds (00–59, or 60 during leap second)
q	Quality Indicator (Space) Time Sync (GPS Lock) (?) No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)
<LF>	Line Feed (ASCII code 0Ah)

### 12.2.13 Format of the ION Time String

The ION time string is a sequence of 16 ASCII characters starting with the <SOH> (Start of Header) ASCII control character and ending with the <LF> (Line Feed, ASCII code 0Ah) character. The format is as follows:

<SOH>ddd:hh:mm:ssq<CR><LF>

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII control character) sent with one-bit accuracy at the change of each second
ddd	Day of Year (001–366)
hh:mm:ss	Current time:
hh	Hours (00–23)
mm	Minutes (00–59)
ss	Seconds (00–59, or 60 while leap second)
q	Quality Indicator (space) Time Sync (GPS Lock) (?) No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)
<LF>	Line Feed (ASCII code 0Ah)

### 12.2.14 Format of the ION Blanked Time String

The ION Blanked Time String is a sequence of 16 ASCII characters starting with the <SOH> (Start of Header) ASCII control character and ending with the <LF> (Line Feed, ASCII code 0Ah) character. The format is as follows:

<SOH>ddd:hh:mm:ssq<CR><LF>

**Important:** The blanking interval of is 2 minutes and 30 seconds long and is added every 5 minutes.

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII control character) sent with one-bit accuracy at the change of each second
ddd	Day of Year (001–366)
hh:mm:ss	Current Time:
hh	Hours (00–23)
mm	Minutes (00–59)
ss	Seconds (00–59, or 60 while leap second)
q	Quality Indicator (space) Time Sync (GPS Lock) (?) No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII Code 0Dh)
<LF>	Line Feed (ASCII Code 0Ah)

### 12.2.15 Format of the IRIG-J Timecode

The IRIG-J timecode consists of a string of ASCII characters sent in "701" format:

- 1 Start Bit
- 7 Data Bits
- 1 Parity Bit (odd)
- 1 Stop Bit

The on-time marker of the string is the leading edge of the start bit. The timecode consists of 15 characters, sent once per second at a baud rate of 300 or greater. The format is as follows:

`<SOH>DDD:HH:MM:SS<CR><LF>`

The letters printed in italics are replaced by ASCII-formatted numbers, whereas the other characters are directly part of the time string. The groups of characters are as defined below:

<code>&lt;SOH&gt;</code>	"Start of Header" ASCII code (0x01h)
<i>DDD</i>	Day of the year (ordinal date, 1 to 366)
<i>HH, MM, SS</i>	Time of the start bit, specified in in hours ( <i>HH</i> ), minutes ( <i>MM</i> ), seconds ( <i>SS</i> )
<code>&lt;CR&gt;</code>	"Carriage Return" ASCII code (0x0Dh)
<code>&lt;LF&gt;</code>	"Line Feed" ASCII code (0x0Ah)

## 12.3 SyncMon Formats

SyncMon format for LANTIME firmware usage:

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0_test 58154 34813 2018-02-05T09:
40: 13 + 00: 00 0.000000494 0.000041453 0.000073266 1 R -0.000011100
0.000041453
```

### Key-Value-Pairs

The Format with Key-Value-Pairs can be accessed directly from a SPLUNK database server and has the following format:

```
isoTime           = 2018-02-05T09: 40: 13 + 00: 00
syncMonName       = SyncMon
optInterfacelp    = 172.27.100.32
utcTime           = 1517823613
node              = M3000_100_57_NTP_LAN0_test
offset1           = 0.000000494
offset2           = 0.000041453
pathDelay         = 0.000073266
status            = Stratum: 1 / [10]
offset1Min        = -0.000011100
offset1Max        = 0.000041453
type              = NTP / SW / CPU
```

### JSON

The JSON format can be processed directly by most databases and has the following format:

```
{
  "isoTime":      "2018-02-05T09: 40: 13 + 00: 00",
  "syncMonName":  "SyncMon",
  "optInterfacelp": "172.27.100.32",
  "utcTime":      1517823613,
  "node":         "M3000_100_57_NTP_LAN0_test",
  "offset1":      0.000000494,
  "offset2":      0.000041453,
  "pathDelay":    0.000073266,
  "status":       "stratum 1 / [10]",
  "offset1Min":   - 0.000011100,
  "offset1Max":   0.000041453,
  "type":         "NTP / SW / CPU"
}
```

## 12.4 Third party software

The LANTIME network timeserver is running a number of software products created and/or maintained by open source projects. A lot of people contributed to this and we explicitly want to thank everyone involved for her/his great work.

The used open source software comes with its own license which we want to mention below. If one of the licenses for a third party software product is violated, we will as soon as possible apply any changes needed in order to conform with the corresponding license after we acknowledged about that violation.

If a license for one of the software products states that we have to provide you with a copy of the source code or other material, we will gladly send it to you on data media via normal post or by e-mail upon request. Alternatively we can provide you with a link to a download location in the internet, allowing you to download the most actual version. Please note that we have to charge you for any incurred expenses if you choose to receive the source code on data media.

### 12.4.1 Operating System GNU/Linux

The distribution of the GNU/Linux operating system is covered by the GNU General Public License (GPL), which we included below.

More information about GNU/Linux can be found on the GNU website  
[www.gnu.org](http://www.gnu.org)

and on the website of GNU/Linux  
[www.linux.org](http://www.linux.org)

### 12.4.2 Samba

The Samba software suite is a collection of programs, which implement the Server Message Block (SMB) protocol for UNIX systems. By using Samba your Lantime is capable of sending Windows popup messages and serves request for network time by clients using the NET TIME command.

The distribution of Samba is covered – like GNU/Linux – by the GNU General Public License, see below.

The website of the Samba project (or a mirror) can be reached at  
[www.samba.org](http://www.samba.org)



### 12.4.3 Network Time Protocol Version 4 (NTP)

The NTP project, lead by David L. Mills, can be reached in the internet at [www.ntp.org](http://www.ntp.org). There you will find a wealthy collection of documentation and information covering all aspects of the application of NTP for time synchronization purposes. The distribution and usage of the NTP software is allowed, as long as the following notice is included in our documentation:

```

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

```

#### 12.4.4 lighttpd

For our web based configuration tool (HTTP and HTTPS) we use Lighttpd. Lighttpd is a free web server, with all the essential functions of a web server. Lighttpd has been developed by the german Software Developer Jan Kneschke.

The use of this software is covered by the following license:

Copyright (c) 2004, Jan Kneschke, incremental  
All rights reserved.

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

## 12.4.5 GNU General Public License (GPL)

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

Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### Preamble

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

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

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

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

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

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

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

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

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

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

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

Whether that is true depends on what the Program does.

---

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

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

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

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

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

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

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

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

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

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

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either

source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

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

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

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

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

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

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

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

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

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

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

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

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

#### **NO WARRANTY**

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

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

#### **END OF TERMS AND CONDITIONS**

## 12.5 List of Literature

- [Mills88] Mills, D. L., "Network Time Protocol (Version 1) - specification and implementation", DARPA Networking Group Report RFC-1059, University of Delaware, July 1988
- [Mills89] Mills, D. L., "Network Time Protocol (Version 2) - specification and implementation", DARPA Networking Group Report RFC-1119, University of Delaware, September 1989
- [Mills90] Mills, D. L., "Network Time Protocol (Version 3) - specification, implementation and analysis", Electrical Engineering Department Report 90-6-1, University of Delaware, June 1989
- Kardel, Frank, "Gesetzliche Zeit in Rechnernetzen", Funkuhren, Zeitsignale und Normalfrequenzen, Hrsg. W. Hilberg, Verlag Sprache und Technik, Groß-Bieberau 1993
- Kardel, Frank, "Verteilte Zeiten", ix Multiuser-Multitasking-Magazin, Heft 2/93, Verlag Heinz Heise, Hannover 1993