The Synchronization Experts.

MANUAL

LTOS 7.08

LANTIME Operating System Firmware
Configuration and
Management Manual

Meinberg Funkuhren GmbH & Co. KG

Table of Contents

1 Imprint and Legal Information 1

2 Copyright and Liability Exclusion 2

3 Important Safety Information 3
- 3.1 Important Safety Information and Safety Precautions . . . 3
- 3.2 Used Symbols . . . 4
- 3.3 Product Documentation . . . 5
- 3.4 Safety During Installation . . . 6
- 3.5 Connection of Protective Earth Conductor/Grounding . . . 9
- 3.6 Safety During Operation . . . 10
- 3.7 Safety During Maintenance . . . 11
- 3.8 Handling of Batteries . . . 12
- 3.9 Cleaning and Care . . . 13
- 3.10 Prevention of ESD Damage . . . 13
- 3.11 Return of Electrical and Electronic Equipment . . . 14

4 Before you start 15
- 4.1 Text and Syntax Conventions . . . 15
- 4.2 Required Tools . . . 16
- 4.3 Abbreviation List . . . 17

5 Introduction 19
- 5.1 Network Configuration Concept . . . 20
- 5.2 Additional Features . . . 20
- 5.3 User Interface . . . 20
- 5.4 Input and Output Options . . . 21
- 5.5 The Network Time Protocol (NTP) . . . 22
  - 5.5.1 Computer Platforms Supported by NTP . . . 22
- 5.6 Option: Precision Time Protocol (PTP) / IEEE 1588 . . . 23
  - 5.6.1 General Information . . . 24
  - 5.6.2 Functionality in Master Systems . . . 25
  - 5.6.3 Functionality in Slave Systems . . . 26
  - 5.6.4 PTPv2 IEEE 1588-2008 Configuration Guide . . . 27

6 Unboxing 33

7 LANTIME Installation 35

8 Security User Guide / Security Advisories 38
- 8.1 General Information . . . 39
- 8.2 Optimizing Management Access Security . . . 41
- 8.3 User Management/Administration . . . 45
  - 8.3.1 LANTIME User Management . . . 45
  - 8.3.2 External User Authentication: LDAP(S), Radius and TACACS+ . . . 47
- 8.4 Securing NTP and NTS . . . 50
  - 8.4.1 Securing the NTP Time Service . . . 50
  - 8.4.2 Configuration of Network Time Security (NTS) . . . 53
- 8.5 Event Log Delivery . . . 55
- 8.6 Update and Backup LANTIME Firmware . . . 56

9 Antenna and Receiver Information 59
9.1 Reference Time Sources . . . 59
9.1.1 Meinberg GPS Receiver . . . 59
9.1.2 Meinberg GNSS Receiver (GPS, GLONASS, Galileo, BeiDou) . . . 60
9.1.3 PZF - DCF77 Long Wave Receiver . . . 61
9.1.4 MSF Receiver . . . 62
9.1.5 WWVB Receiver . . . 64
9.1.6 TCR Receiver . . . 65
9.2 GNSS Signal Reception . . . 66
9.2.1 Installing a GPSANTv2 . . . 67
9.2.2 Installation of a GNSS Antenna . . . 74
9.2.3 Powering up a GNSS Receiver . . . 80
9.3 Long Wave Signal Reception . . . 81
9.3.1 Introduction . . . 81
9.3.2 Installation of a Longwave Antenna . . . 82
9.3.3 Powering up a DCF77 / PZF Receiver . . . 90
9.4 Surge Protection and Grounding . . . 91

10 LTOS7 Management and Monitoring 97
10.1 Via Web GUI . . . 97
10.1.1 Session Handling . . . 97
10.1.2 Main Menu . . . 98
10.1.3 Network . . . 104
10.1.4 Notification . . . 121
10.1.5 Security . . . 135
10.1.6 NTP . . . 147
10.1.7 PTP . . . 173
10.1.8 FDM - Frequency Deviation Monitoring . . . 198
10.1.9 System . . . 221
10.1.10 Clock . . . 246
10.1.11 I/O Configuration . . . 278
10.1.12 SyncMon . . . 300
10.1.13 Documentation and Support . . . 350
10.2 Via Front Panel Display . . . 352
10.2.1 LANTIME Display Types . . . 352
10.2.2 Front Display - Root Menu . . . 357
10.2.3 Menu: Reference Time . . . 359
10.2.4 Menu: Time Service . . . 376
10.2.5 Menu: Network . . . 397
10.2.6 Menu: System . . . 402
10.2.7 USB Stick Menu . . . 409
10.3 Via Serial Connection . . . 412
10.4 Via SNMP . . . 413
10.4.1 The Simple Network Managment Protocol . . . 413
10.4.2 MIB Objects of a LANTIME . . . 414
10.4.3 SNMP Traps . . . 419

11 Troubleshooting and Alarming 428
11.1 NTP Messages . . . 428
11.2 Ref. Clock Messages . . . 429
11.3 Network Messages . . . 434
11.4 Miscellaneous Messages . . . 435

12 Support Information 437
12.1 Basic Customer Support . . . 438
12.2 Support Ticket System . . . 438
12.3 How to download a Diagnostic File . . . 439
12.3.1 Download via Web GUI . . . 439
12.3.2 Download via USB Stick . . . 439
12.4 Self-Help Online Tools . . . 440
12.5 NTP and IEEE 1588-PTP online tutorials . . . 440

12.6 The Meinberg Academy introduction and offerings . . . 441
12.7 Meinberg Newsletter . . . 441
12.8 Meinberg Customer Portal - Software and Documentation . . . 442

13 Appendix 443
13.1 LANTIME CPU - Central Processing Unit . . . 443
13.1.1 Technical Specifications LAN CPU . . . 444
13.1.2 Technical Specifications - IMS CPU-C15G2 . . . 445
13.2 Technical Data - Antennas for LANTIME Systems . . . 447
13.2.1 Technical Specifications: GPSANTv2 Antenna . . . 447
13.2.2 Technical Specifications: 40 dB Multi-GNSS Antenna for Fixed-Location Applications . . . 450
13.2.3 Technical Specifications: 27 dB Mobile Multi-GNSS Antenna for Mobile Applications . . . 451
13.2.4 Technical Specifications: GNSS Multi-Band Antenna . . . 452
13.2.5 Technical Specifications: AW02 Antenna . . . 454
13.2.6 Technical Specifications: MBG-S-PRO Surge Protector . . . 456
13.3 Time String Formats . . . 457
13.3.1 Meinberg Standard Time String . . . 457
13.3.2 Meinberg GPS Time String . . . 458
13.3.3 Meinberg Capture Time String . . . 459
13.3.4 ATIS Time String . . . 460
13.3.5 SAT Time String . . . 461
13.3.6 Uni Erlangen Time String (NTP) . . . 462
13.3.7 NMEA 0183 String (RMC) . . . 464
13.3.8 NMEA 0183 Time String (GGA) . . . 465
13.3.9 NMEA 0183 Time String (ZDA) . . . 466
13.3.10 ABB SPA Time String . . . 467
13.3.11 Computime Time String . . . 468
13.3.12 RACAL Time String . . . 469
13.3.13 SYSPLEX-1 Time String . . . 470
13.3.14 ION Time String . . . 471
13.3.15 ION Blanked Time String . . . 472
13.3.16 IRIG-J Timecode . . . 473
13.3.17 6021 Time String . . . 474
13.3.18 Freelance Time String . . . 476
13.3.19 ITU-G8271-Y.1366 Time-of-Day Message . . . 478
13.3.20 CISCO ASCII Time String . . . 479
13.3.21 NTP Type 4 Time String . . . 480
13.4 Time Code Formats . . . 481
13.5 Overview of Programmable Signals . . . 483
13.6 SyncMon Formats . . . 486
13.7 Fundamentals of IEC 61850 . . . 487
13.7.1 Data Sets . . . 488
13.7.2 Structure of a IEC 61850 CID File . . . 489
13.8 How Navigation Message Authentication Works . . . 491
13.8.1 Galileo OSNMA . . . 494
13.8.2 Fugro AtomiChron® . . . 496
13.9 Third party software . . . 497
13.9.1 Operating System GNU/Linux . . . 497
13.9.2 Samba . . . 497
13.9.3 Network Time Protocol Version 4 (NTP) . . . 498
13.9.4 lighttpd . . . 499
13.9.5 GNU General Public License (GPL) . . . 500
13.10 List of Literature . . . 504

1 Imprint and Legal Information

Publisher

Meinberg Funkuhren GmbH & Co. KG

Registered Place of Business:
Lange Wand 9
31812 Bad Pyrmont
Germany

Telephone:
+49 (0) 52 81 – 93 09 - 0

Fax:
+49 (0) 52 81 – 93 09 - 230

The company is registered in the "A" Register of Companies & Traders (Handelsregister A) maintained by the Local Court of Hanover (Amtsgericht Hannover) under the number:

17HRA 100322

Executive Management:	Heiko Gerstung Andre Hartmann Natalie Meinberg Daniel Boldt
Website:	https://www.meinbergglobal.com
Email:	info@meinberg.de

Document Publication Information

Manual Version:	1.5
Revision Date:	April 28, 2025
PDF Export Date:	May 22, 2025

2 Copyright and Liability Exclusion

Except where otherwise stated, the contents of this document, including text and images of all types and translations thereof, are the intellectual property and copyright of Meinberg Funkuhren GmbH & Co. KG ("Meinberg" in the following) and are subject to German copyright law. All reproduction, dissemination, modification, or exploitation is prohibited unless express consent to this effect is provided in writing by Meinberg. The provisions of copyright law apply accordingly.

Any third-party content in this document has been included in accordance with the rights and with the consent of its copyright owners.

A non-exclusive license is granted to redistribute this document (for example, on a website offering free-of-charge access to an archive of product manuals), provided that the document is only distributed in its entirety, that it is not modified in any way, that no fee is demanded for access to it, and that this notice is left in its complete and unchanged form.

At the time of writing of this document, reasonable effort was made to carefully review links to third-party websites to ensure that they were compliant with the laws of the Federal Republic of Germany and relevant to the subject matter of the document. Meinberg accepts no liability for the content of websites not created or maintained by Meinberg, and does not warrant that the content of such external websites is suitable or correct for any given purpose.

While Meinberg makes every effort to ensure that this document is complete, suitable for purpose, and free of material errors or omissions, and periodically reviews its library of manuals to reflect developments and changing standards, Meinberg does not warrant that this specific document is up-to-date, comprehensive, or free of errors. Updated manuals are provided at https://www.meinbergglobal.com and https://www.meinberg.support.

You may also write to techsupport@meinberg.de to request an updated version at any time or provide feedback on errors or suggested improvements, which we are grateful to receive.

Meinberg reserves the right to make changes of any type to this document at any time as is necessary for the purpose of improving its products and services and ensuring compliance with applicable standards, laws & regulations.

3 Important Safety Information

3.1 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. Meinberg accepts no responsibility for damage caused by a failure to observe these 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 word 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.

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

3.3 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.

3.4 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.

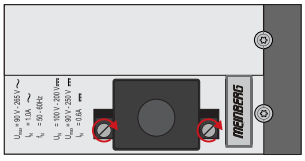
Before the device is connected to the power supply, a grounding conductor must be connected to the earth terminal of the device.

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

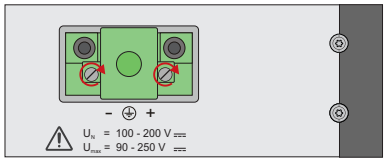
Before operation, check that all cables and lines work properly and are undamaged. Ensure in particular that the cables do not have kinks, that they are not wound too tightly around corners, and that no objects are placed on the cables.

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
• The device is a Protection Class 1 device and may only be connected to a grounded outlet (TN system). • 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. • The disconnection of the appliance from the mains power supply must always be performed from the mains socket and not from the appliance itself. • 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. • 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.	• 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). • 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). • Supply cables must be adequately secured and have an adequate wire gauge size. *Connection Cable Wire Gauge:* *1 mm^2 – 2.5 mm^2* *17 AWG – 13 AWG* • 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.

3.5 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 mm^2, as well as a suitable grounding clamp/lug. Always ensure that the connection is properly crimped!

3.6 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 (electriomagnetic 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.

3.7 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 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.

3.8 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

3.9 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.

3.10 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.

3.11 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.

4 Before you start

4.1 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
               =-_.:#*?@/+![]
```

4.2 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 / M150	LANTIME M200 / M250	LANTIME M300 / M320	LANTIME M400 / M450	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

4.3 Abbreviation List

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

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

5 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 correctl,y 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.

5.1 Network Configuration Concept

The LANTIME 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 7th generation of LANTIME firmware (LTOS7) can manage up to 99 physical network interfaces as a theoretical maxmium.

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.

5.2 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

5.3 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

5.4 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-SQ, OCXO-HQ, OCXO-DHQ)
- 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(S)	up to 25 (+24) Network Ports	up to 26 (+24) Network Ports
LANTIME M2000S	up to 25 (+24) Network Ports	up to 26 (+24) Network Ports
LANTIME M1000(S)	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 M450		up to 6 (+4) Network Ports
LANTIME M300	up to 6 (+4) Network Ports	
LANTIME M320		up to 6 (+4) Network Ports

5.5 The Network Time Protocol (NTP)

The NTP protocol has been invented in the 1980's by Dave L. Mills at the University of Delaware. The ambition was to achieve the highest possible time synchronization accuracy for computers across the network. The protocol and related algorithms have been specified in several RFCs.

The public domain software package called NTP is the reference implementation of this protocol. Since the original implementation NTP has been enhanced and is now widely used around the world. The protocol supports an accuracy of time down to nanoseconds. However, the real accuracy which can be achieved also depends on the operating system and the network performance.

The current NTP v4 protocol version has being standardized by the IETF, and the basic format of the network packets is compatible with earlier NTP versions, so current NTP implementations can be used together with older versions, unless specific NTP v4 features are being used. In addition to NTP there's also a simplified version called SNTP (Simple Network Time Protocol) which uses the same TCP/IP UDP packet structure like NTP but due to the simpler algorithms, it usually provides only reduced accuracy and is thus mostly used for simple clients. The NTP package contains a background program (daemon or service) which synchronizes the computer's system time to one or more external reference time sources which can be either other devices on the network, or a hardware reference time source connected to the computer.

Additionally, the NTP distribution contains programs which can be used to control or monitor the time synchronization status, and a complete set of documentation in HTML format.

Learn more about the Network Time Protocol in our white paper "Computer Time Synchronization Concepts" chapter 6:
https://www.meinbergglobal.com/english/info/#whitepaper

5.5.1 Computer Platforms Supported by NTP

NTP's native operating system is UNIX. Today, however, NTP runs under many UNIX-like systems, and NTP v4 has also been ported to Windows. It can be used under Windows NT, Windows 2000, and newer Windows versions up to Windows Vista, Windows 7 / Windows 8 and Windows Server 2008 / 2012.

The standard NTP distribution can **not** be run under Windows 3.x and Windows 9x/ME because there are some kernel features missing which are required for precision time keeping. For Windows 9x/ME and other platforms which are not supported directly by the NTP package there are some NTP or SNTP programs available on the internet. An overview of available programs can be found on the NTP support home page:
https://support.ntp.org/Main/ExternalTimeRelatedLinks

5.6 Option: Precision Time Protocol (PTP) / IEEE 1588

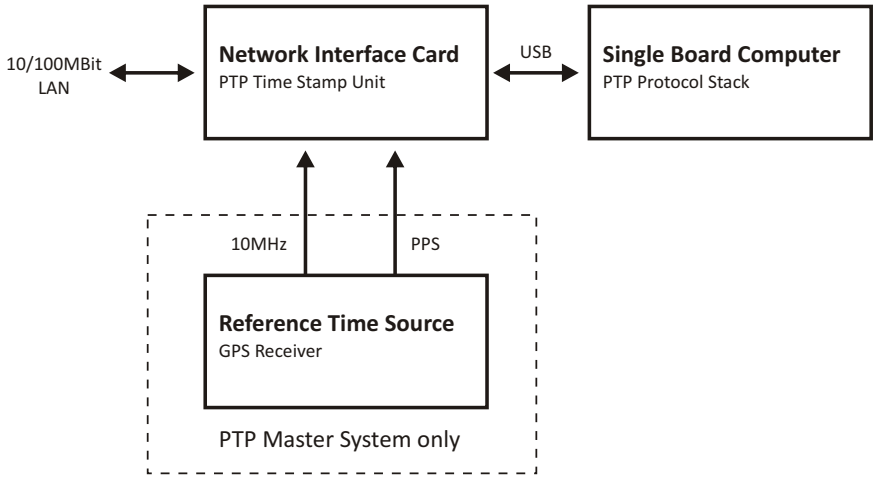
Precision Time Protocol (PTP or IEEE 1588) is a time synchronization protocol that offers sub-microsecond accuracy over a standard Ethernet connection. This accuracy can be achieved by adding a hardware timestamping unit to the network ports that are used for PTP time synchronization. The timestamping 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).

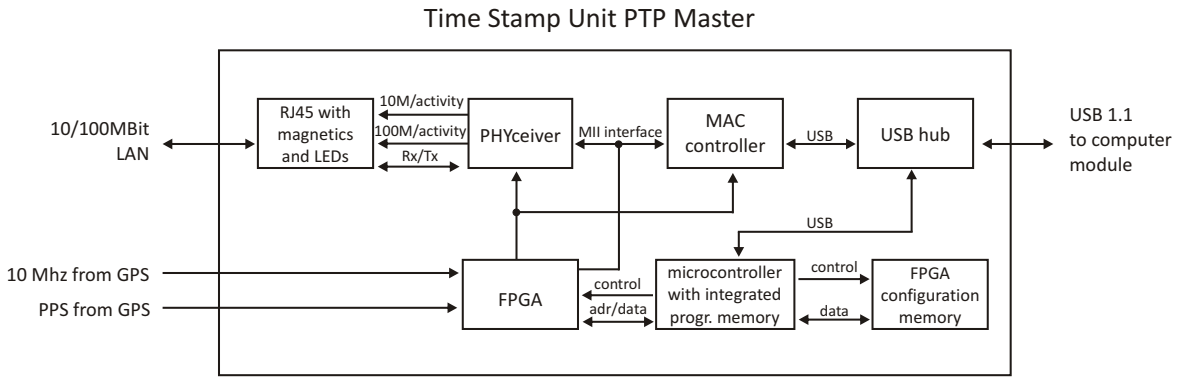
5.6.1 General Information

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:



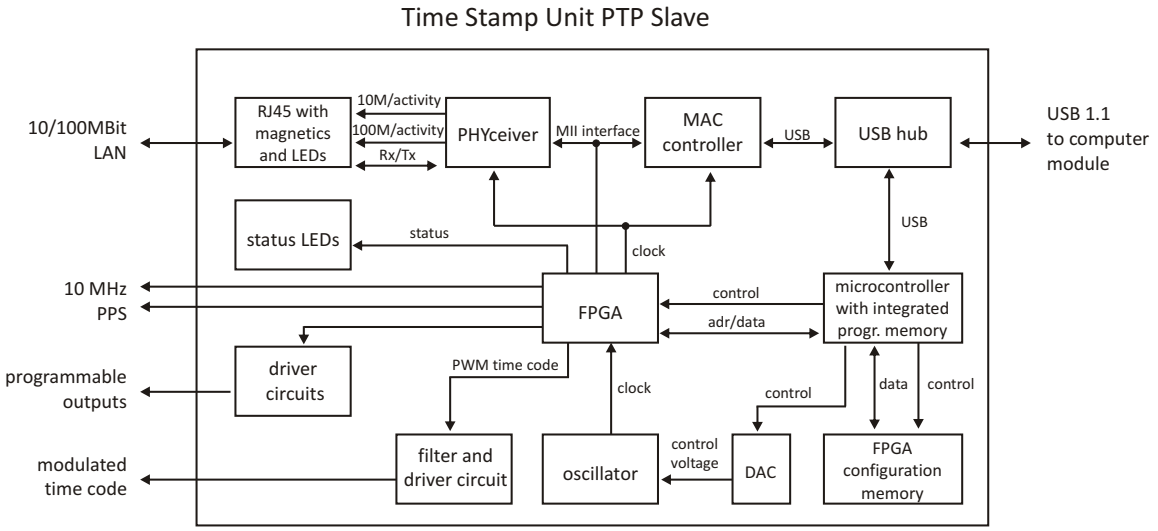
The Time Stamp Unit, integrated in an FPGA (Field Programmable Gate Array, a programmable logic device), checks the data traffic on the MII-interface between the PHY receiver (physical connection to the network) and the Ethernet controller (MAC) on the PTP module. If a valid PTP packet is detected, the 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.

5.6.2 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.

5.6.3 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).

5.6.4 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.

5.6.4.1 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 (E2E) or Peer-to-Peer (P2P) Delay Mechanism

The above options need to be defined for the whole setup; if devices do not adhere to a common configuration, they will not be able to establish a working synchronization link.

5.6.4.2 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.

5.6.4.3 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.

5.6.4.4 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.

5.6.4.5 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). With P2P measurement, 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.

E2E is therefore 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.

5.6.4.6 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

5.6.4.7 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.

5.6.4.8 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.

5.6.4.9 (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. In E2E mode, the slaves will perform delay measurements every 8 seconds by default; a DELAY_REQUEST message is sent to the master, which in turn sends a DELAY_RESPONSE packet back to the slave, containing the time of arrival of the DELAY_REQUEST message. This can be increased in case the network path delay variation in the network is relatively large—this allows for faster reactions to outlier measurements caused by delays within the network.

Meinberg slave devices will limit the effect of an outdated path delay measurement by using filters and optimized PLL algorithms, thus preventing major time jumps in a slave clock, even if high network loads cause measurement outliers. The master clock is observed for a certain time period before the internal oscillator is adjusted. With a low-cost oscillator 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; Meinberg grandmasters specify a DELAY_REQUEST rate of 8 seconds by default.

5.6.4.10 HQ Filter

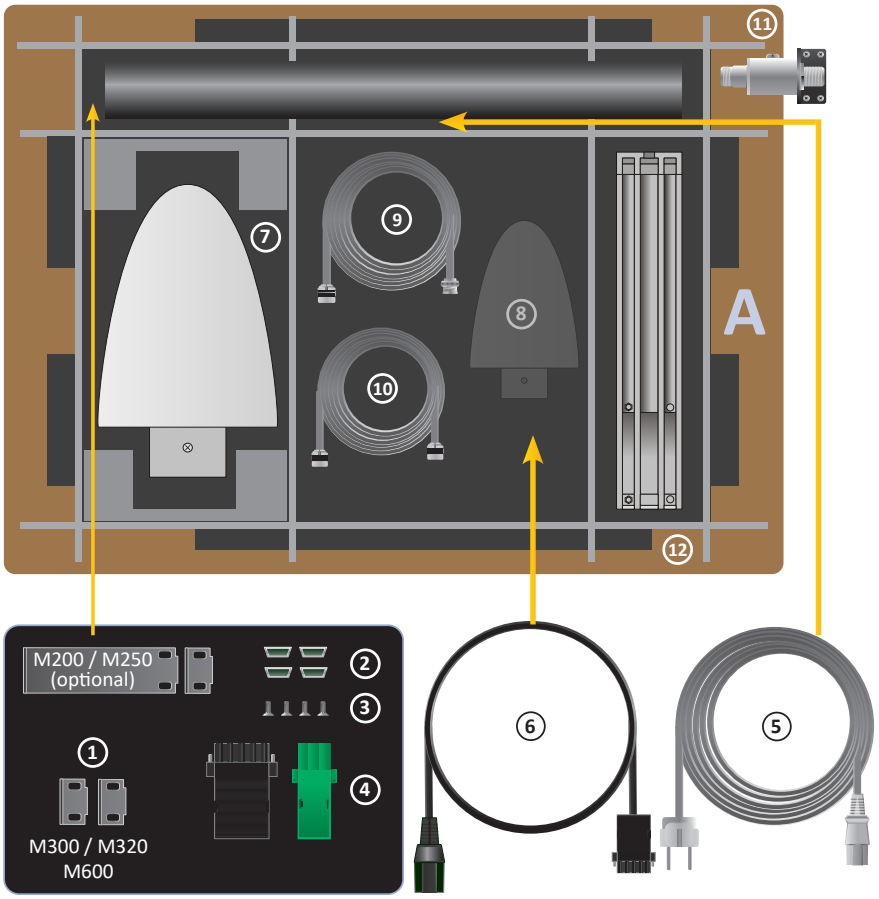
If you use non PTP aware switches in a network where PTP should be used then the timing accuracy of the offset depends on the characteristic of the switches. Non PTP switches will cause time jitters (due to non deterministic delays in each path direction) in PTP measurement. In this section, the term "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.

6 Unboxing

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

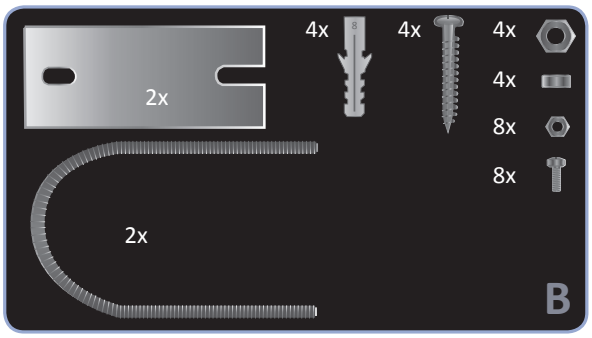


A LANTIME Package Contents

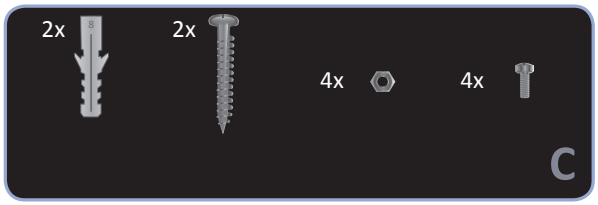
1. Assembly brackets for 19 Inch rack mounting (optional for LANTIME M200 / M250)
2. Protection spacer (M200 / M250 / M300 / M320 / M600 / IMS rack systems)
3. Screws for brackets (M200 / M250 / M300 / M320 / M600 / IMS rack systems)
4. 3-pin DFK connector or 5-pin DFK connector
   (additional connector in case of AC/DC or DC power supply)
5. Power cord (only in case of AC power supply)
6. Option: power cable with 5-pin connector

Only with delivered Antenna

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

7 LANTIME Installation

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

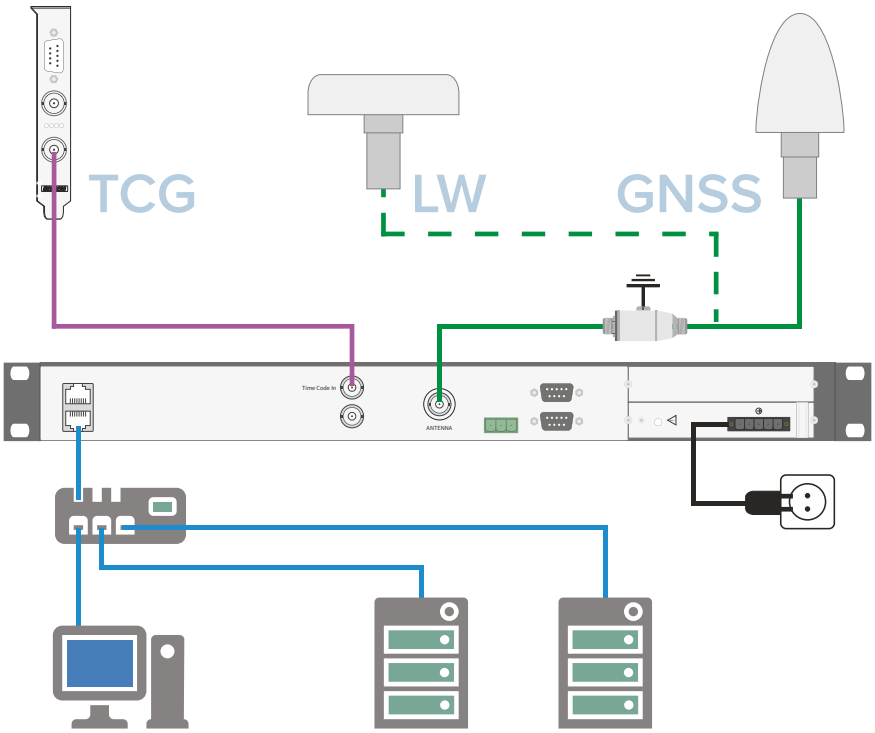


Figure: LANTIME Connection diagram TCG = Time Code Generator; LW = Long Wave Receiver; GNSS = Global Navigation Satellite System

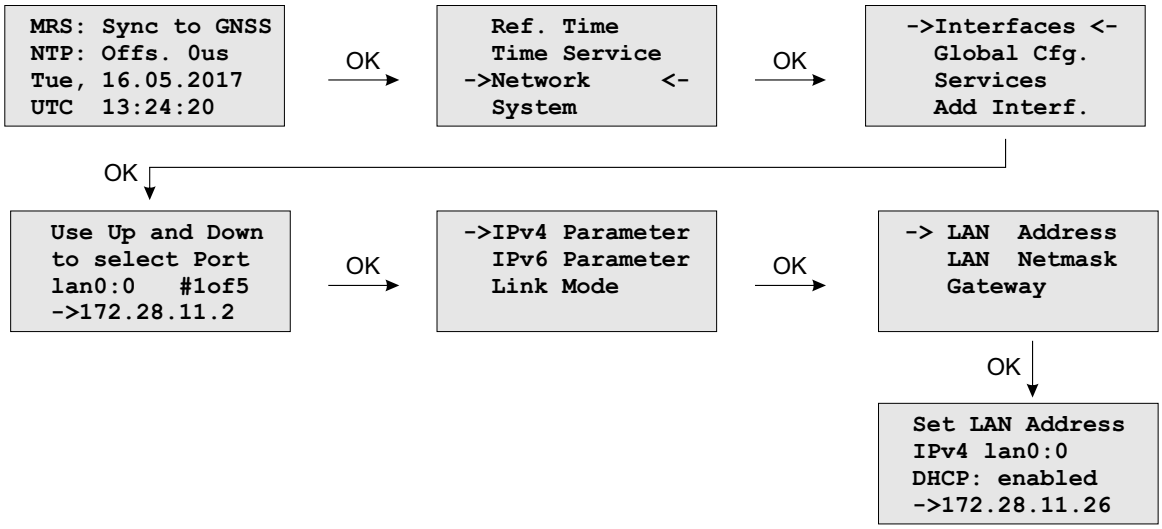
Make sure that the power switch (if available) is in the "0" position (off), and plug the power cord into the power socket of your LANTIME. Then connect the device to your computer network using a suitable network cable. After switching on power, the following message is displayed:

```
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 (↓ | ↑).

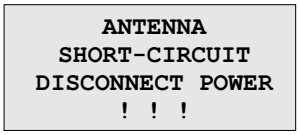
Entering the IP Address manually (not using DHCP)

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:



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 fieldhttp://xxx.xxx.xxx.xxx

2. LOGIN
   user: root
   password: timeserver

8 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, NTS, NTP and SNMP is assumed.

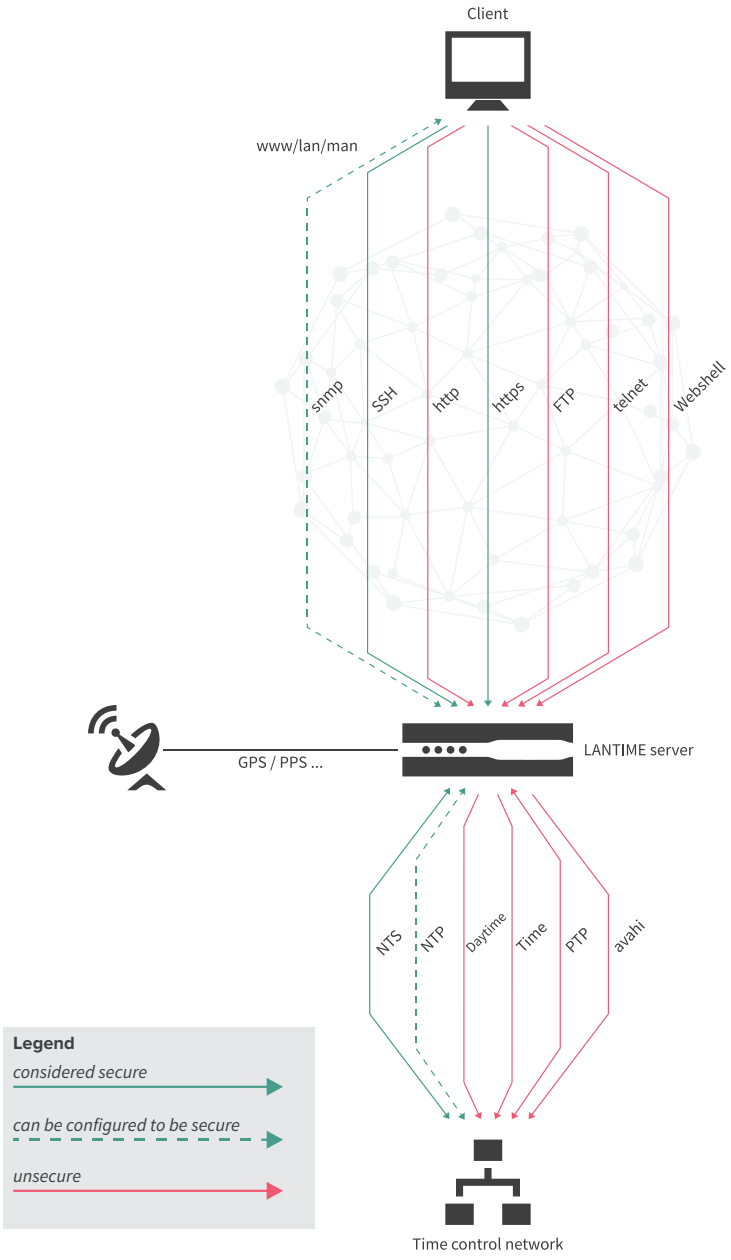


Figure 8.1: LANTIME Services

8.1 General Information

Before you begin configuring your system, review Figure 8.1 to identify which services can be secured.

Generally speaking, a LANTIME can be managed securely over SSH, HTTPS, and SNMP. If configuring your LANTIME over SNMP, the only way to implement a secure connection with the system is via Version 3 of the SNMP protocol. It is recommended to disable any unused services in order to minimize the number of potential attack vectors. You should therefore—if possible—leave only one of the services active (while SNMP does not provide full configuration support, you can still enable the other services on a need basis via SNMP).

Time information via NTS and NTP can be authenticated. Please note that the NTP protocol only provides integrity testing and authentication, not confidentiality. The NTS protocol provides anonymity for clients outside of network boundaries, but while the NTS protocol encrypts sensitive data, the time data itself is not encrypted as it is not considered to be sensitive. The NTS protocol is preferable to the NTP protocol and symmetric key authentication.

The PTP implementation in LTOS does not currently support any IT security features, so the only way to ensure that your synchronization infrastructure is secure is to use NTS and NTP.

Another important aspect is to make sure that the latest browser and service clients are used so as to ensure that the best security algorithms are used for server and client communication. The prompt installation of updates also ensures that vulnerabilities are patched out and the risk of an attack succeeding is minimized.

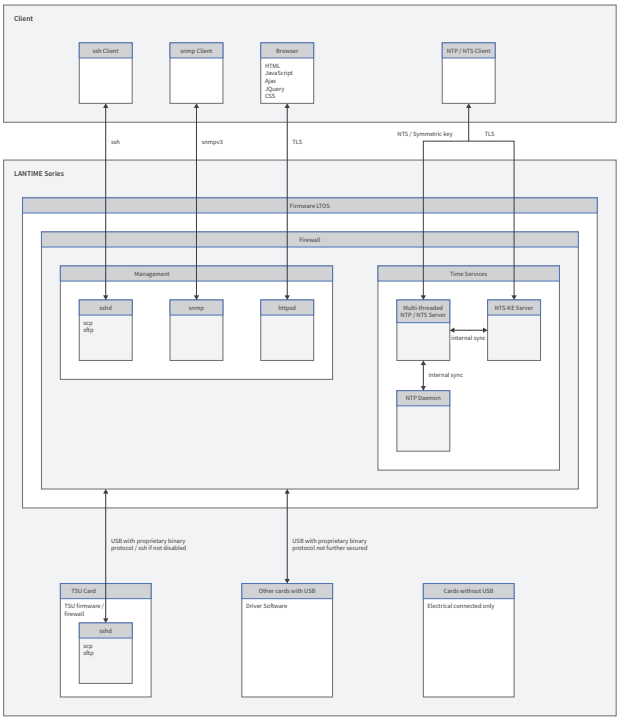


Figure 8.2: The Secure Protocols in Detail

Under recent LTOS v7 versions, Meinberg TSU modules no longer allow an SSH connection to be established over the network; access is only possible via the IMS LANTIME system's CPU module. However, it is still possible to disable a TSU module's SSH service entirely, as shown in Figure 8.3

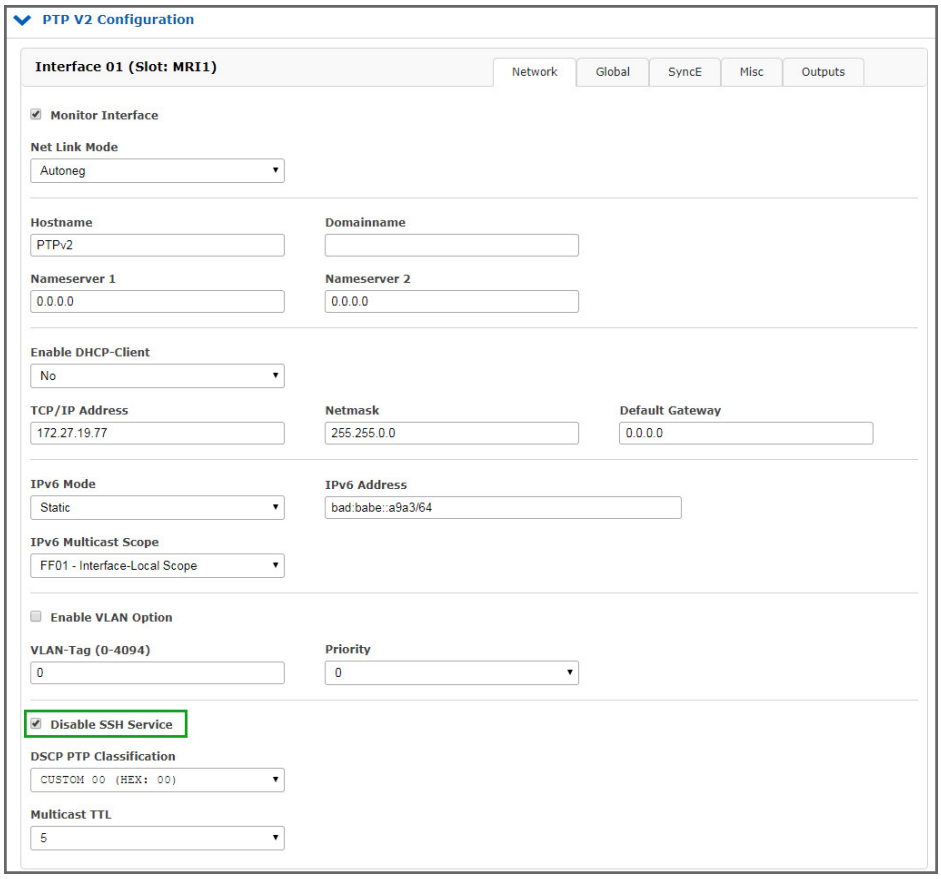


Figure 8.3: Disabling SSH on TSU

Services	Confidentiality	Integ.	Avail.	Auth.	Account.
https	x	x	0	x	(x)
ssh	x	x	0	x	(x)
nts	0	x	0	x	(x)
ntp	-	x	0	x	(x)

Table: Security Targets

The table above briefly illustrates which objectives each of the secure protocols seeks to achieve. While responsibility for actions performed by each user or process is documented in detail by syslog, it remains given that log files can be tampered with by an account with root or superuser permissions. For this reason, the log files cannot be considered to be beyond reproach. The availability of services can be maximized by ensuring that IP blocking is used strategically and the latest updates are always installed. Additional protection can be provided in your network by conventional and web application firewalls capable of detecting and preventing DoS/DDoS attacks.

Whenever any changes are made to the configuration, it is important to bear in mind that these changes will be lost or can be rejected by admins or superusers if not saved to the start-up configuration beforehand.

8.2 Optimizing Management Access Security

The most secure way to configure a LANTIME is to connect the client directly to the LANTIME until only secure channels are left available. This manual uses the Web Interface over SSL as an example.

Once a reference clock is connected and the LANTIME has completed the subsequent start-up process, an IP address can be set via the front panel (see chapter "LTOS Management and Monitoring → Via Web GUI → Network"). Once done, a connection can be established to the Web Interface via the configured IP address, for which the default login credentials should be used to log in:

User: *root*
Password: *timeserver*

Once you have successfully logged in, you should first verify if a new Firmware Version is available (refer to the chapter "Firmware/Software Update" for instructions on how to perform an update). Once any update has been installed, you should generate or inject an SSL certificate—a new certificate will be used in this example. Figure 8.4 shows the button used to launch the generation process.

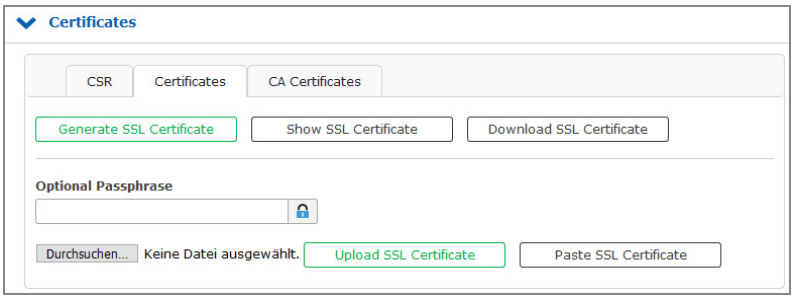


Figure 8.4: Generating an SSL Certificate - Step 1

The next step is to enter the information required for the certificate (refer also to the chapter "LTOS Management and Monitoring → Via Web GUI → Security"). The form is displayed as shown in Figure 8.5. A key length of 2048 bits or higher should be used, and a shorter validity period for certificates is preferable to longer periods. This example uses three years, which is a good trade-off between minimizing the validity period and keeping management costs at an acceptable level.

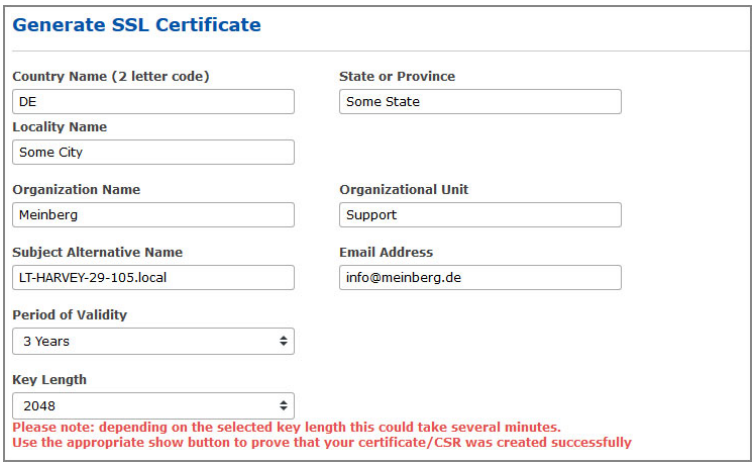


Figure 8.5: Generating an SSL Certificate - Step 2

Figure 8.6: |Displaying the Generated SSL Certificate

The generated certificate can be displayed using the "Show SSL Certificate" button, and the information shown here should be used to compare the new certificate with the certificate provided by your browser when an HTTPS connection is next established with the LANTIME—the two certificates should be identical! Figure 8.7 illustrates the import process. The numbers in the image show the order in which the actions should be performed—Step 4 shows the information that should be compared with the certificate previously downloaded from the LANTIME. If both certificates are identical, you can proceed with Step 5 to confirm the trustworthiness of the LANTIME certificate. Modern browser configurations will display a warning that a connection is insecure when using a self-signed certificate, and for this reason we recommend establishing a public-key infrastructure to suppress the warning. You should also ensure that you use a Subject Alternative Name (SAN), as modern browsers also check for this. To this end, you can generate, download, and sign a certificate request and re-upload the signed certificate via the web frontend as shown in Figure 8.4.

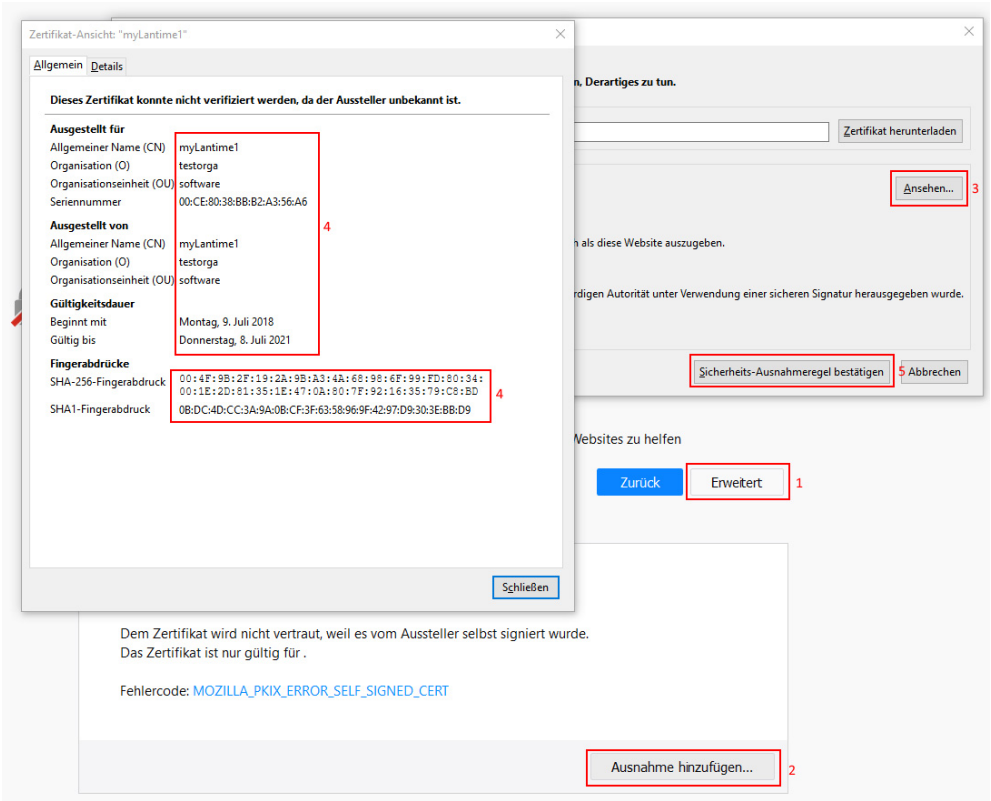


Figure 8.7: Importing the New SSL Certificate into the Browser

Once a connection can be established over HTTPS, you can disable all of the other unused services as shown in Figure 8.8. It is worth noting that this example also only provides HTTPS access via a single network interface to show how scenarios such as a dedicated network for management access are also possible.

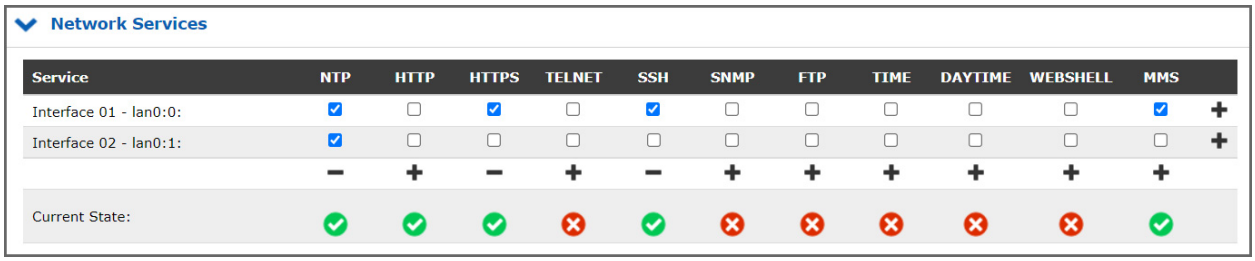


Figure 8.8: Disabling Services

For the next step a second superuser (other than root) is required. Create a new superuser as described in Chapter 8.3. Once the new superuser has been created, log in with the corresponding account credentials and disable root login as described under "Security → Login/Access → Disable Root Login". If necessary, you can also disable the front panel, USB port, and local console as described under "Security → Front Panel" and shown in Figure 8.9. It is also possible to limit Web Interface access to 'whitelisted' IP addresses (note: Remote Access Control is not effective for SSH connections).

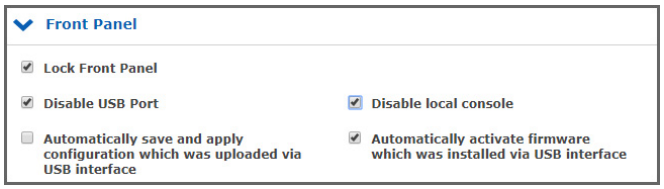


Figure 8.9: Disabling the Front Panel and USB Port

The timeout for web sessions is configured via the "Security" tab in the Web Interface under "Login/Access", which is shown in Figure 8.10—the shorter the timeout, the lesser the security risk.

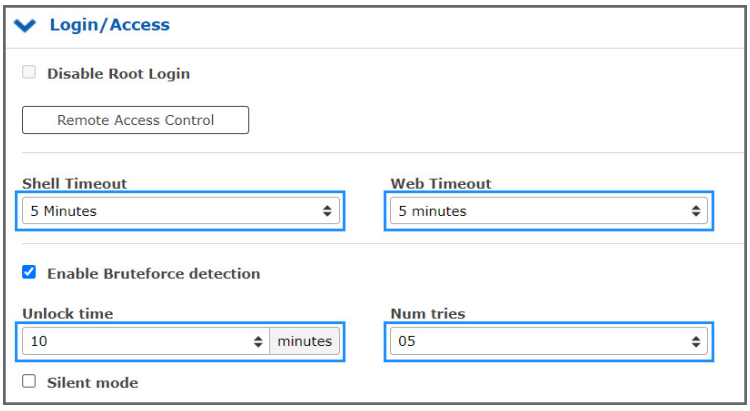


Figure 8.10: Setting the Web Interface Timeout

Brute-force attacks on password phrases can be impeded by enabling "Security → Login → Enable Bruteforce Detection". If a lockout time and a number of attempts is set, accounts will be locked out for that amount of time after the specified number of failed login attempts. It is also possible to enable Silent Mode so that the lockout status of a user account is not disclosed over the SSH interface—this prevents hackers from harvesting a list of valid users, but may also confuse users who accidentally enter the wrong account details too often and are thus unable to subsequently log in using correct credentials during the lockout period.

It is also possible for locked-out users to be notified over the channels configured under "Notification → Notification Events → Faillock: user banned". *syslog-auth.log* also always lists the messages about banned users.

If all of these steps are properly followed, the LANTIME will be configured in such a way that enables it to be managed and monitored securely. Remember to check that the IP configuration and Remote Access Control settings work properly in your live network environment.

You can also optionally configure SNMP to manage your LANTIME. The security options are provided under "Security → SNMP". Figure 8.11 shows the corresponding form.

To establish a secure connection via SNMP, Version 3 and **authPriv** mode must be used. The additional Version 3-specific parameters are Security Name, Rights, Authentication Protocol, and Privacy Protocol, for which SHA512 and AES256 should be used as the authentication and privacy protocol algorithms respectively. As always, longer passwords are preferable. You can then launch the SNMP service from the "Network → Network Services" tab.

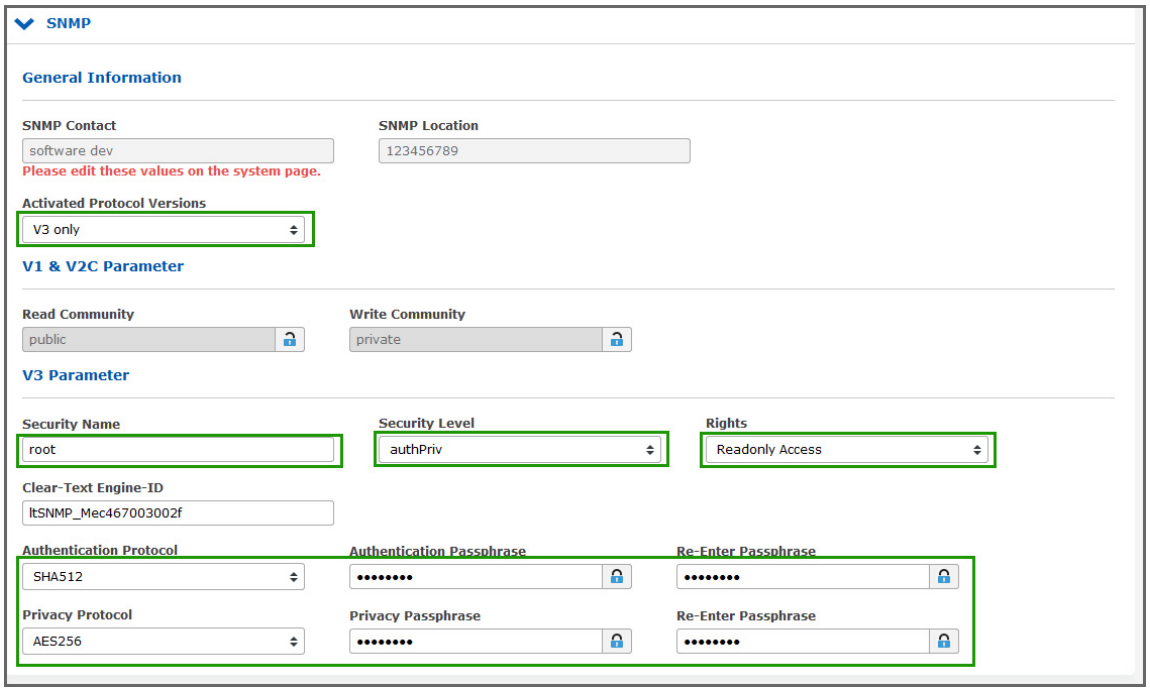


Figure 8.11: SNMP Options

8.3 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 Authentification" for further information.

8.3.1 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.

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 a 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

To create a User, use the form that is shown on Figure 8.12. 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.

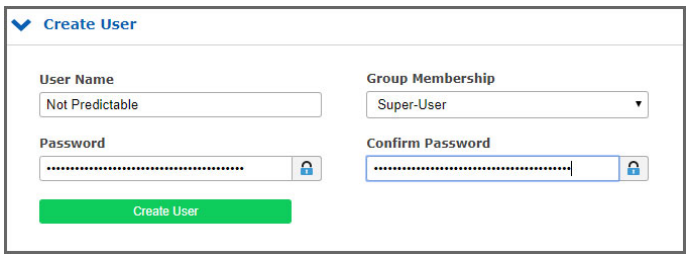


Figure 8.12: Create new Super User

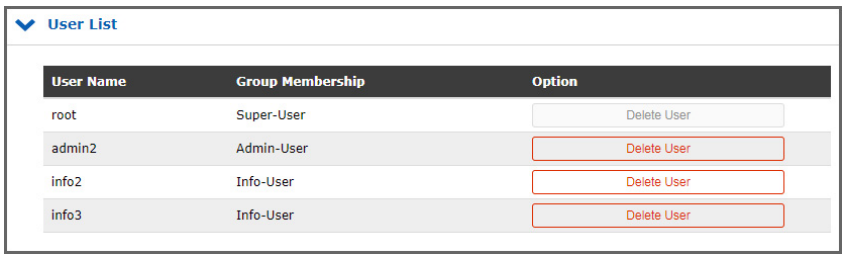


Figure 8.13: User List

For passwords, there are some additional options that are depicted in Figure 8.14. Choose a long password length and a periodical change interval. In addition, you can use the "Allow secure passwords only" checkbox to force a password that contains many different character sets.

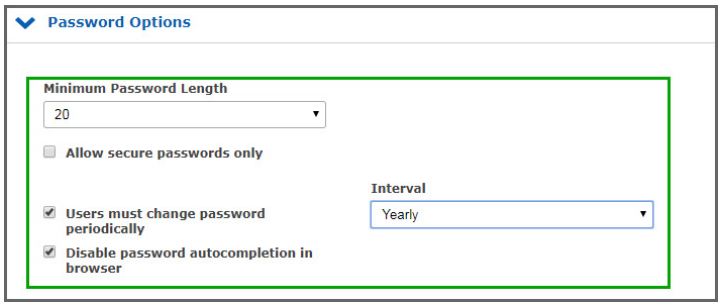


Figure 8.14: Password Options

8.3.2 External User Authentication: LDAP(S), Radius and TACACS+

This chapter describes the possible external authentication methods provided by the LANTIME firmware.

LDAP (Lightweight Directory Access Protocol)
LDAP is based on the client-server model and is used for so-called directory services. LDAP describes the communication between the LDAP client and the directory server. Object-related data, such as personal data or computer configurations, can be read from such a directory.

RADIUS (Remote Authentication Dial-In User Service)
A RADIUS server is a central authentication server used by services to authenticate clients on a physical or virtual network (VPN). The RADIUS server handles the authentication for the service, i.e. checking the user name and password.

TACACS (Terminal Access Controller Access-Control-System)
TACACS is a communication protocol for authentication, which is standardized and widely used by the IETF. TACACS servers provide a central authentication instance for users. In typical Cisco network environments (e.g. routers and switches), TACACS+ is used for central user management.

8.3.2.1 Order of Authentication Procedures

The order of authentication is as follows once all authentication methods (LDAP, RADIUS, TACACS+ and LOCAL) have been activated and configured

1. LDAP
2. RADIUS
3. TACACS+
4. local authentication

So if the same user names/password phrases are used in different systems, it is possible that the access rights do not work out as desired. In addition, this can quickly lead to intransparent log messages. So you should always pay attention to the order and consistent user data/rights in the services.

8.3.2.2 LDAP and LDAPS

The LANTIME supports the connection to an LDAP server via LDAP and LDAPS. Meinberg recommends setting up secure communication via LDAPS. For this purpose a central trust center (RootCA) must be made known to the LANTIME.

A certificate of a certification authority can be uploaded via the web interface menu "Security →" Certificates → CA Certificates". The section CA Certificates describes the options for uploading root CA certificates. If the LDAP server uses a certificate signed/issued by a global certificate authority, this step is omitted. The list of trusted global certificate authorities is updated with each LANTIME update.

The configuration of an LDAP(S) connection is described in chapter "Web Interface → User Management → External Authentication → 10.1.9.7 (LDAP Setup)".

8.3.2.3 External Authentication via LDAP

External authentication via LDAP can be configured in the web interface under "System → User Management → User Administration → External Authentication → LDAP / LDAPS". The LANTIME firmware supports anonymous as well as user related logon. For a Microsoft Active Directory logon, a user name (LDAP user or binddn) and a password phrase (LDAP password or bindpw) must be specified. The search strategy (Search Scope) for AD entries can be changed via base (baseObject), one (singleLevel) and sub (wholeSubtree). The corresponding search path in AD can be specified via the field "Search Base". An example for a path would be *"CN=Users,DC=test,DC=mbg,DC=en"*.

To map the AD information to the local settings, "Filter" and "Mappings" must be created. In AD, the attributes that contain the information needed for a LTOS user can be freely selected. A filter is specified to limit the result set of the LDAP response to the required attributes. The mapping is needed to map attributes of the LDAP directory service that differ from RFC2307 to the correct attributes specified in the RFC that are used by the LDAP service on the LANTIME. For example, the user ID for the passwd mapping is mapped from the freely selected attribute "sAMAccountName" to the attribute "uid" provided for this purpose in RFC2307 by the following mapping: *"passwd uid sAMAccountName"*.

The minimum information to be provided is:

- The User-ID (the login name)
- The User ID number (a number that is not or could not be assigned by a local user)
- The User group number (see below for group membership)
- The user home directory (new folder under /home/)

The only value that cannot be freely assigned in the directory server is the group membership in LTOS. The following values can be stored e.g. in the "gidNumber" attribute:

- The group Super-User has the group ID = 0
- The group Admin-User has the group ID = 4
- The group Info-User has the group ID = 100

The connection to the LDAP server can be specified under the menu item "Global" as soon as a new LDAP server has been added via the button "Add LDAP Server". You can choose between "ldap" and "ldaps" and the URI of the LDAP server must be specified.

Hint
For a LDAPS connection, the URI must match the URI (in the Common Name or the Subject Alternative Names) of the LDAP server certificate, otherwise the verification fails.

The mode controls whether a configured LDAP server is queried. If the port differs from the defaults (389, 636), another can be selected using the "Alternative Port" field. LDAP servers can be removed via the "Misc" tab. If everything is set, the settings must be transferred to the current configuration by clicking the button "**Save**". After the function test the current configuration can be saved as start configuration.

For the current firmware version 7.02.003, error messages of the ldap service can be viewed via the system messages (CLI or WEB). Authentication errors are written to the */var/log/auth.log* file.

8.3.2.4 Radius and TACACS+ Connection

In addition to the LANTIME's own internal user management, it is also possible to authenticate users via a Radius or TACACS+ connection. Such a connection is configured under User Administration → Add External Authentication Server. See Figure 8.15 for an illustration of the configuration options. External Authentication must first be enabled. Radius or TACACS+ should be then be selected from the drop-down menu and the hostname, the previously exchanged key (shared secret), and the correct port should be entered. You will now be able to log in using the external authentication mechanism. The system will first query the external server for the user; if no user exists with the specified credentials, the system will query the local users. The process of configuring an external authentication server is described in the chapter "LTOS Management and Monitoring → Via Web GUI → External Authentication Options".

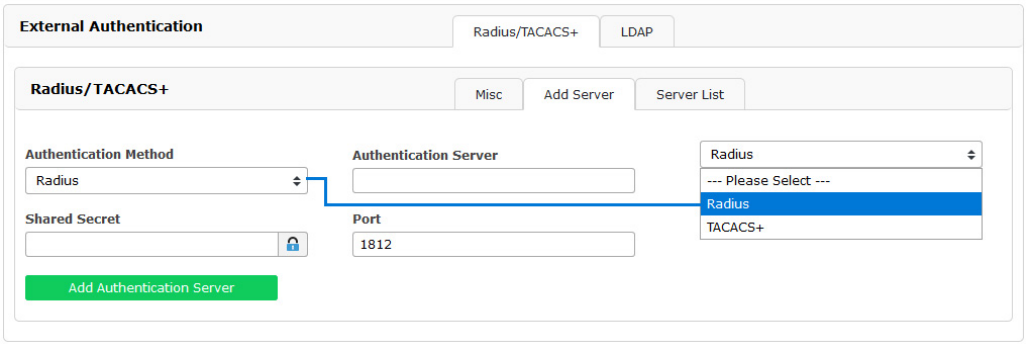


Figure 8.15: Webinterface Menu "System → User Management → External Authentification"

8.4 Securing NTP and NTS

8.4.1 Securing the NTP Time Service

The NTP time service provides several methods of authenticating and monitoring the integrity of packet transmission. At the time of writing, the NTP autokey method is considered to be insecure, which is why this guide only explains how to configure the symmetric key method and the Network Time Security implementation.

Please refer to "LTOS Management and Monitoring → Via Web GUI → NTP" for a detailed description of each of the configuration options.

8.4.1.1 Configuring Symmetric Key Authentication

To configure a connection, the system requires a key. You can either use newly generated keys or add existing keys to the key file using the **Edit NTP Keys** button, which is located under "NTP → NTP Symmetric Keys". If you have keys automatically generated by the system, MD5 and SHA1 keys will be added to the key file. However, for the best security currently available, AES-128-CMAC keys should be used, and these cannot yet be generated automatically.

The process of generating AES-128-CMAC keys is described in the chapter "Configuration → Web Interface → NTP → NTP Symmetric Keys".

Figure 8.16 shows examples of generated and manually modified (AES-128-CMAC) NTP keys. The key IDs must be added to the Trusted Keys under the **General Settings** section of the **NTP** tab (see Figure 8.17). In the **NTP Restrictions** section you can also disable Mode 6 and 7 packet support. It is also possible to enable access controls here here so that access is only granted to known IP addresses. The symmetric keys are used for all connection types, i.e. server-to-client connections, connections with external NTP servers, broadcast connections, multicast connections, and manycast connections.

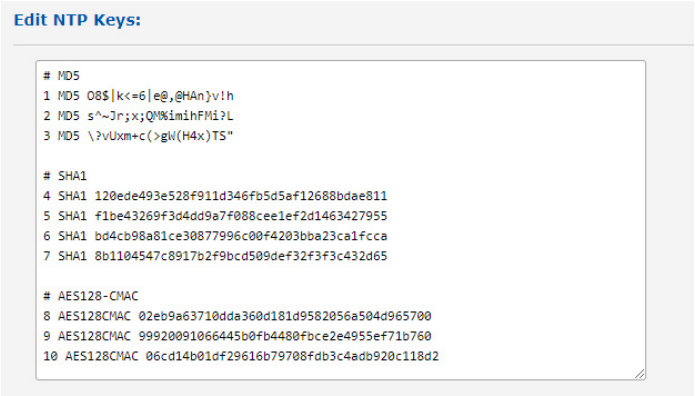


Figure 8.16: Symmetric NTP Keys

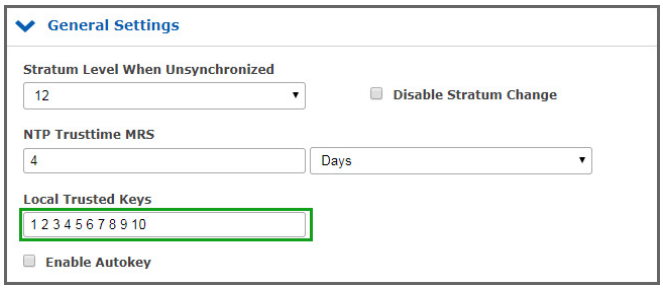


Figure 8.17: Trusted Key IDs

The relevant fields for the proper key IDs are marked in Figures 8.18, 8.19, and 8.20. An example configuration file for a client is illustrated in Figure 8.21, showing the path to the key file, the trusted key IDs, and the server IP, which in this case use the key with the ID 1.

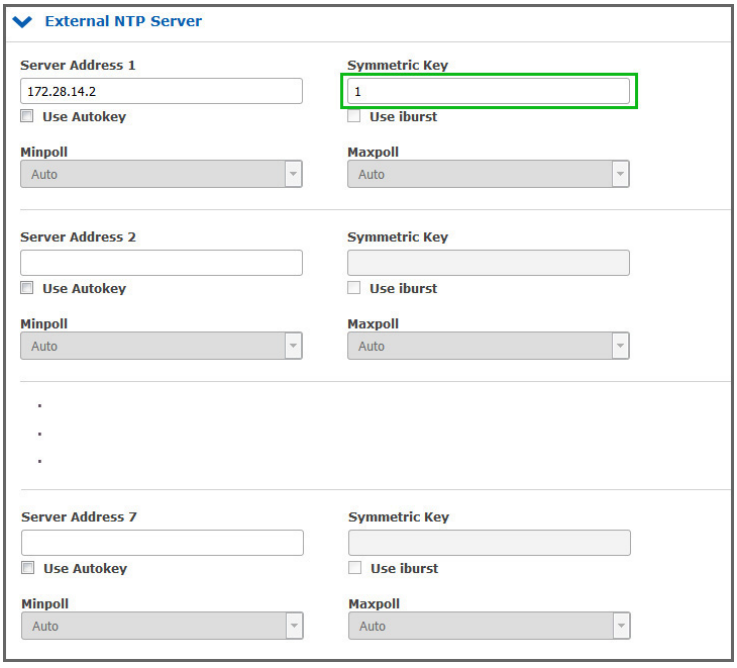


Figure 8.18: External server configuration

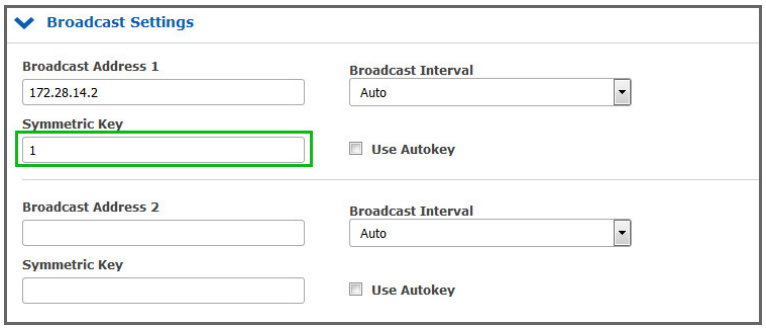


Figure 8.19: Broadcast configuration

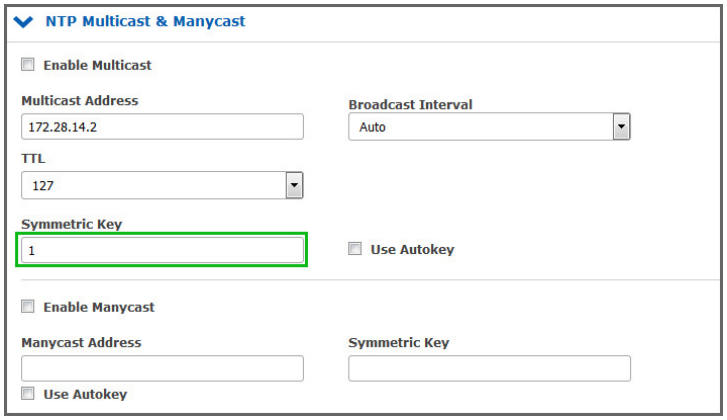


Figure 8.20: Multi and many cast configuration

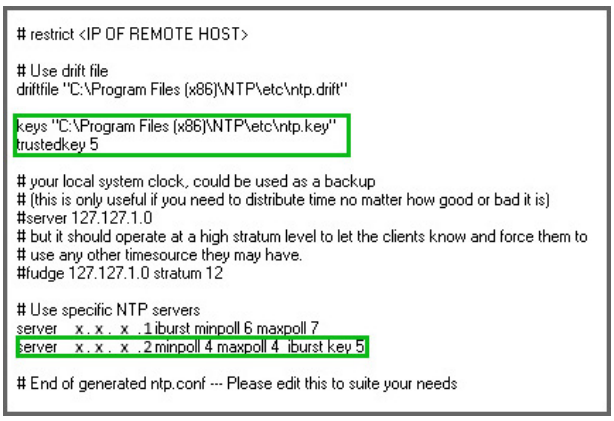


Figure 8.21: NTP client configuration

8.4.2 Configuration of Network Time Security (NTS)

As of Version 7.08, LTOS provides Network Time Security (NTS) support in both server and client mode.

8.4.2.1 Configuring the LANTIME System to Operate as an NTS Server

Information:

This option is not available on LANTIME systems using a CPU module type C05F1.

The NTS server mode of LTOS comprises both an NTS key establishment server and an NTP server implementation with NTS support. For TLS-based communication, the key establishment server uses the same SSL certificate used by the web server for HTTPS access.

As such, the presence of a valid SSL certificate is required for the operation of an NTS server on a LANTIME device. Please refer to the chapters Optimizing Management Access Security and Certificates for more information on how to generate or inject an SSL certificate.

Figure 8.22: Web Interface Menu "NTP → NTS Configuration"

To enable NTS server mode, activate the checkbox "Enable NTS Server" under "NTP → NTS Configuration" (see illustration 8.22).

8.4.2.2 Configuring Network Time Security for External NTP Servers

Note: This option is currently only supported on LANTIME/MRS devices.

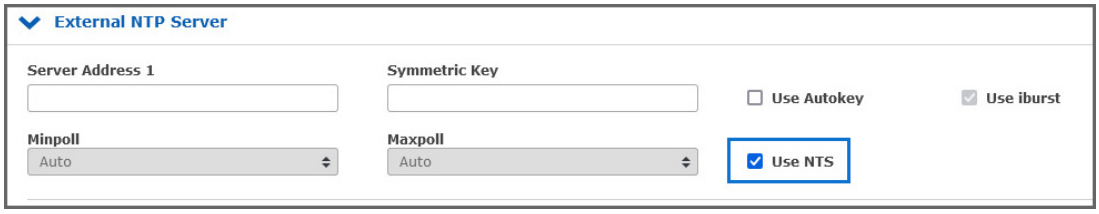


Figure 8.23: External NTP Server

To enable NTS-secured time synchronization with external NTP servers, "Use NTS" must be checked in the menu "NTP → External NTP Server" (see Figure 8.23). The **Server Address** must be the IP address or hostname of the corresponding NTS-KE server in this case.

When connecting to a NTS-KE server with a TLS certificate signed by a public certificate authority, it will not usually be necessary to take any further action. It is important to ensure that the system's own root certificates are also verified under "Security → Certificates → CA Certificates".

If the NTS-KE server is a non-public one, the corresponding root certificate must be present on the LANTIME device. For more information on the process of uploading custom CA certificates, please refer to the chapter "CA Certificates".

8.5 Event Log Delivery

The LANTIME offers many transport channels for event log information and a fine grained notification selection for each of these channels. Currently, Syslog and SNMPv3 can be secured from the event transport channels. It is a good practice to collect event log informations on a central server to correlate and check them for anomalies. Be aware of potential security related information leakage due to the lack of encryption for services other than **syslog** and **SNMPv3**.

External syslog servers can be configured under "Notifications → External syslog servers". To address them securely the transport protocol "TLS" must be selected. The full configuration options are described in chapter "Web Interface → Notification → External Syslog Server".

The chapter "LTOS Management and Monitoring → Via Web GUI → Notification" describes the configuration options for the transport channels. If you use **SNMPv3** with selected **authPriv** security level, SNMP traps are also sent securely. Configure the SNMP authPriv setting as described in "Security → SNMP" in chapter Optimizing Management Access Security.

8.6 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 8.24. The LTOS V7 firmware is equipped with a digital signature, which is checked during the "Preflight Checks" test directly after upload. If this test detects a faulty signature, a warning is displayed. If this happens, download the new firmware from the Meinberg web site again and repeat the process. In case of repeated warnings please contact the Meinberg support.

In the next step, you have to confirm the update and activate the new firmware like in Figure 8.25. The update was successful if Figure 8.26 is displayed.

Figure 8.24: Upload firmware

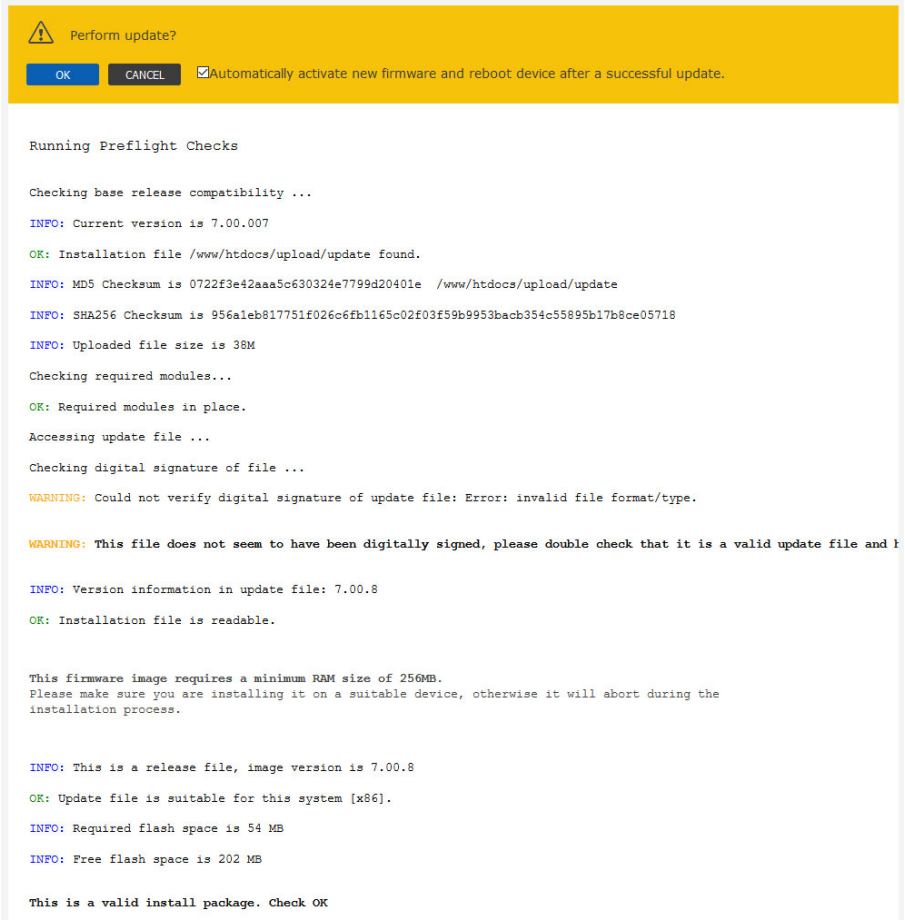


Figure 8.25: Update process of the firmware

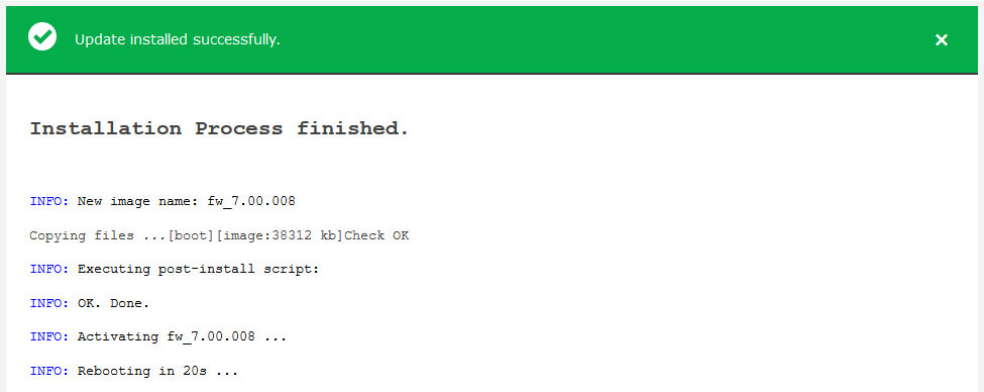


Figure 8.26: Successful firmware update

The configuration settings of the LANTIME will be preserved during a firmware update, except the configuration files of the web server and the SSH service. These files will be overwritten during an update to be able to deliver current cryptographic methods with an update. If, contrary to our recommendation, the automatic update is not desired, a separate customer-specific configuration file can be stored for these services.

SSH configuration:
The configuration file /etc/ssh/ssh.cfg defines which configuration file the SSH service should use. In factory configuration the file contains the following entry:

```
[SSHD]
CONFIGFILE=/etc/standard/sshd_config
```

If the file */etc/standard/sshd_config* is defined as an SSH configuration file, this file is updated during a firmware update. If the file */etc/ssh/sshd_config* is entered, an own configuration can be created in this file, which is not replaced during an update.

Web server configuration:
The configuration file */etc/webUI/webUI_custom.cfg* defines which configuration file the web server should use. In the factory configuration the file contains the following entry:

```
[CUSTOM CONFIGURATION]
CUSTOM_CONFIG_PATH=
```

If no file is defined as web server configuration file, the factory configuration file, which is updated during a firmware update, is used. If an arbitrary file is entered under */mnt/flash/data/*, an own configuration can be created in this file, which is not replaced during an update. Files that are stored under */mnt/flash/data/* are not part of a configuration, but they are stored reboot-secure (persistent).

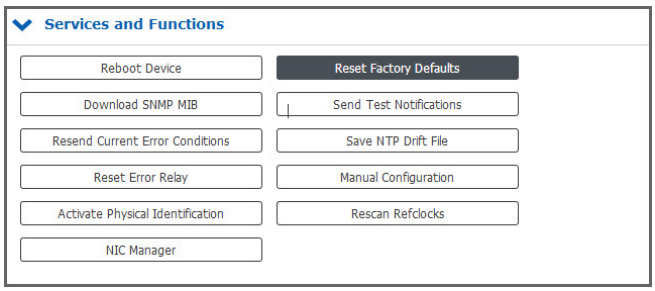


Figure 8.27: Reset factory defaults

To restore automatic configuration updates to the SSH service and the Web server, you can restore the factory paths in these two files.

Restoring the factory defaults via the web interface, as shown in 8.27, resets all custom configuration settings in the current startup configuration except the network settings. In detail, this means that your certificates, credentials, SNMP, NTP and SSH keys, among others, will be lost. Configurations previously saved under a different name are retained even in the event of a factory reset. If desired, these configurations must also be deleted via the web interface.

After the reset via the web interface, all certificates are exchanged to the factory defaults. The SSH key is randomly regenerated at startup after reset.

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.

9 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.

9.1 Reference Time Sources

9.1.1 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.

9.1.2 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.

GPS was installed by the United States Department of Defense (US DoD) and operates at two performance levels: the Standard Positioning Service, or SPS, and the Precise Positioning Service, or PPS. The structure of the messages transmitted by the SPS has been openly published and reception is provided for public use. The timing and navigation data of the more precise PPS is encrypted and is thus only accessible to certain (usually military) users.

GLONASS was originally developed by the Russian military for real-time navigation and ballistic missile guidance systems. GLONASS satellites also send two types of signal: a Standard Precision Signal (SP) and an encrypted High Precision Signal (HP).

BeiDou is a Chinese satellite navigation system. The second-generation system, officially referred to as the BeiDou Navigation Satellite System (BDS) and also known as "COMPASS", consists of 35 satellites. BeiDou entered service in December 2011 with ten satellites and was made available to users in the Asia-Pacific region. The system was completed in June 2020 with the launch of the final satellite.

Galileo is an in-development global European satellite navigation and time reference system controlled by a civilian authority (European Union Agency for the Space Programme, EUSPA). Its purpose is the worldwide delivery of high-precision navigation data and is similarly structured to the American GPS, Russian GLONASS and Chinese BeiDou systems. The main differences in the systems lie in their approaches to frequency usage & modulation and the satellite constellation.

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.

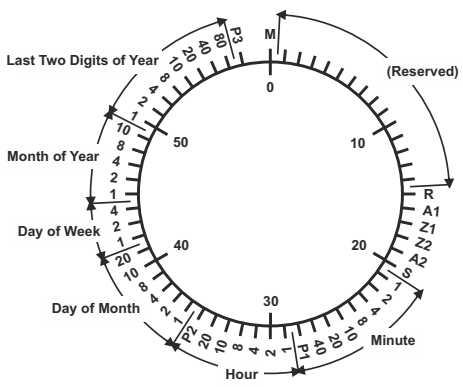
9.1.3 PZF - DCF77 Long Wave Receiver

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.

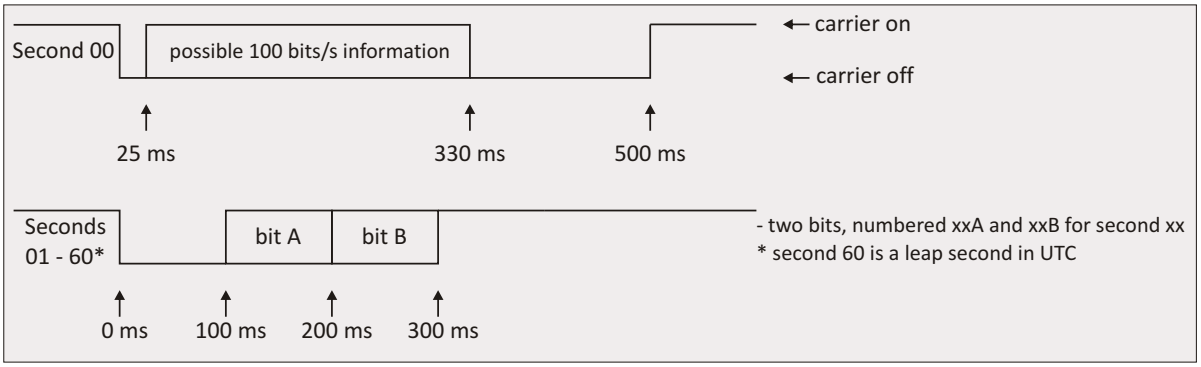
9.1.4 MSF Receiver

The transmission of the MSF signal from Anthorn 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 +-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 +/-800ms. 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.

9.1.5 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.

9.1.6 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.

9.2 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° 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° North and 55° 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).

9.2.1 Installing a GPSANTv2

The following chapters explain how to select a suitable location for your antenna, how to fit the antenna, and how to implement effective anti-surge protection for your antenna installation.

9.2.1.1 Selecting the Antenna Location

There are essentially two ways a compatible Meinberg GPS Antenna (such as a GPSANTv2) can be installed using the accessories included:

1. Mounted on a pole

2. Mounted on a wall

To avoid difficulties with synchronization of your connected Meinberg product, select a location that allows for an unobstructed view of the sky (Fig. 1) so as to ensure that enough satellites can be found.

To ensure that your antenna has the best 360° view possible, Meinberg recommends mounting the antenna on a roof on a suitable metal pole (see Fig. 1, antenna on right). If this is not possible, the antenna may be mounted on the wall of a building, but must be high enough above the edge of the roof (see Fig. 1, antenna on left).

This prevents the line of sight between the antenna and the satellites from being partially or fully obstructed and limits the impact of GNSS signal reflections from other surfaces such as house walls.

1. Mounted on a pole
2. Antenna Cable
3. Mounted on a wall
4. Point of entry into building

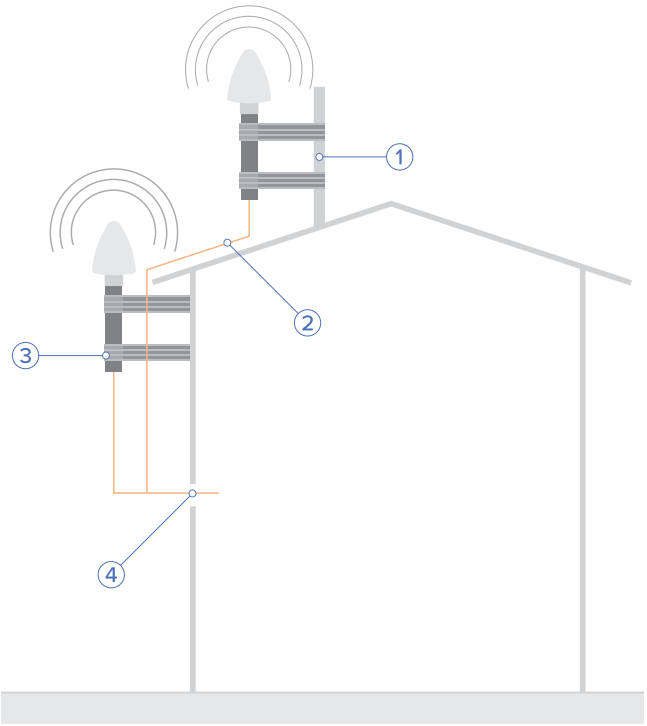


Fig. 1: Ideal Positioning

If there is a solid obstacle (a building or part of a building) in the line of sight between the antenna and each of the satellites (see Fig. 2), it is likely that the satellite signals will be partially or fully obstructed or that reflected signals will cause interference, causing problems with signal reception.

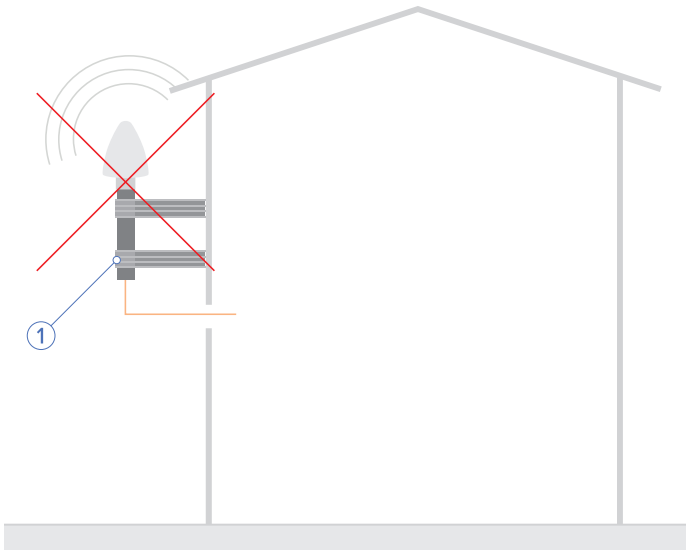


Fig. 2: Not recommended positioning of a wall-mounted antenna (1)

There must also be no conductive objects, overhead power lines, or other electrical lighting or power circuits within the signal cone of the antenna (approx. 98 degrees), as these can cause interference in the already weak signals transmitted in the frequency band of the satellites.

Other Installation Criteria for Optimum Operation:

- Vertical installation of antenna (see Fig. 1)
- At least 50 cm (1.5 ft) distance to other antennas
- A clear view towards the equator
- A clear view between the 55th north and 55th south parallels (satellite orbits).

Information:

Problems may arise with the synchronization of your Meinberg product if these conditions are not met, as four satellites must be located to calculate the exact position.

9.2.1.2 Installation of the Antenna

Please read the following safety information carefully before installing the antenna and ensure that it is observed during the installation.

Danger!

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 at height without a suitable and effective fall arrester!

Danger!

Do not work on the antenna installation during thunderstorms!

Danger of death from electric shock!

- Do not carry out any work on the antenna installation or the antenna cable if there is a risk of lightning strike.
- Do not perform any work on the antenna installation if it is not possible to maintain the prescribed safety distance from exposed power lines or electrical substations.

Mount the Meinberg GPSANTv2 Antenna or GNSS Multi-Band Antenna (as shown in Fig. 3) at a distance of at least 50 cm to other antennas using the mounting kit provided, either onto a vertical pole of no more than 60 mm diameter or directly onto a wall.

Item	Description	QTY
1	Antenna	1
2	M8 grounding stud	1
3	safety washer	1
4	M8 hex nut	1
5	Antenna pole	1
6	M4 hex nut	8
7	M4 x 12 phillips-head screw	8
8	threaded U-bolt (pole diameter max. 60 mm)	2
9	M6 spacer	4
10	M6 hex nut	4
11	pole clamp halves	4
12	pole bracket	2

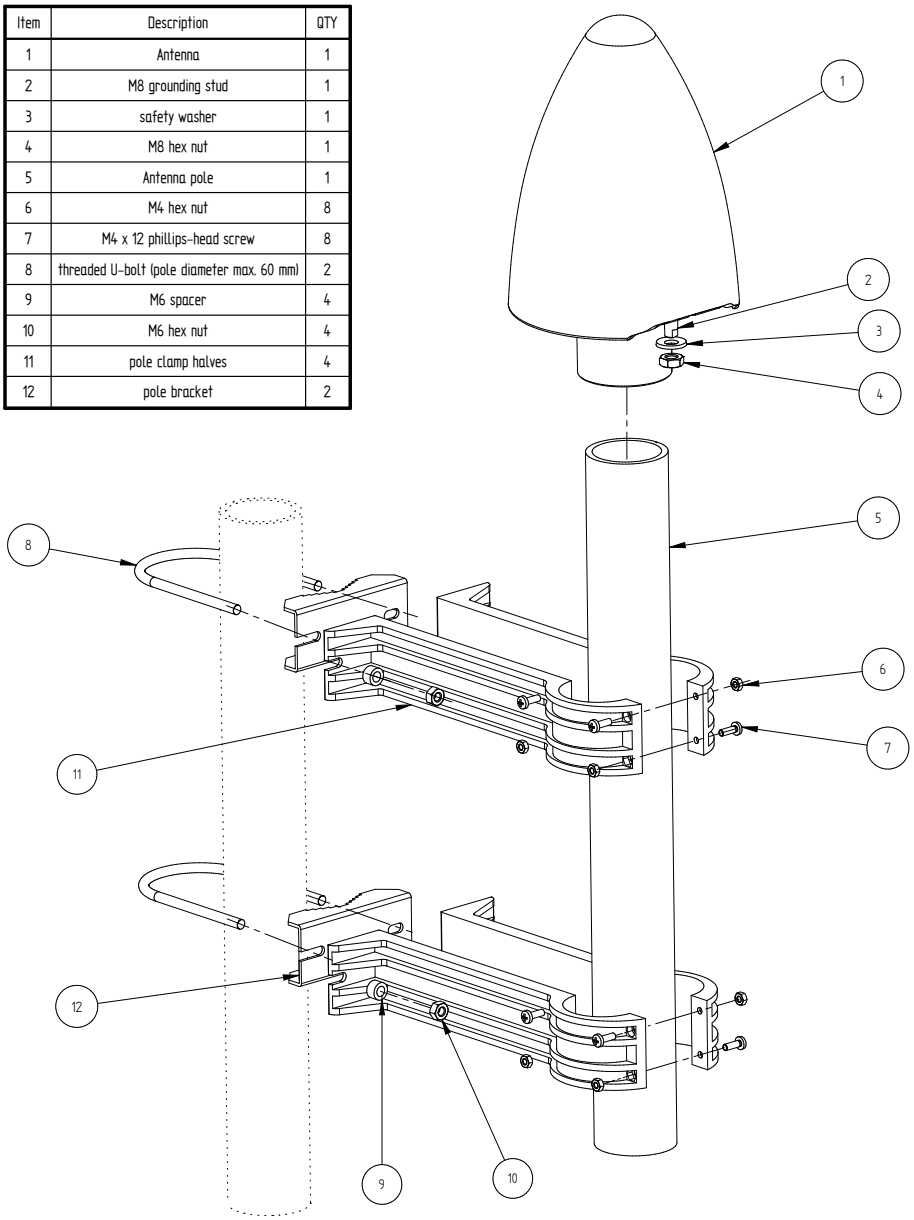


Fig. 3: Mounting a Meinberg GPS Antenna or GNSS Multi-Band Antenna onto a Pole

Fig. 3 illustrates the mounting of a Meinberg Antenna on a pole by way of example. When mounting the antenna on a wall, the four wall plugs and M6x45 screws should be used to mount the two halves of the pole clamp (Fig. 3, Pos. 12) using the provided screw slits.

The next chapter explains how the antenna cable should be laid.

9.2.1.3 Antenna Cable

Selecting the Appropriate Cable

Meinberg provides suitable cable types with its antennas and these are ordered together with the antenna to match the length you need from your antenna to your Meinberg reference clock. The route to be covered for your antenna installation should be determined and the appropriate cable type selected accordingly before confirming your order.

Important!

Please avoid using a mixture of different cable types for your antenna installation. This should be taken into consideration in particular when purchasing additional cable, for example to extend an existing cable installation.

The cable is shipped with both ends fitted with the appropriate connectors as standard, although the cable can also be shipped without any pre-fitted connectors if so requested.

GPS/GNS-UC Clocks

The table below shows the specifications of the supported cable types for the transmission of the 35 MHz intermediate frequency:

Cable Type	RG58C/U	RG213	H2010 (Ultraflex)
Signal Propagation Time at 35 MHz*	503 ns/100 m	509 ns/100 m	387 ns/100 m
Attenuation at 35 MHz	8.48 dB/100 m	3.46 dB/100 m	2.29 dB/100 m
DC Resistance	5.3 Ω/100 m	1.0 Ω/100 m	1.24 Ω/100 m
Cable Diameter	5 mm	10.3 mm	10.2 mm
Max. Cable Length	300 m	700 m	1100 m

Table: Specifications of Cable Types Recommended by Meinberg

** The propagation times are specified on the basis of 100 m cable; these values can be used as a reference to calculate the propagation time of any other arbitrary length of cable.*

Laying the Antenna Cable

When laying the antenna cable, ensure that the specified maximum cable length is not exceeded. This length will depend on the selected cable type and its attenuation factor. If the specified maximum length is exceeded, correct transmission of the synchronization data and thus proper synchronization of the reference clock can no longer be guaranteed.

Lay the coaxial cable from the antenna to the point of entry into the building as shown in Figures 5 and 6 in the chapter "Surge Protection and Grounding". Like any other metallic object in the antenna installation (antenna and pole), the antenna cable must be integrated into the grounding infrastructure of the building and also connected to the other metallic objects.

Caution!

When laying the antenna cable, ensure that sufficient distance is maintained from live cables (such as high-voltage power lines), as these can cause severe interference and compromise the quality of the antenna signal significantly. Surges in power lines (caused, for example, by lightning strike) can generate induced voltages in a nearby antenna cable and damage your system.

Further Points to Consider when Laying Antenna Cable:

- The minimum bend radius of the cable must be observed.[1]
- Any kinking, crushing, or other damage to the external insulation must be avoided.
- Any damage or contamination of the coaxial connectors must be avoided.

[1] *The bend radius is the radius at which a cable can be bent without sustaining damage (including kinks).*

Compensating for Signal Propagation Time

GPS/GNS-UC Clocks

The propagation of the signal from the antenna to the receiver (reference clock) can incur a certain delay. This delay can be compensated for in the LANTIME Web Interface.

To do this, log into the Web Interface of your LANTIME system and proceed as follows:

1. Open the menu "**Clock**" → "**State & Configuration**".
2. Select the corresponding clock module.
3. Click on the "**Miscellaneous**" tab.
4. Select the compensation method and enter the appropriate value.

A fixed offset value for the propagation delay can be entered in nanoseconds by selecting "**By Delay**" as the offset method. This value is calculated either based on the cable specifications provided in the data sheet of your cable or based on your own delay measurements.

A manually calculated signal propagation offset will provide the best accuracy. However, the length of the cable can also be entered in meters by selecting "**By Length**" to provide an automatically estimated offset based on the known specifications of standard RG58 cable.

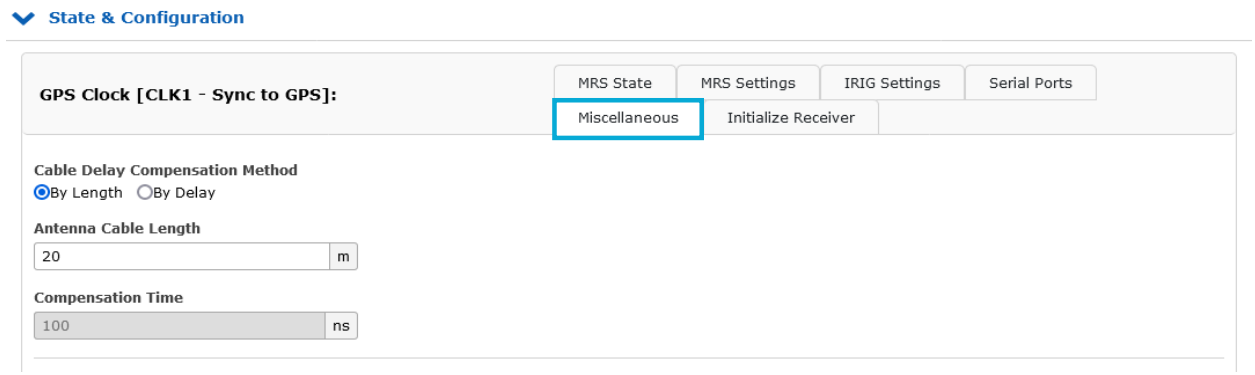


Fig. 4.1: "Clock" menu in LANTIME OS Web Interface

→ Chapter 9.4, "Surge Protection and Grounding" explains how to implement effective surge protection for an antenna installation.

9.2.2 Installation of a GNSS Antenna

Two different antennas are available for our combined GPS/GLONASS/Galileo/BeiDou satellite receivers that are each designed to fulfill different tasks or applications.

The active Multi-GNSS L1 antenna is the standard accessory and can receive signals from the GPS, GLONASS, Galileo, and BeiDou satellite systems. This antenna is ideal for fixed-location systems, operates using a 5 V DC supply voltage supplied by the receiver, and features an integrated surge protector.

For mobile applications, such as cars, RVs, vans, ships, trains, and aircraft, we recommend the use of the RV-76G, an active GNSS antenna that is suitable for direct installation in an enclosure (chassis, panels, etc.)

9.2.2.1 Selecting the Antenna Location

There are essentially two ways the Multi-GNSS Antenna can be installed using the accessories included:

1. Mounted on a pole

2. Mounted on a wall

To avoid difficulties with synchronization of your Meinberg time server, select a location that allows for an unobstructed view of the sky (fig. 1) so as to ensure that enough satellites can be found.

To ensure that your antenna has the best 360° view possible, Meinberg recommends mounting the antenna on a roof on a suitable metal pole (see Fig. 1, antenna illustration on right). If this is not possible, the antenna may be mounted on the wall of a building, but must be high enough above the edge of the roof (see Fig. 1, antenna illustration on left).

This prevents the line of sight between the antenna and the satellites from being partially or fully obstructed and limits the impact of GNSS signal reflections from other surfaces such as house walls.

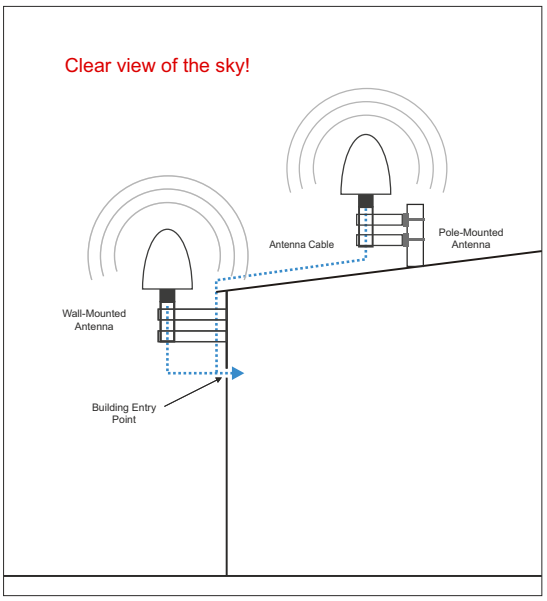


Fig. 1: Ideal Positioning

If there is a solid obstacle (a building or part of a building) in the line of sight between the antenna and each of the satellites (see Fig. 2), it is likely that the satellite signals will be partially or fully obstructed or reflected signals will cause interference, causing problems with signal reception.

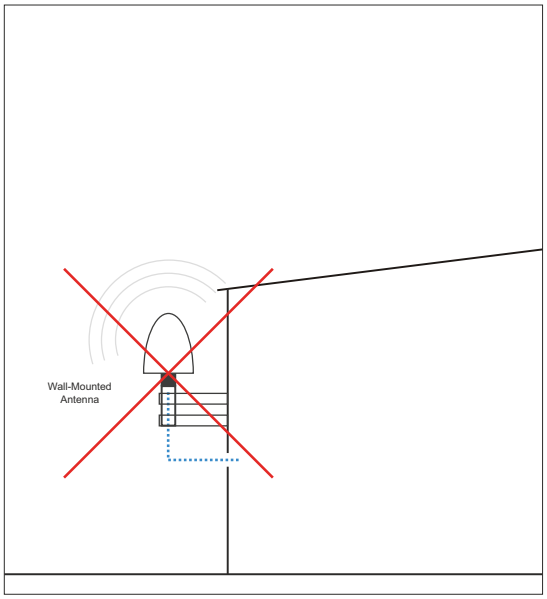


Fig. 2: Poor positioning of a wall-mounted antenna

There must also be no conductive objects, overhead power lines, or other electrical lighting or power circuits within the signal cone of the antenna (approx. 120 degrees), as these can cause interference in the already weak signals transmitted in the frequency band of the satellites.

Other Installation Criteria for Optimum Operation:

- Vertical installation of antenna (see Fig. 1)
- At least 50 cm (1.5 ft) distance to other antennas
- A clear view towards the equator
- A clear view between 55th north and 55th south parallels (satellite orbits).

Information:

Problems may arise with the synchronization of your Meinberg time server if these conditions are not met, as four satellites must be located to calculate the exact position.

9.2.2.2 Mounting the Antenna

Please read the following safety information carefully before installing the antenna and ensure that it is observed during the installation.

Danger!

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 at height without a suitable and 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 installation or the antenna cable if there is a risk of lightning strike.
- Do not perform any work on the antenna installation if it is not possible to maintain the prescribed safety distance from exposed power lines or electrical substations.

Meinberg GNS Receiver

Use the included mounting kit to mount the L1 antenna at a distance of 50 cm from other antennas on a vertical pole of a diameter of between 60 mm and 215 mm ($2\frac{1}{2}$" – $8\frac{1}{2}$").

For detailed installation instructions, please refer to the "Downloads" section on the manufacturer's product page:
https://www.pctel.com/antenna-product/gps-timing-reference-antenna-2/

The following chapter explains how the antenna cable should be laid.

9.2.2.3 Antenna Cable

Selecting the Appropriate Cable

Meinberg provides suitable cable types with its antennas and these are ordered together with the antenna to match the length you need from your antenna to your Meinberg reference clock. The route to be covered for your antenna installation should be determined and the appropriate cable type selected accordingly before confirming your order.

Important!

Please avoid using a mixture of different cable types for your antenna installation. This should be taken into consideration in particular when purchasing additional cable, for example to extend an existing cable installation.

The cable is shipped with both ends fitted with the appropriate connectors as standard, although the cable can also be shipped without any pre-fitted connectors if so requested.

GNS Clocks

The table below shows the specifications of the supported cable types for the transmission of the typical GNSS frequency bands:

Cable Type	H155	H2010 (Ultraflex)
Signal Propagation Time at 1575 MHz*	423 ns/100 m	386 ns/100 m
Attenuation at 1575 MHz	40.20 dB/100 m	17.57 dB/100 m
DC Resistance	3.24 Ω/100 m	1.24 Ω/100 m
Cable Diameter	5.4 mm	10.2 mm
Max. Cable Length	70 m	150 m

Table: Specifications of Cable Types Recommended by Meinberg

** The propagation times are specified on the basis of 100 m cable; these values can be used as a reference to calculate the propagation time of any other arbitrary length of cable.*

Laying the Antenna Cable

When laying the antenna cable, ensure that the specified maximum cable length is not exceeded. This length will depend on the selected cable type and its attenuation factor. If the specified maximum length is exceeded, correct transmission of the synchronization data and thus proper synchronization of the reference clock can no longer be guaranteed.

Caution!

When laying the antenna cable, ensure that sufficient distance is maintained from live cables (such as high-voltage power lines), as these can cause severe interference and compromise the quality of the antenna signal significantly. Surges in power lines (caused, for example, by lightning strike) can generate induced voltages in a nearby antenna cable and damage your system.

Further Points to Consider when Laying Antenna Cable:

- The minimum bend radius of the cable must be observed.[1]
- Any kinking, crushing, or other damage to the external insulation must be avoided.
- Any damage or contamination of the coaxial connectors must be avoided.

[1] *The bend radius is the radius at which a cable can be bent without sustaining damage (including kinks).*

The next chapter "Surge Protection and Grounding" explains how to implement effective surge protection for an antenna installation.

Compensating for Signal Propagation Time

GNS Clocks

The propagation of the signal from the antenna to the receiver (reference clock) can incur a certain delay. This delay can be compensated for in the LANTIME Web Interface.

To do this, log into the Web Interface of your LANTIME system and proceed as follows:

1. Open the menu "**Clock**" → "**State & Configuration**".
2. Select the corresponding clock module.
3. Click on the "Miscellaneous" tab.
4. Select the compensation method and enter the appropriate value.

A fixed signal propagation offset can be entered in nanoseconds by selecting "**By Delay**". This value is calculated either based on the cable specifications provided in the data sheet of your cable or based on your own delay measurements.

A manually calculated signal propagation offset will provide the best accuracy. However, the length of the cable can also be entered in meters by selecting "**By Length**" to provide an automatically estimated offset based on the known specifications of standard Belden H155 cable.

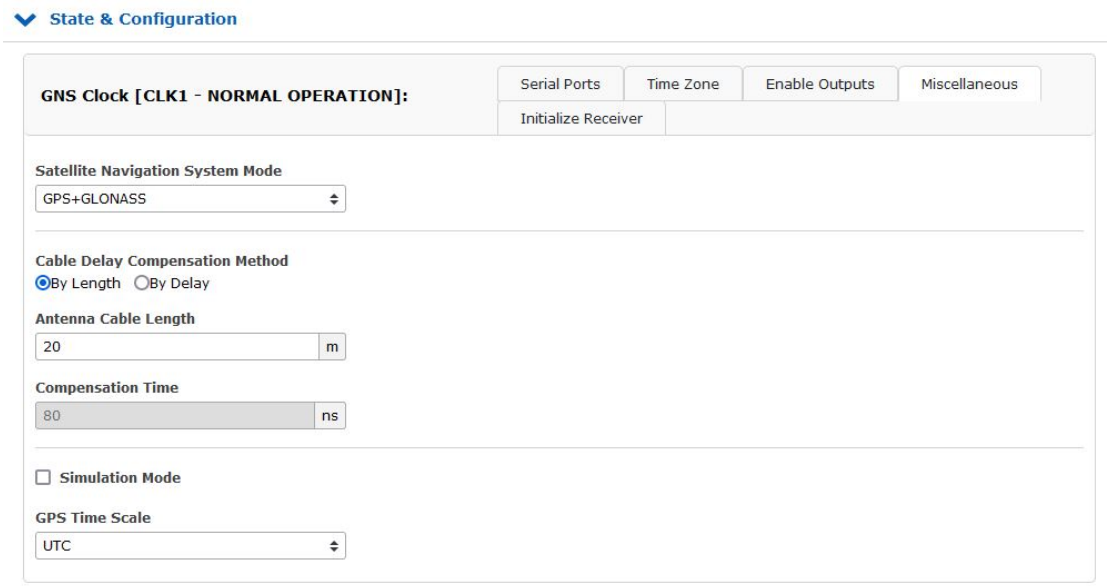


Fig. 4.1: "Clock" menu in the LANTIME OS web interface

9.2.3 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).

9.3 Long Wave Signal Reception

9.3.1 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.

9.3.2 Installation of a Longwave Antenna

9.3.2.1 Geographical Considerations

The antenna location plays a critical role in determining the quality of reception and thus the signal strength of the signal, and should therefore be selected carefully so as to avoid difficulties with synchronization. If the antenna is not precisely aligned, signal reception and timing accuracy will be affected.

AWO2 - DCF77

The antenna must be directed towards Mainflingen, Germany, near Frankfurt am Main, in accordance with the installation conditions specified below.

The DCF77 signal has a theoretical range of 2000 km (measured fromm the transmission tower) and enables DCF77 receiver-clocks in not only Germany but also countries such as France, Denmark, Sweden, Austria, and Italy to be synchronized. Depending on the time of day, sensitive receivers can receive a sufficiently strong signal even in the furthermost regions of the reception area.

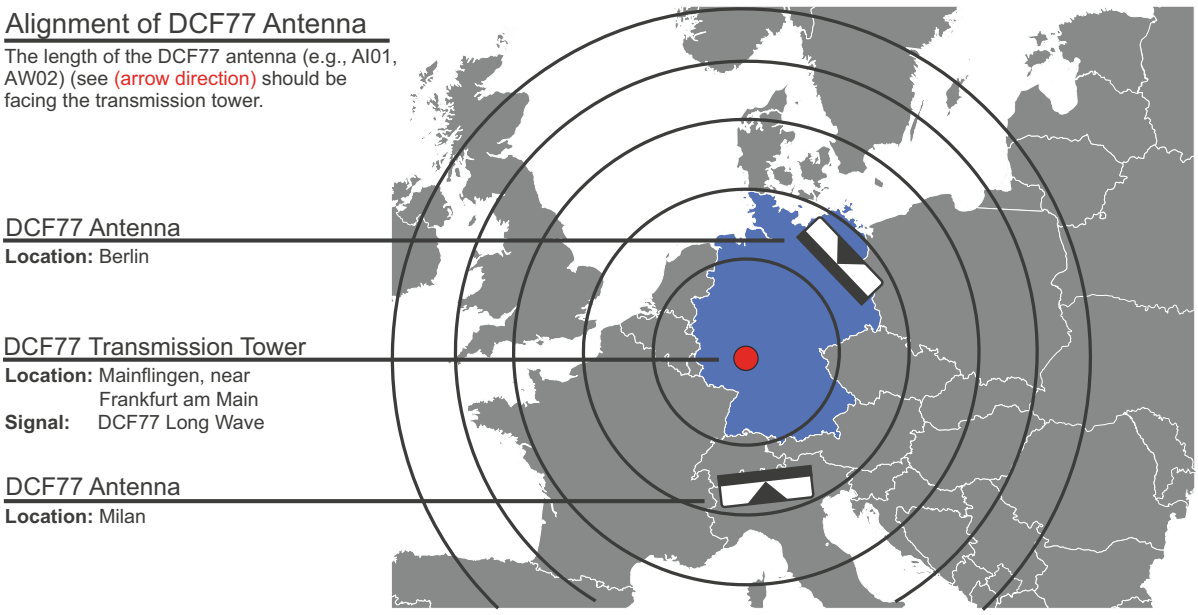


Illustration: Installation of a Meinberg long-wave antenna directed towards the DCF77 transmitter tower in Mainflingen, near Frankfurt-am-Main in Germany.

AWO2-60 - MSF and WWVB

Depending on the country of use, the AW02-60 antenna must be directed towards Anthorn, in Cumbria, or towards Fort Collins, Colorado, in accordance with the installation conditions specified below.

Reception of the MSF signal covers a theoretical range of 1000 km and is thus comprehensive and guaranteed in the UK and Ireland. The MSF signal is receivable in parts of northern and western Europe but this cannot be guaranteed.

Reception of the WWVB signal in the USA is limited to a theoretical range of 1500 km from the transmission tower in Colorado. As such, cities such as San Diego, Chicago, and Sacramento represent the extremes of the reception range, at which reception may become intermittent, especially in built-up areas such as urban centers.

The maps on the next page provide an overview of reception coverage in the UK and USA.

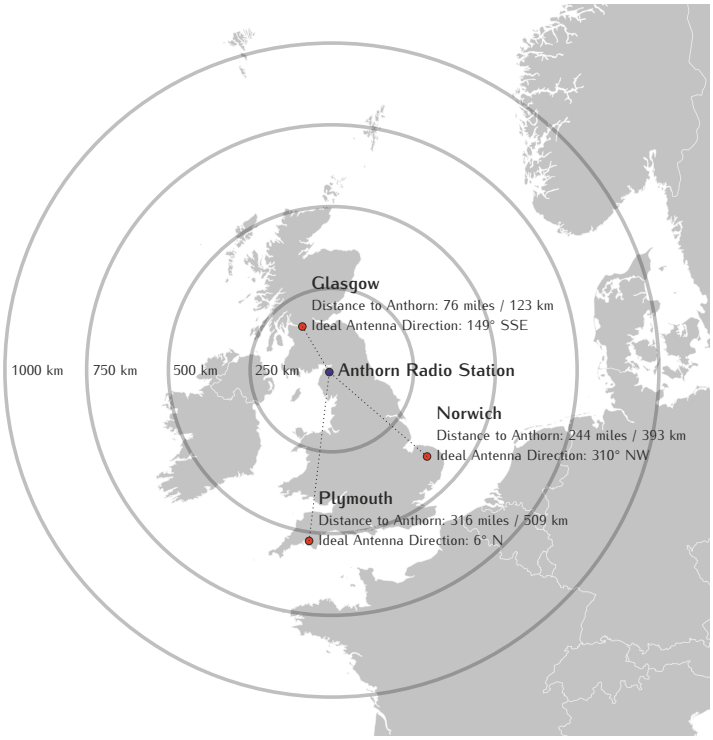


Illustration: Installation of how an AW02-60 antenna is directed towards the MSF transmitter tower in Anthorn, Cumbria, UK from various locations in the UK.

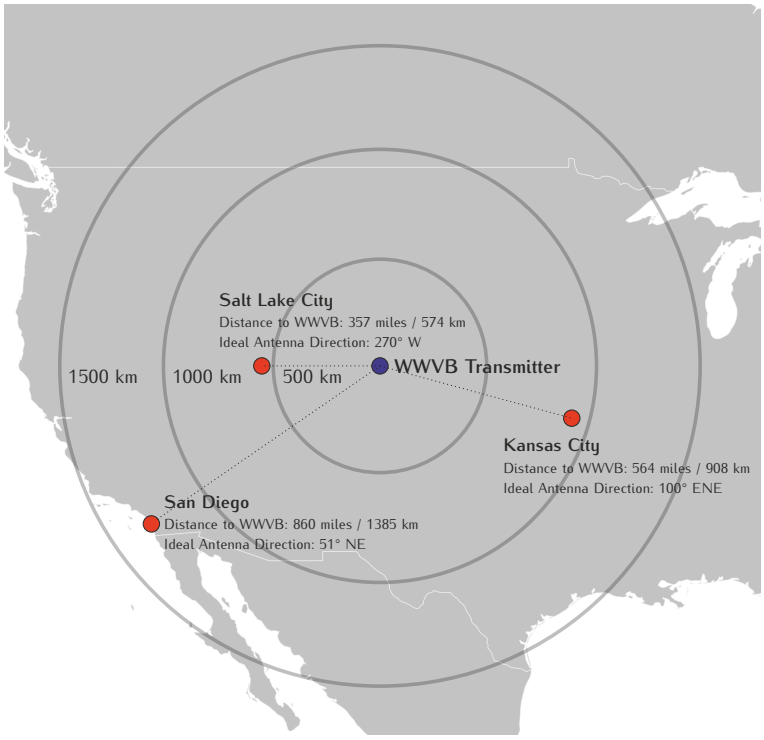


Illustration: Installation of how an AW02-60 antenna is directed towards the WWVB transmitter tower near Fort Collins, Colorado, USA from various locations in the USA.

9.3.2.2 Selecting the Antenna Location

There are two ways of mounting the antenna using the mounting kit included in the packaging.

1.Mounting on a pole

2.Mounting on a wall

To ensure that the long wave signal can be reliably received and avoid difficulties with synchronization of your Meinberg product, select a location that allows for an unobstructed view towards Mainflingen, Germany (near Frankfurt am Main).

When using an AWO2-60 antenna to receive MSF or WWVB time signals, select a location that allows for an unobstructed view towards Anthorn (UK) or Fort Collins (USA).

The line of sight between the antenna and signal source must therefore not be obstructed in any way. The antenna must also not be installed under power lines or other electrical lighting or power circuits.

Other Installation Criteria for Optimum Operation:

- The antenna should be mounted horizontally (see illustration).
- It should be at a distance of at least 30 cm (1 ft) from other antennas.
- The length of the antenna must be facing the transmission tower (see illustration).

Information:

Problems may arise with the synchronization of your Meinberg system if these conditions are not met.

9.3.2.3 Installation of the Meinberg AW02 Antenna

Please read the following safety instructions carefully before installation and be sure to observe them.

Danger!

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 at height without a suitable and effective fall arrester!

Danger!

Do not work on the antenna installation during thunderstorms!

Danger of death from electric shock!

- **Do not** carry out any work on the antenna installation or the antenna cable if there is a risk of lightning strike.
- **Do not** perform any work on the antenna installation if it is not possible to maintain the prescribed safety distance from exposed power lines or electrical substations.

9.3.2.4 Antenna Cable

Selecting the Appropriate Cable

Meinberg provides suitable cable types with its antennas and these are ordered together with the antenna to match the length you need from your antenna to your Meinberg reference clock. The route to be covered for your antenna installation should be determined and the appropriate cable type selected accordingly before confirming your order.

The cable is shipped with both ends fitted with the appropriate connectors as standard, although the cable can also be shipped without any pre-fitted connectors if so requested.

Important!

Please avoid using mixed types of coaxial cable in your antenna installation (for example, RG58 and RG174 together in a single installation). This should also be noted when purchasing cable, for example to expand an existing installation.

The table below shows the specifications of the supported cable types for the transmission of the 77 kHz long-wave frequency:

Cable Type	RG58C/U	RG174U
Signal Propagation Time at 77.5 kHz	528 ns/100 m	558 ns/100 m
Attenuation at 77.5 kHz	0.57 dB/100 m	3.35 dB/100 m
DC Resistance	5.3 Ω/100 m	33.8 Ω/100 m
Cable Diameter	5 mm	2.8 mm
Max. Cable Length	300 m	300 m

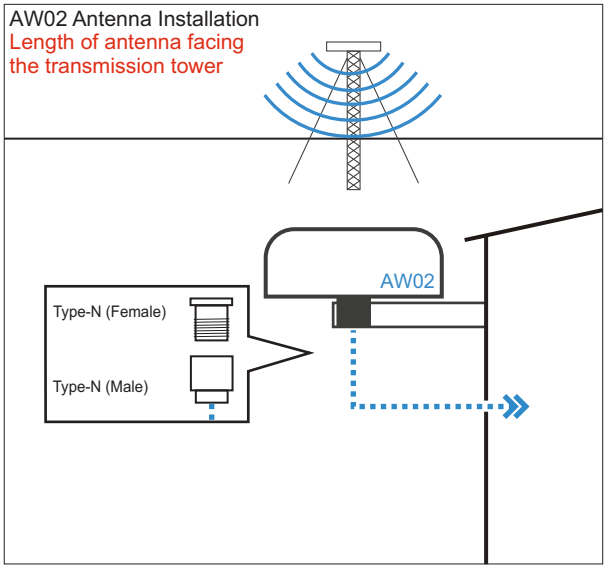
Table 1: Specifications of Cable Types Recommended by Meinberg

** The propagation times are specified on the basis of 100 m cable; these values can be used as a reference to calculate the propagation time of any other arbitrary length of cable.*

Laying the Antenna Cable

When laying the antenna cable, ensure that the specified maximum cable length is not exceeded. This length will depend on the selected cable type and its attenuation factor. If the specified maximum length is exceeded, correct transmission of the synchronization data and thus proper synchronization of the reference clock can no longer be guaranteed.

The antenna cable should then be connected to the Type-N connector of the antenna. Feed the other end of the cable into the building through the wall.



Caution!

When laying the antenna cable, ensure that sufficient distance is maintained from live cables (such as high-voltage power lines), as these can cause severe interference and compromise the quality of the antenna signal significantly. Surges in power lines (caused, for example, by lightning strike) can generate induced voltages in a nearby antenna cable and damage your system.

Further Points to Consider when Laying Antenna Cable:

- The minimum bend radius of the cable must be observed.[1]
- Any kinking, crushing, or other damage to the external insulation must be avoided.
- Any damage or contamination of the coaxial connectors must be avoided.

[1] *The bend radius is the radius at which a cable can be bent without sustaining damage (including kinks).*

The next chapter "Surge Protection and Grounding" explains how to implement effective surge protection for an antenna installation.

Compensating for Signal Propagation Time

The propagation of the long-wave signal from the transmission tower to the receiver (reference clock) can incur a certain delay. This delay can be compensated for by registering the distance in kilometers (point to point, straight line) between the location of the antenna and the DCF77 transmission tower in Mainflingen, Germany.

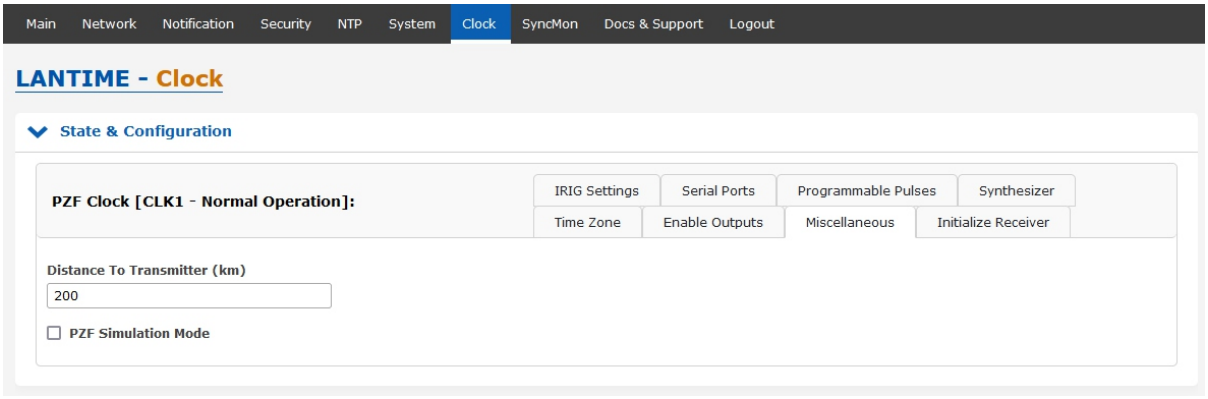


Fig. 4.1: "Clock" menu in LANTIME OS Web Interface

9.3.2.5 Procedure for Antenna Alignment

The antenna itself provides no visual indication of the reception quality of the DCF77 signal while aligning it.

Step 1: A field strength meter can be used to determine the ideal direction of the installed DCF77 antenna. First, the length of the antenna (using the arrow printed on the antenna) is pointed in the general direction of Frankfurt am Main, in Germany. Finer adjustments are then made to the direction of the antenna until the field strength is in the optimum range of –60 dB to –70 dB.

If no field strength meter is available, Meinberg recommends that two people perform the process of turning the antenna and verifying the reception quality. Person 1 (at the antenna) should remain in communication with Person 2 (at the receiver) to this end.

Step 2: Person 1 rotates the antenna slowly in an **anticlockwise** direction until Person 2 sees that the "Mod" LED is flashing rhythmically once a second without intermittent flickering.

If the LED does not flash in this way, the antenna should be turned slowly in a **clockwise** direction from the approximate direction until Person 2 sees that the "Modulation" LED is flashing rhythmically once a second without intermittent flickering.

Please note that a high signal level alone is no guarantee of good reception, as it can also be caused by electrical noise in the associated frequency range.

With good reception, the connected DCF reference clock should synchronize within three minutes after initialization.

Successful synchronization is signaled by the "Sync After Reset" LED turning green. Reception problems are signaled by the "Free Run" LED turning red again at the start of the next minute. If the clock is running off the oscillator alone for more than 12 hours, the "Sync" LED will begin to flash.

9.3.3 Powering up a 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 "rough" 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.

9.4 Surge Protection and Grounding

The greatest risk to an antenna installation and the electronic devices connected to it is exposure to lightning strikes. An indirect lightning strike in the vicinity of the antenna or coaxial cable can induce significant surge voltages in the coaxial cable.

Without inline protection, such induced surge voltages can be passed to the antenna and to other indoor devices patched into the coaxial line (specifically, your Meinberg System), potentially causing significant damage to or even destroying not only your antenna but also any connected receivers and signal distributors. Such surge voltage scenarios also present a risk of fire and injury.

This is why antennas and antenna cables must always be integrated into a building's equipotential bonding infrastructure as part of an effective lightning protection strategy to ensure that voltages induced by lightning strikes directly on or indirectly near the antenna are redirected safely to ground.

Warning!

Surge protection and lightning protection systems may only be installed by persons with suitable electrical installation expertise.

Meinberg GPSANTv2

Meinberg's new-generation "GPSANTv2" antenna features integrated surge protection in accordance with IEC 61000-4-5 Level 4 to reliably shield the antenna against surge voltages. The antenna also has a grounding terminal to allow it to be connected as directly as possible to a bonding conductor using a grounding cable. Please refer to the standards regarding antenna installations (e.g., DIN EN 60728-11) for more information.

However, in order to preserve the safety of the building and to protect your Meinberg system, Meinberg recommends the use of the MBG-S-PRO surge protector, which is addressed in more detail later in this chapter.

Surge Protection

VDE 0185-305 (IEC 62305) (relating to buildings with lightning protection systems) and VDE 0855-1 (IEC 60728-11) (addressing bonding strategies and the grounding of antenna installations in buildings with no external lightning protection system) are the lightning protection standards applicable to antenna installations on a building. Antennas must generally be integrated into a building's lightning protection system or bonding infrastructure.

If the antenna represents the highest point of a building or pole, the lightning protection strategy should incorporate a safe zone (e.g., formed by a lightning rod) positioned above the antenna. This increases the likelihood of lightning being 'caught' by the lightning rod, allowing surge currents to be safely passed from the lightning rod along a grounding conductor to ground.

Electrical Bonding

Electrical bonding is the connection of all metallic, electrically conductive elements of the antenna installation in order to limit the risk of dangerous voltages for people and connected devices.

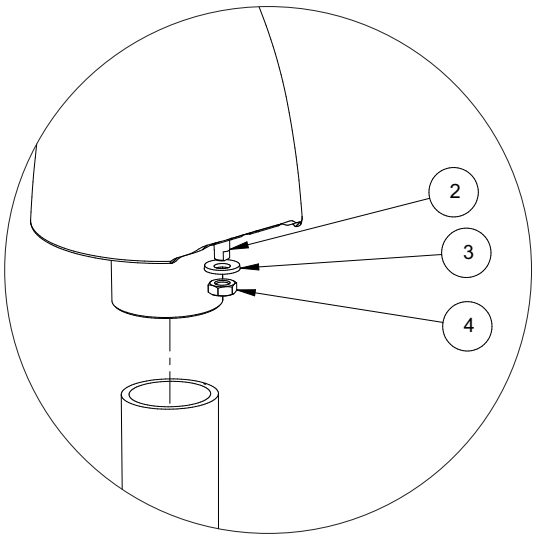
To this end, the following elements should be connected and integrated into a bonding system:

- the antenna cable shielding using cable shield bonding connectors*
- the core conductor of the antenna cable using surge protection devices
- antennas, antenna poles
- ground electrodes (e.g., foundation electrode)

* Minimum IP rating IP X4 when using bonding connectors outdoors.

Connecting the Grounding Terminal of the Antenna

As mentioned previously, the antenna must be connected to a grounding busbar using a grounding cable (not included). A grounding cable must be assembled for this purpose; the recommended conductor thickness is 4 mm^2 – 6 mm^2 and a ring terminal fitting the M8 (0.315 inch) grounding bolt must be used.



Grounding Cable Installation Procedure:

1. Remove the nut (Pos. 4) and the safety washer (Pos. 3).
2. Place the ring terminal onto the grounding bolt (Pos. 2).
3. First place the safety washer (Pos. 3) onto the grounding bolt (Pos. 2), then screw the M8 nut (Pos. 4) onto the thread of the grounding bolt.
4. Tighten the nut (Pos. 4) with a max. torque of 6 Nm.

Once the antenna has been correctly installed with the grounding cable, connect the grounding cable to the bonding bar (see Fig. 5 and 6).

The following drawings illustrate how a Meinberg GPS Antenna can be installed in accordance with the above conditions on a pole (e.g., antenna pole) or building roof.

Antenna Installation without Insulated Lightning Rod System

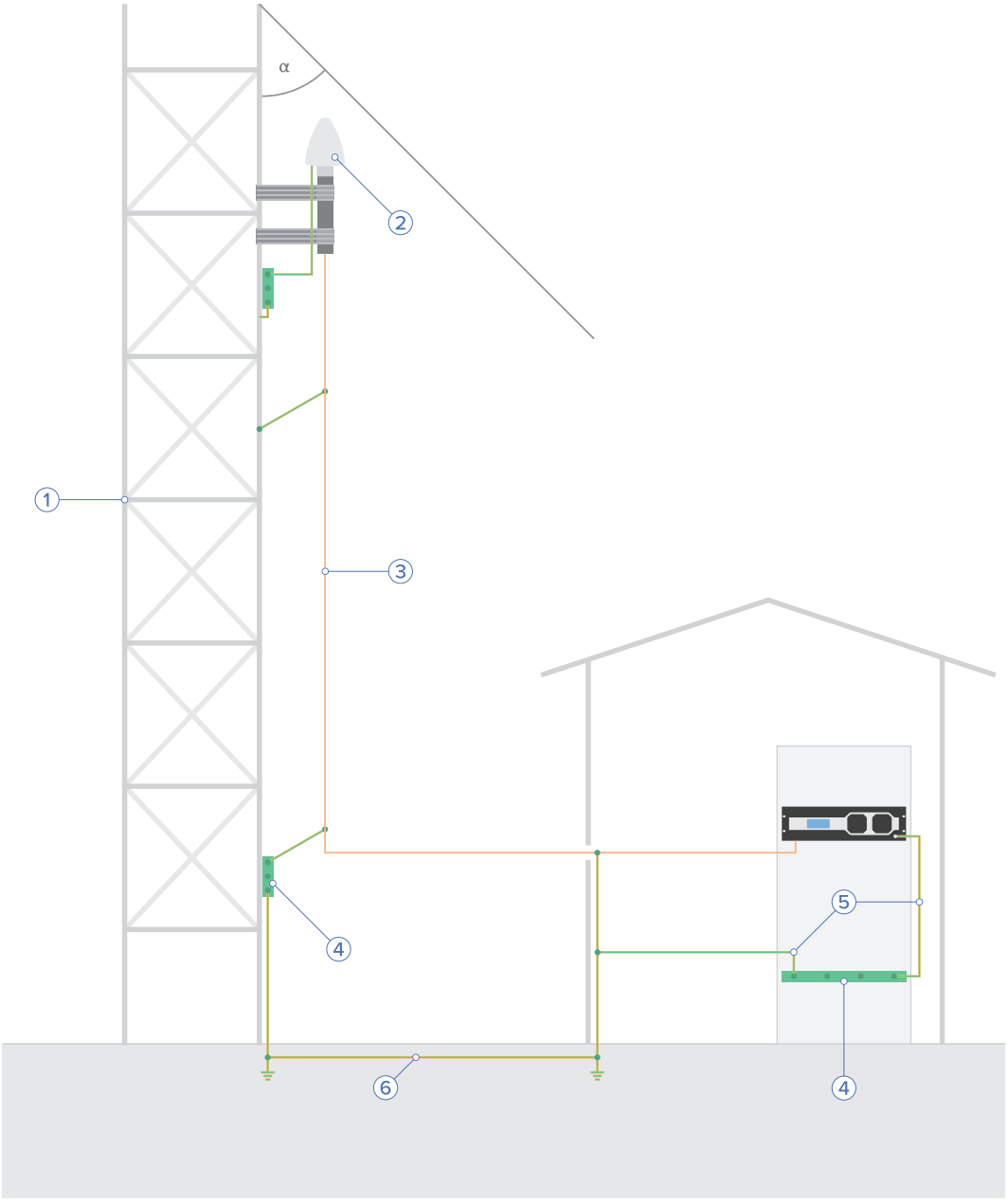


Fig. 5: Installation on a Pole

1 Antenna Pole
2 Meinberg GPS Antenna
3 Antenna Cable
4 Bonding Bar
5 Bonding Conductor
6 Foundation Electrode
α Safety Zone

Antenna Installation with Insulated Lightning Rod System

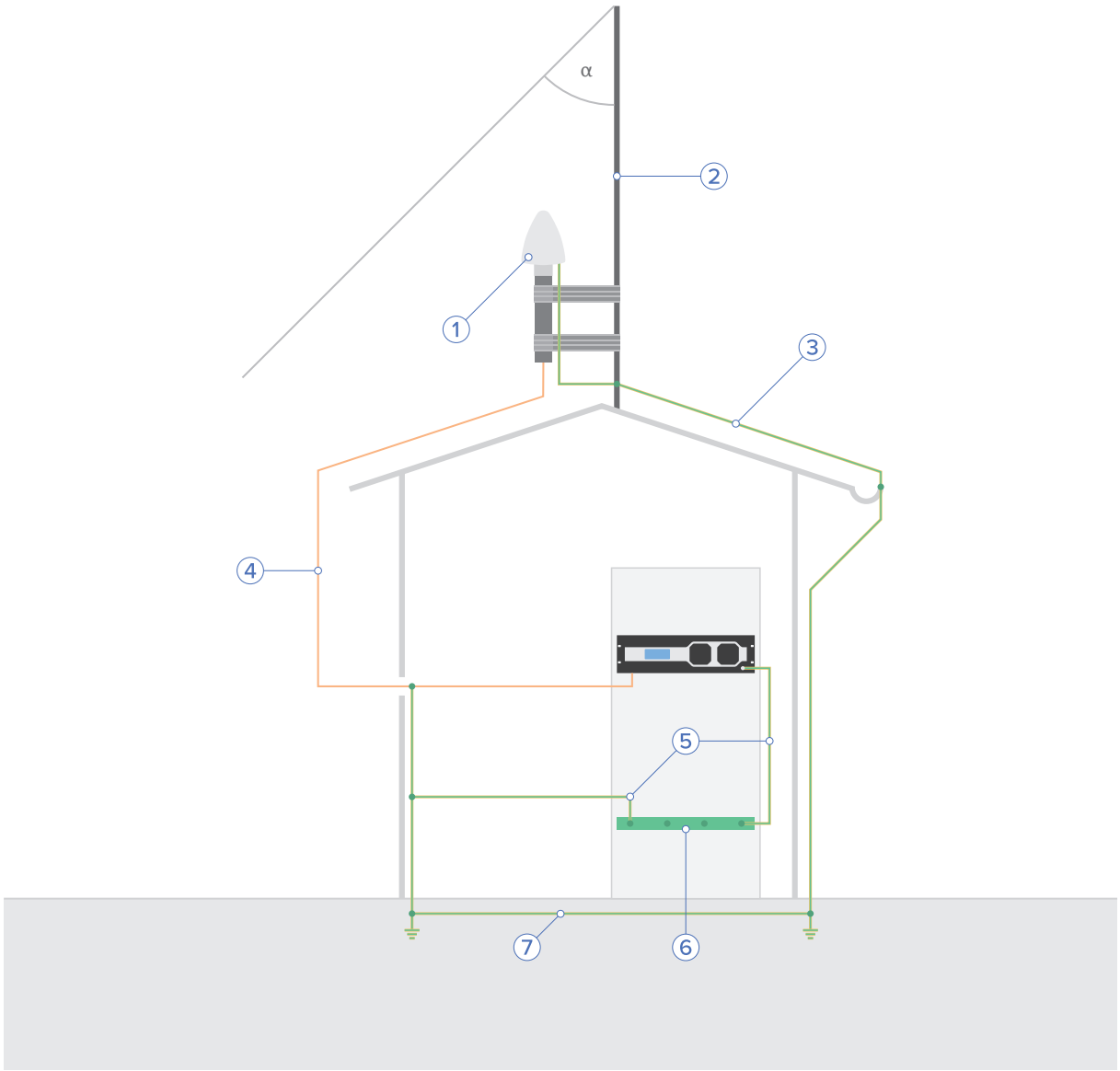


Fig. 6: Roof Installation

1 Meinberg GPS Antenna
2 Lightning Rod
3 Lightning Rod Conductor
4 Antenna Cable
5 Bonding Conductor
6 Bonding Bar
7 Foundation Electrode
α Safety Zone

Optional MBG S-PRO Surge Protector

Information:

The surge protector and suitable coaxial cable are not included as standard with a Meinberg GPS Antenna, but can be ordered as an optional accessory.

Construction

The MBG-S-PRO is a surge protector (Phoenix CN-UB-280DC-BB) for coaxial connections. It is patched directly into the antenna line and consists of a replaceable gas discharge tube that redirects the energy from the cable shielding to the ground potential when ignited.

Installation Conditions

To protect the building from possible surge voltages, the MBG-S-PRO is installed at the point of entry of the antenna cable into the building. The MBG-S-PRO must be shielded against water spray and water jets, either by means of a suitable enclosure (IP65) or a protected location.

Ideal Installation Conditions:

- Installation at the point where the antenna cable passes through the building wall
- Ground conductor cable from surge protector to grounding busbar as short as possible

Installation and Connection

This surge protector has no dedicated input or output polarity and therefore has no preferred installation orientation. It features Type-N female connectors at both ends.

Installation

1.
Fit the surge protector to the supplied mounting bracket as shown in the illustration.

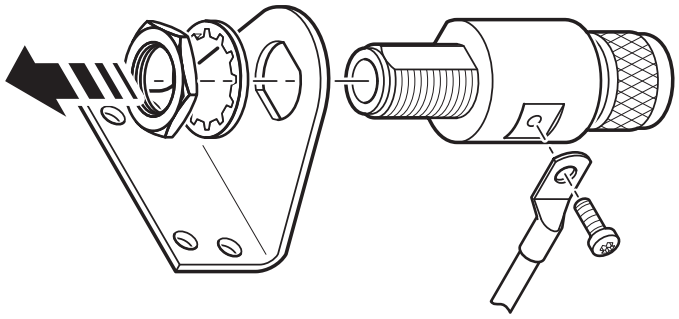


Fig. 7: Installation of the Surge Protector

2.
Connect the MBG-S-PRO to a grounding busbar using a ground conductor cable that is as short as possible. It is also important for the ground terminal of the surge protector to be connected to the same bonding bar as the connected Meinberg system in order to prevent destructive potential differences.

3.
Connect the coaxial cable from the antenna to one of the surge protector connectors, then connect the other surge protector connector to the coaxial cable leading to the Meinberg reference clock.

Caution!

For safety reasons, the antenna cable must not exceed a certain length if there are no other devices such as a power distributor between the surge protector and the downstream electronic device with integrated surge protection at the mains connector level.

Please refer to the document "Technical Specifications: MBG-S-PRO Surge Protector" in the appendix as well as the manufacturer's data sheet for detailed installation instructions and technical specifications for the surge protector.

Data Sheet (Download):

https://www.meinbergglobal.com/download/docs/shortinfo/english/cn-ub-280dc-bb_pc.pdf

10 LTOS7 Management and Monitoring

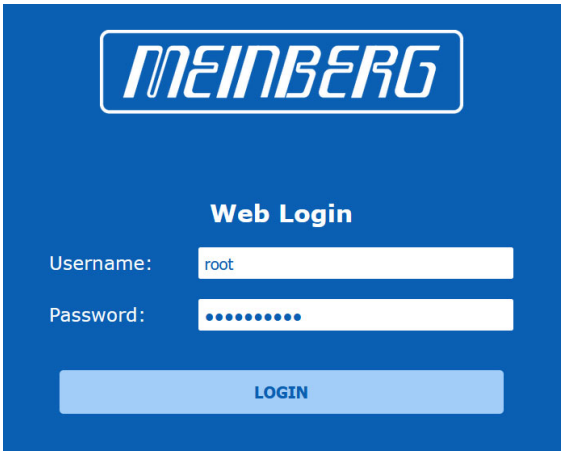
10.1 Via Web GUI

10.1.1 Session Handling

Session Handling of the WebUI as of LTOS v7.08
The Web Interface's session handling supports form-based authentication as of LTOS v7.08.002. This replaces the previous "basic auth" type authentication method used for the web-based UI in earlier versions of LTOS. The session key is now stored in a cookie, which is transmitted to prove that the user is authorized to access the Web Interface upon successful login. Most browsers support this authentication method automatically, provided that cookies are enabled; users should not notice any other fundamental changes to the Web Interface user experience.

The illustration on the right shows the login page of the LANTIME system. Once you have opened the Web Interface by entering the IP address of the LANTIME in the address bar of your browser, you can log in here. In the system's factory-default state, the following credentials are used to log in:

User: **root**
Password: **timeserver**

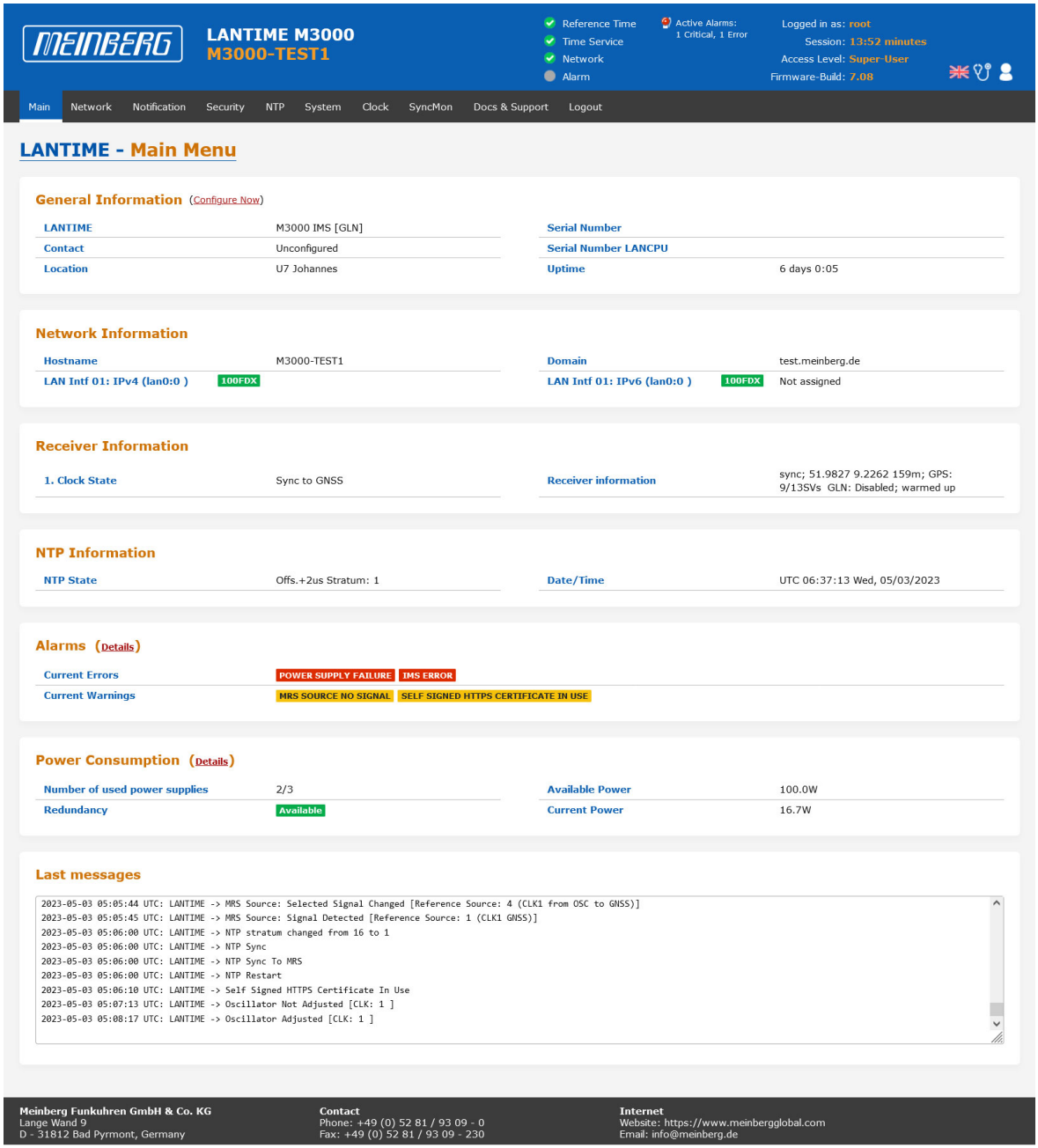


Important Note:
You should immediately change the account details for the "root" user in the Web Interface menu "System → User Administration". You can then create as many users as needed with a variety of permissions (see → Chapter 10.1.9.4, "User Management").

Important!

In the system's factory-default state, the setting for "Bruteforce Detection" is set to three attempts. If the wrong account details are entered three times when logging in under certain circumstances, the user must wait three minutes before another login attempt is possible. The settings for bruteforce detection and the lockout time are described in the chapter "Security".

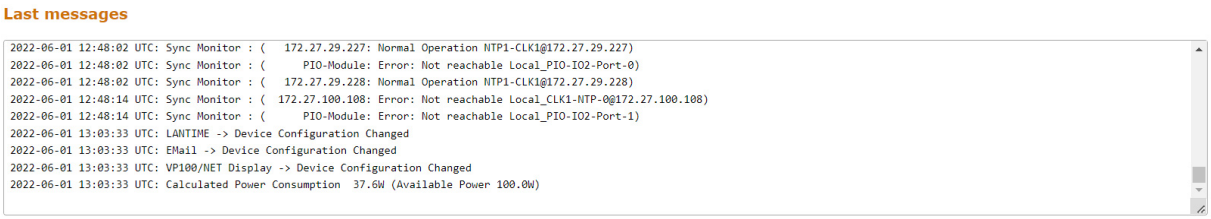
10.1.2 Main Menu



This chapter provides you with configuration options and status information of your LANTIME system accesssed via Web GUI. The main page contatins 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 ...)
- Advanced statistics with Sync Monitor
- 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 bottom 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.

10.1.2.1 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. Per default configuration https protocol is enabled at each network interface. Http requests are automatically redirected to https.

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.

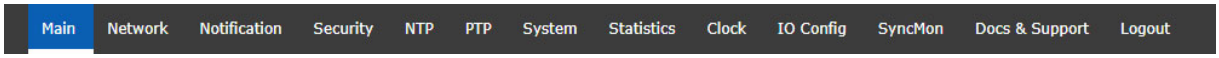
After entering the correct password, the main menu page of the web interface of a LANTIME system shows up.

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".

10.1.2.2 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.



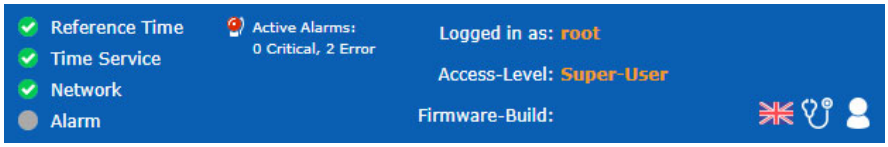
Scrolling down the main page you will find a section containing last log messages generated during the LANTIME operation. The messages in this field are limited to the last 50 and are chronologically ordered. The messages are stored in the file /var/log/lantime_messages, which is created after every 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 Command Line Reference.

10.1.2.3 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 SyncMon) 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 "SyncMon" 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).

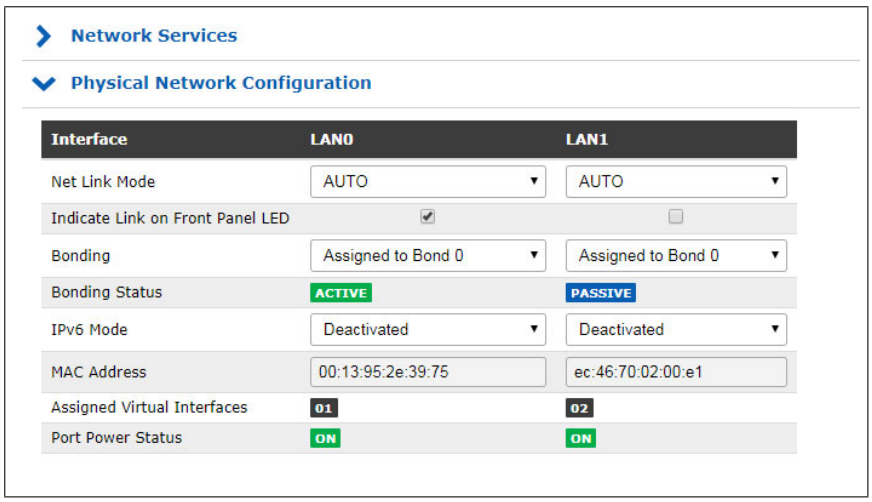


Figure: A tree structure of each menu. Opening a subtree by clicking a "+" and closing by "-" at the beginning of the submenu name

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".

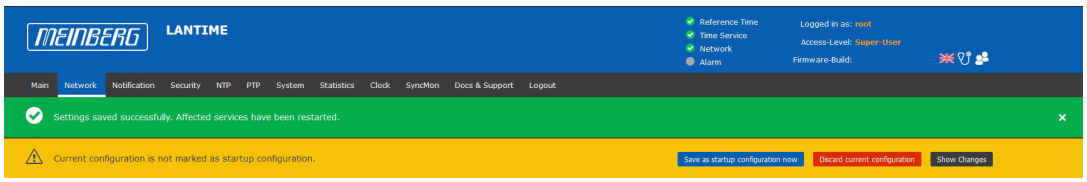


Figure: Settings saved successfully. Affected services have been restarted

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.

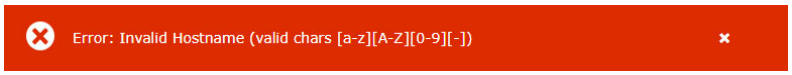
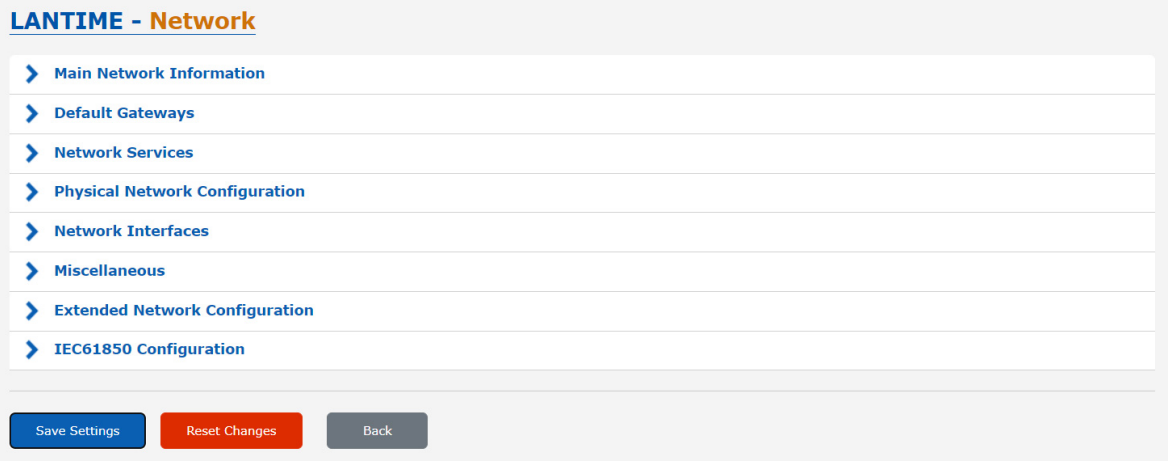


Figure: A display of a warning message with a type of error and indication to which feature it belongs

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.

10.1.3 Network



10.1.3.1 Main Network Information

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
An alternate nameserver can be defined here.

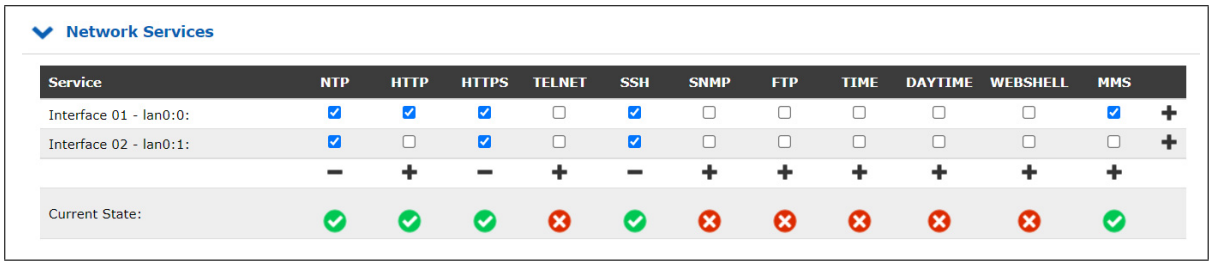
10.1.3.2 Default Gateways

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.

10.1.3.3 Network Services



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

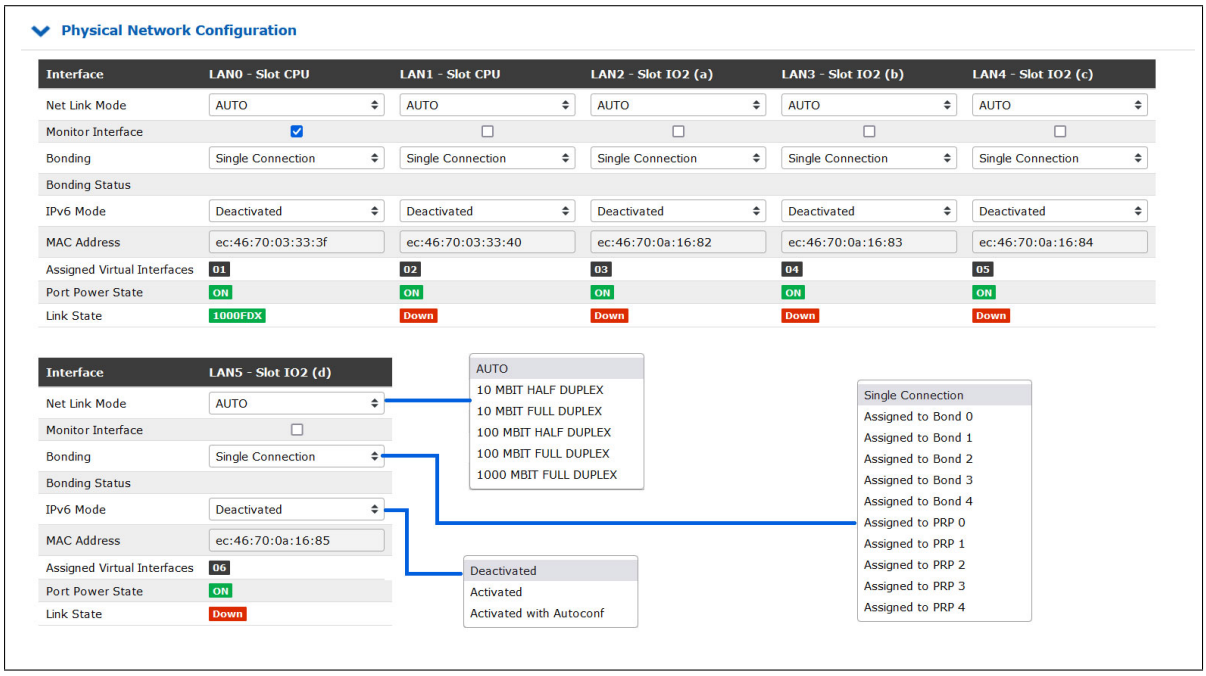
DAYTIME: UDP Port 13

WEBSHELL: Login to a command line interface of a Lantime via a webbrowser. WEBSHELL works on port 4200. Input in the web browser: [IP/HOSTNAME]: 4200

MMS: The Manufacturing Message Specification (MMS) standardises the exchange of messages in the production area.

Note: In order to perform an IEC61850 configuration, this service must be must be activated (see chapter IEC 61850 Configuration).

10.1.3.4 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.

Monitor Interface

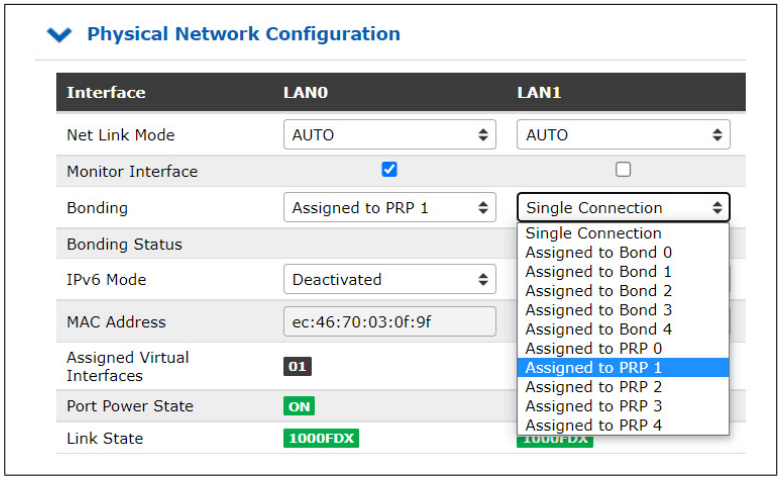
As soon as one of the selected network ports has no link, this status will be indicated by a red "Network" LED on the front panel and the "Network Link Down" event will be reported. If a network link is available on all selected ports, the "Network" LED on the front panel will light up green.

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.

PRP

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).



As of LANTIME firmware version 7.0, PRP can also be conveniently set via the web interface menu "Network → Physical Network Configuration". Select the same PRP group for at least two interfaces in the drop-down menu "Bonding".

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.

Information:

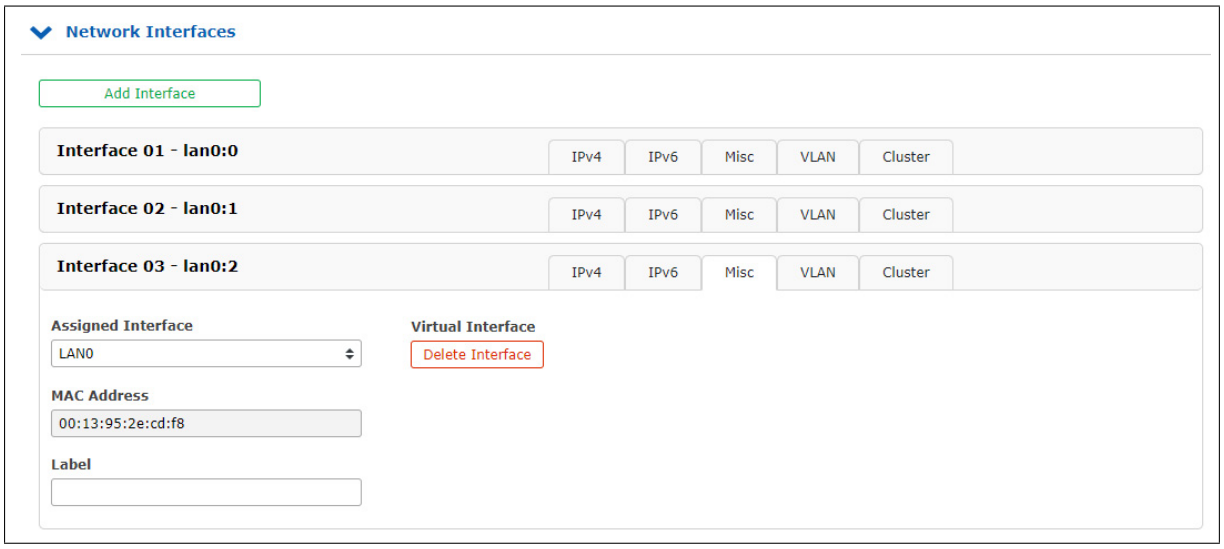
The status of the power supply (Port Power Status) can only change to "off" for network interfaces that are located on an LNE-SFP network card. If, for example, the maximum available power is no longer sufficient when retrofitting an IMS module, an existing LNE-SFP module is switched off.

Before using an additional IMS module, please always check the maximum available power of the existing power supply units in the web interface menu "System → Power consumption".

Link Status

The Link Status indicates the speed detected by the respective network interface.

10.1.3.5 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).

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.

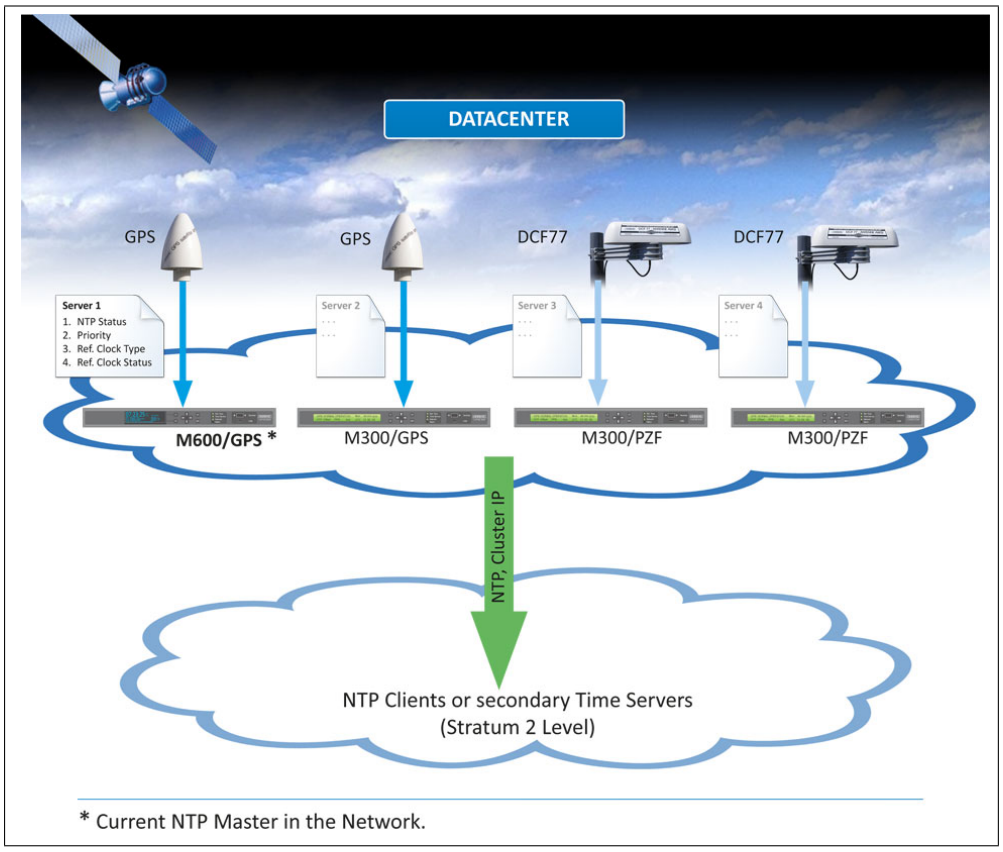
Submenu Cluster:

The Cluster mode is a method for providing redundant time synchronization by groupping (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).



10.1.3.6 IPv4 Cluster Configuration

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

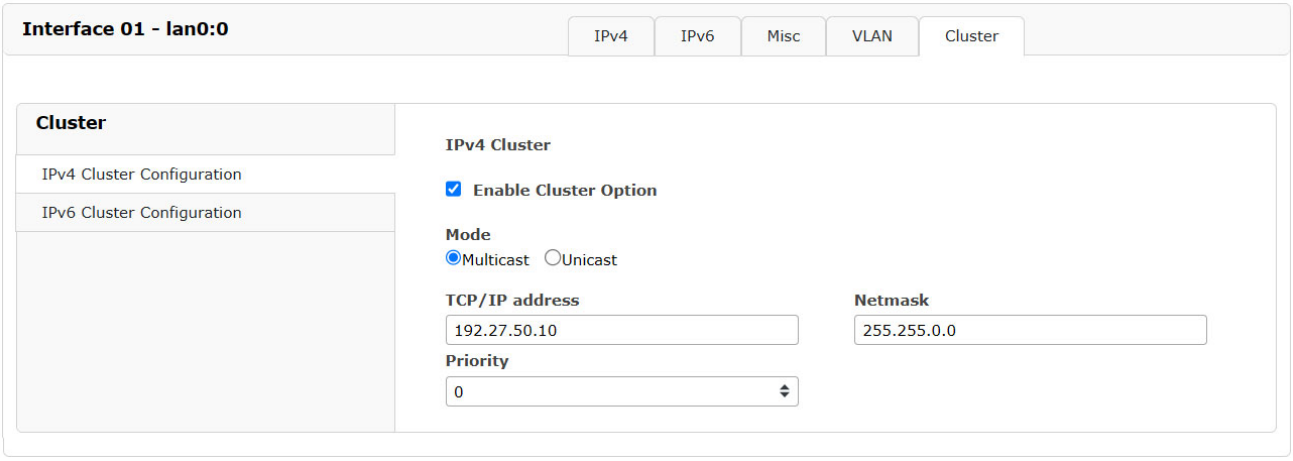
Mode: The cluster members can share their status information either via multicast or unicast messages. For multicast, a cluster multicast address 239.192.0.1 is used by default. This setting can be changed in the menu "Network → Miscellaneous". In addition, the network port which is used for the cluster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

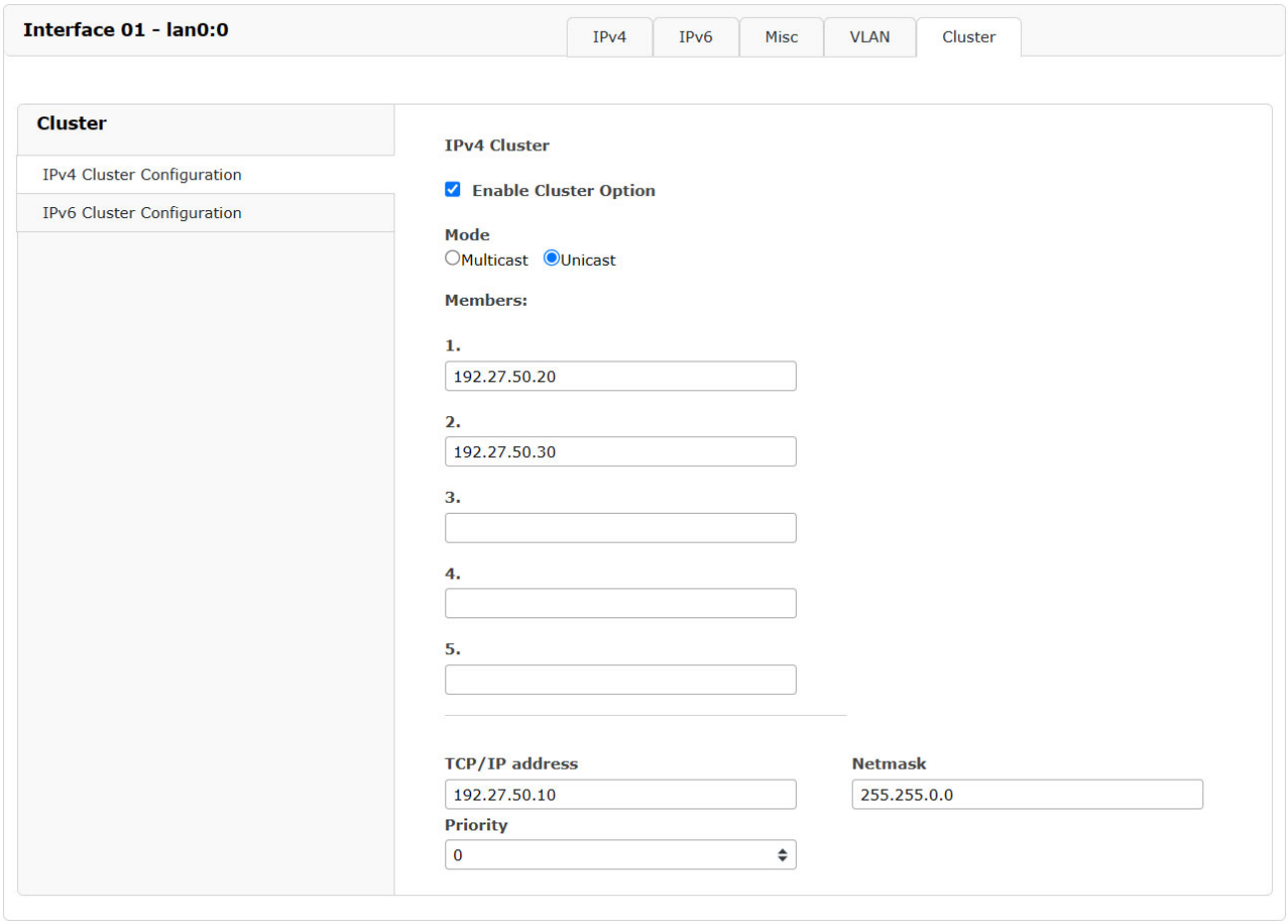
Netmask: Netmask Configuration for the IPv4 cluster interface.

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 an IPv4 multicast cluster:



Example configuration for an IPv4 unicast cluster:



In the Unicast cluster, the IP addresses of the cluster members must be entered in the "Members" fields.

10.1.3.7 IPv6 Cluster Configuration

Information:

The IPv6 cluster configuration is available as from LTOS firmware 7.08.007.

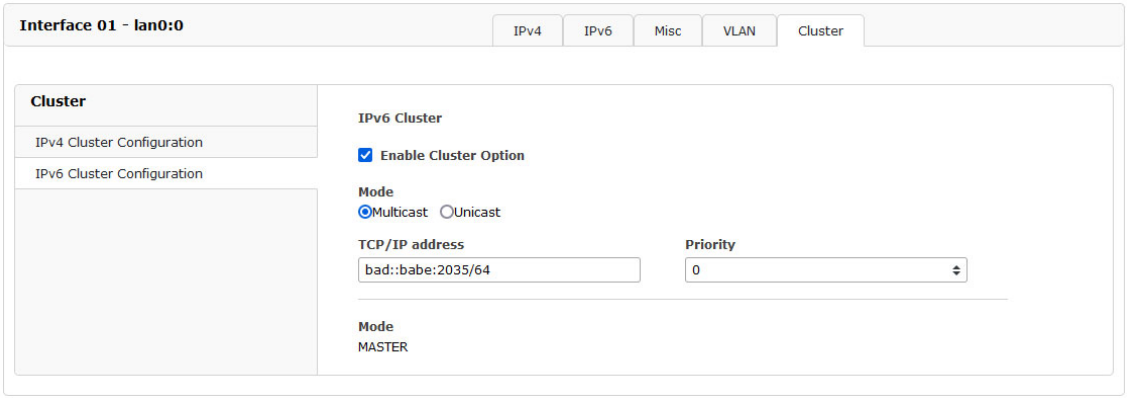
Enable Cluster Option: The cluster function can be activated via this selection box.

Mode: The cluster members can share their status information either via multicast or unicast messages. For multicast, a cluster multicast address FF08::c123:feed: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 7001 is used for the cluster messages.

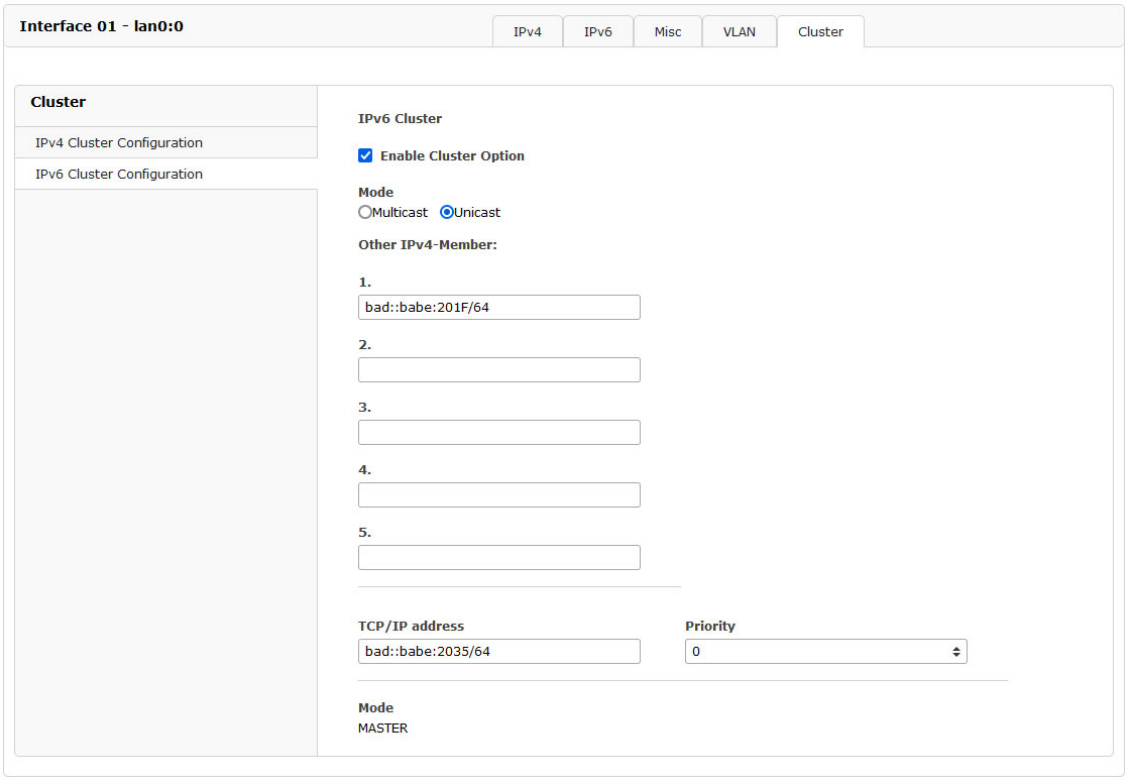
TCP/IP Address: IP address of the NTP cluster interface. The same cluster IP needs to be configured on all cluster members. It is recommended to configure a cluster IP in the same subnet as the corresponding virtual interface.

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 an IPv6 multicast cluster:

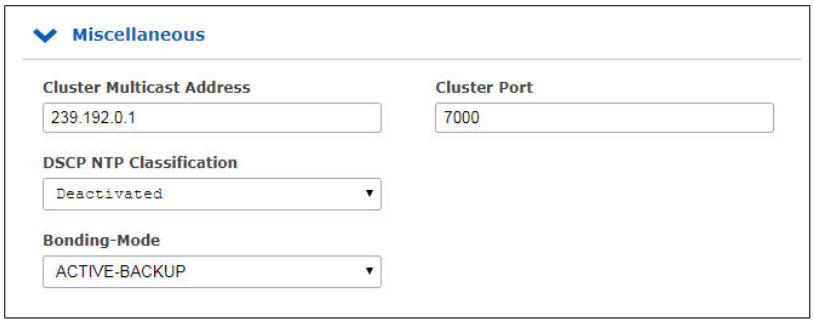


Example configuration for an IPv6 unicast cluster:



In the Unicast cluster, the IPv6 addresses of the cluster members must be entered in the "Other IPv6 Member" field.

10.1.3.8 Miscellaneous



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

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

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 DSCP is 6 bits in length, enabling 2*6 = 64 different values (0 to 63). These are the default DSCP values. 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.

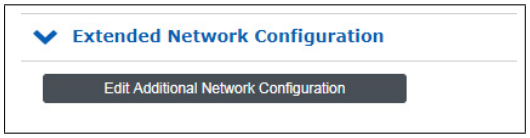
Bonding-Mode:
In the menu “Network → Physical Network Configuration", two or more physical network ports can be grouped into a bond (group). The Bonding Mode is used to configure either the “ACTIVE BACKUP” or the "LACP" mode (Link Aggregation Control Protocol), which are supported on the LANTIME.

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.

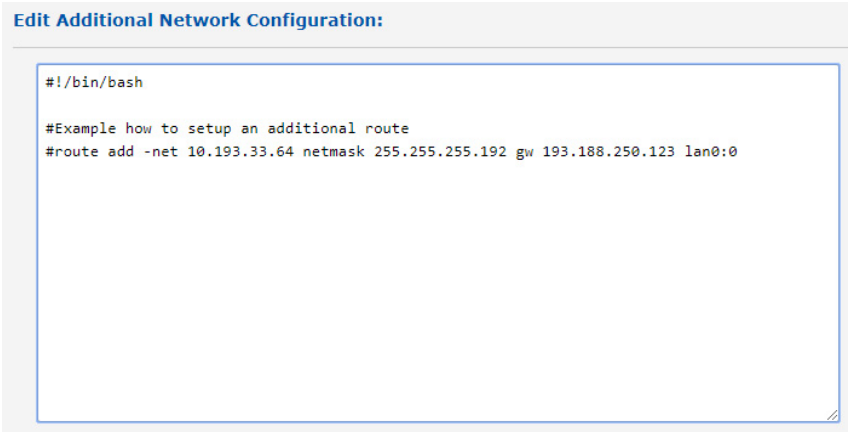
LACP: LACP (802.3ad) allows a combination of multiple physical connections to a logical one. This results in a load sharing and, in addition, increases the safety in case of a failure compared to "Active Backup". It is important that other connected network devices also support LACP and the network ports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

10.1.3.9 Extended Network Configuration

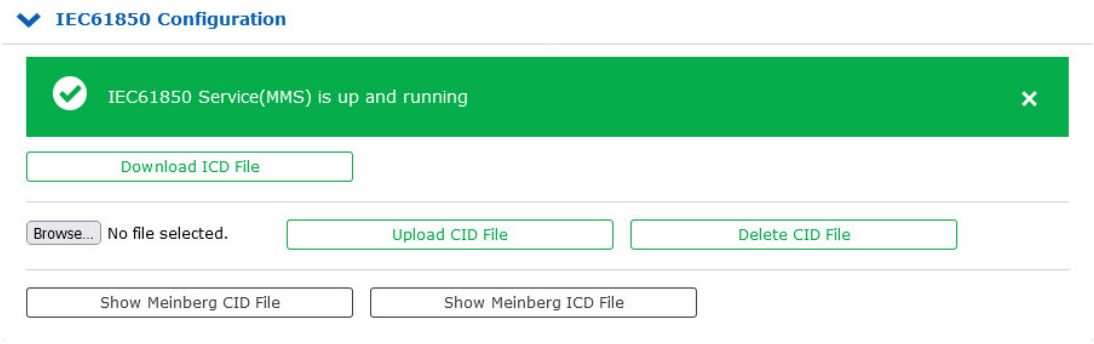
The Extended Network Configuration are not enabled for security reasons. This function can be subsequently enabled / controlled via an SSH connection in */etc/mbg/msc.cfg* with the "DISABLE SCRIPT" parameter.



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.



10.1.3.10 IEC 61850 Configuration

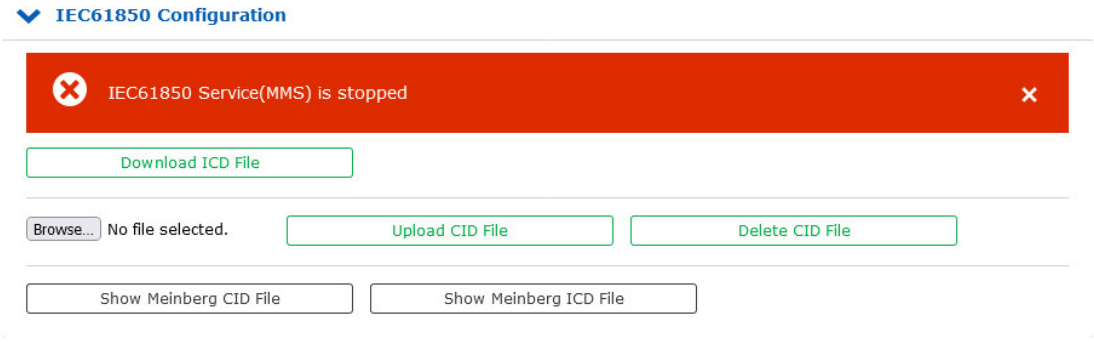


The IEC 61850 standard defines communication protocols used by networked devices in electrical substations for data exchange. These protocols can run over a TCP/IP network (OSI Layer 3) or directly over an OSI Layer 2 Ethernet network (a substation LAN, for example). The standard also describes protocol mappings to a variety of established real-time data model mechanisms, specifically the **Manufacturing Message Specification (MMS)**, **Generic Object Oriented System Events (GOOSE)**, **Sampled Values (SV)**, and **Sampled Measure Values (SMV)**.

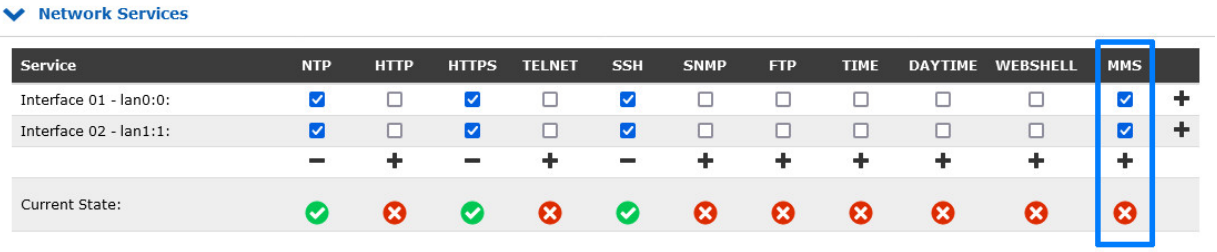
This communication and data modeling standard establishes a common approach to communication between a number of networked device types in substation management, specifically IEDs (Intelligent Electronic Devices) and SCADA control systems (Supervisory Control and Data Acquisition).

The capabilities of IEDs are described using the XML-based **System Configuration Language (SCL)** in **IED Capability Description (ICD) files**. These files are imported into a **System Configuration Tool (SCT)** to form part of a **System Configuration Description (SCD) file** intended to describe all devices present in a substation.

LANTIME servers support the aforementioned MMS protocol for communication with IEDs in the substation network. This requires the LANTIME's MMS service to be enabled; if it is not, a warning dialog box will be displayed prominently to this effect:



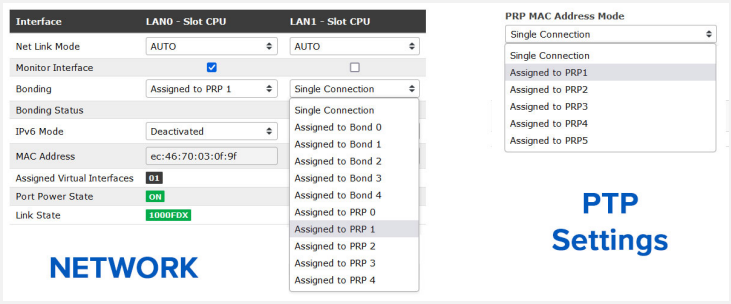
The MMS service can be enabled under the **Network Services** panel of the **Network** menu by activating the checkbox for the relevant virtual interfaces as shown below:



Manufacturers of devices intended to be used in substations usually supply the corresponding ICD files for their devices themselves, and Meinberg's LANTIME servers are naturally no exception in this regard; clicking on **Download ICD File** from this section of the Web Interface will cause the browser to download the corresponding file. Alternatively, the contents of the ICD file can be viewed directly in the Web Interface by clicking on **Show Meinberg ICD File**.

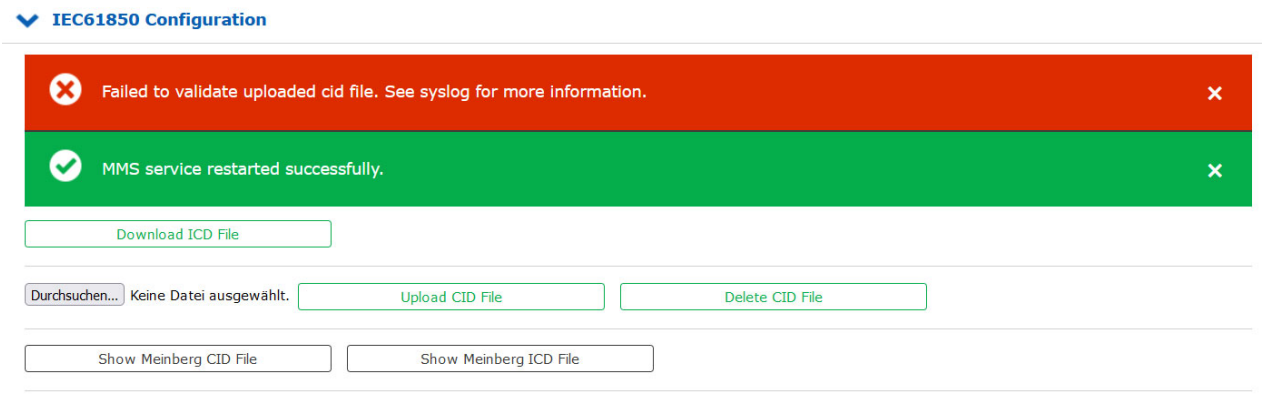
Important!

Before the ICD file is downloaded, any PRP-related network configuration must be performed via the menu "Network → Physical Network Configuration" and in the drop-down box "PRP MAC Address Mode" under "PTP → PTP Configuration → Network".



Once the ICD file has been imported into your SCT, it should be able to export a **Configured IED Description (CID) file** that contains information needed by the "IED" (in this case, the LANTIME) to allow it to configure itself for the substation in question. This CID file can be uploaded to the LANTIME by clicking on the "***Browse***" button, selecting the corresponding CID file from the appropriate folder via the file browser, and then clicking on the button **Upload CID File**. If it is successful, you should be prompted to save the new startup configuration.

If the process fails (e.g., due to a malformed CID file), the following error will be displayed:

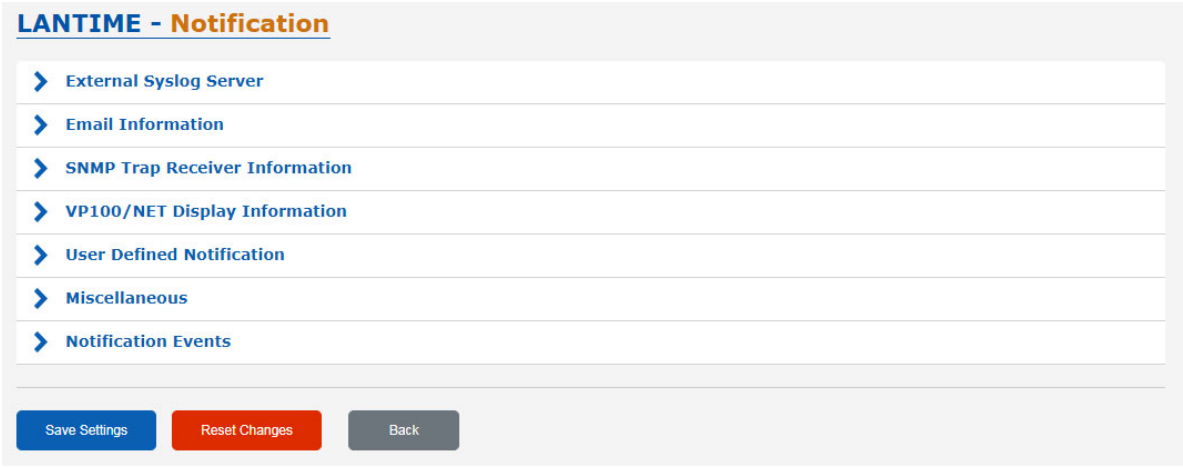


Information:

This error will also be displayed if **Upload CID File** is clicked on before a file is selected. Clicking on **Upload CID File** will not open the file browser; this can only be done by clicking on the ***Browse...*** button.

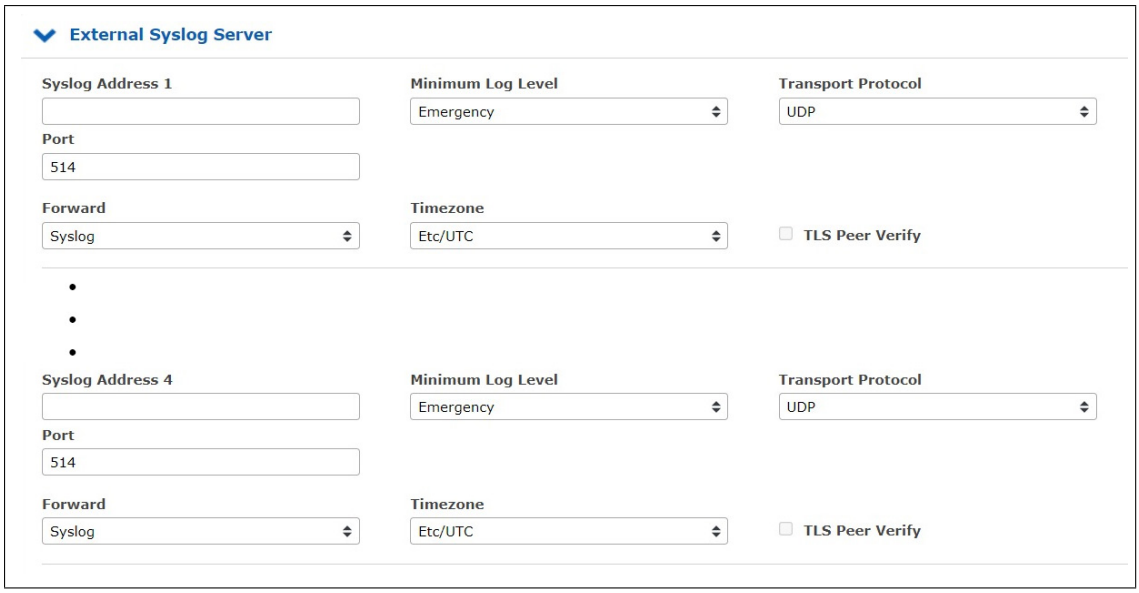
Detailed information about the IEC 61850 standard can be found in the appendix in the chapter Fundamentals of IEC 61850.

10.1.4 Notification

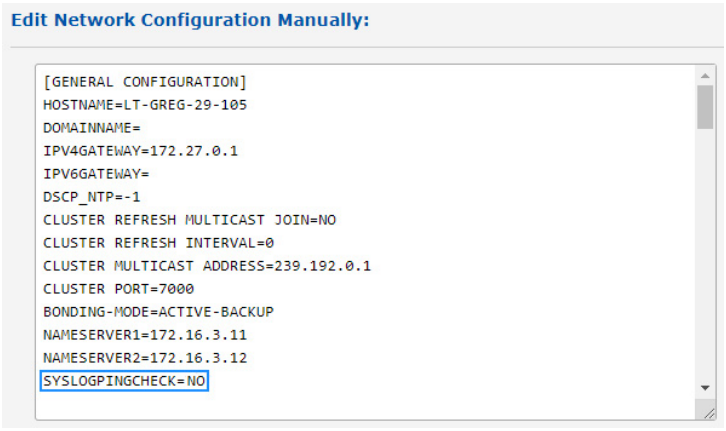


10.1.4.1 External Syslog Server

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



Syslog-Address(es):
You can enter up to 4 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.

Minimum Log Level: Log Level Configuration
Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug

Transport-Protocol: Transport - Protocol Configuration:

UDP	connectionless transmission
TCP	connection oriented
TLS	can be selected to securely transport the logging information to an external syslog server.

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

Forward: Syslog
Everything that is logged internally to the /var/log/messages file is also sent to the configured syslog server (of course considering the configured log level).

Format:
```
Mar 22 15:35:56 su-rims1-1 PAM-tacplus[3431]:
user not authenticated by TACACS+
```

Notification/Text
Only the events that are listed in the event list under "Notification → Notification Events" are sent to the syslog server.

Format:
```
DAEMON.INFO: Mar 22 14:39:55 su-rims1-1 ext_syslog_cfg_text:
Device Configuration Changed
```

Notification/Splunk
Same as before, only the format differs:

Format:
```
Mar 22 14:41:46 su-rims1-1 ext_syslog_cfg_splunk:
msg_nr=20, msg_name=Device Configuration Changed,
msg_txt=, add_txt=
```

Notification/JSON
Same as before, only the format differs:

Format:

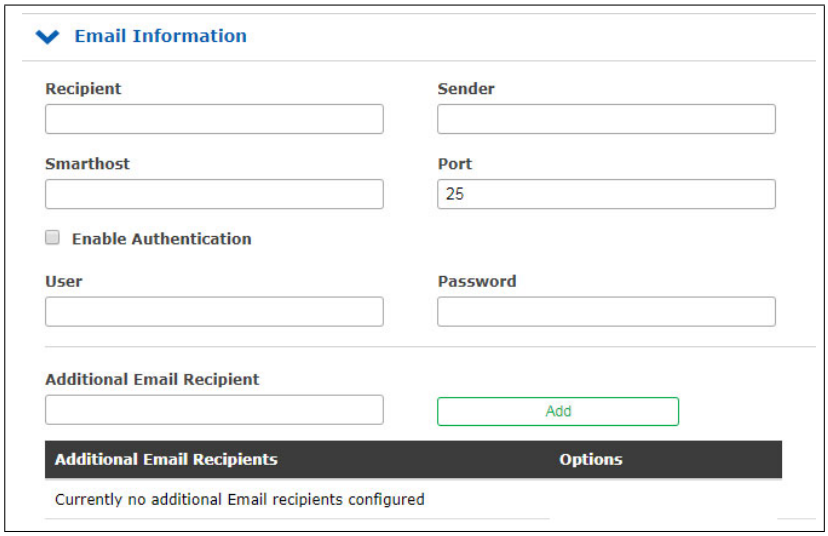
```
Mar 22 14:43:57 su-rims1-1 ext_syslog_cfg_json:
{
 'msg_nr':  '20',
 'msg_name':  'Device Configuration Changed',
 'msg_txt':  '...',
 'add_txt':  '...'
}
```

Timezone: Specifies the time zone of forwarded log events.

TLS Peer Verify: The TLS Peer Verify option specifies whether the logging server's certificate should be verified. An authentic connection is only possible with this setting. If this option is active, make sure that a root CA certificate for the syslog server has been uploaded under "Security → Certificates → CA Certificates"
has been uploaded. For information on uploading CA certificates, see chapter CA Certificates.

10.1.4.2 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.



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.

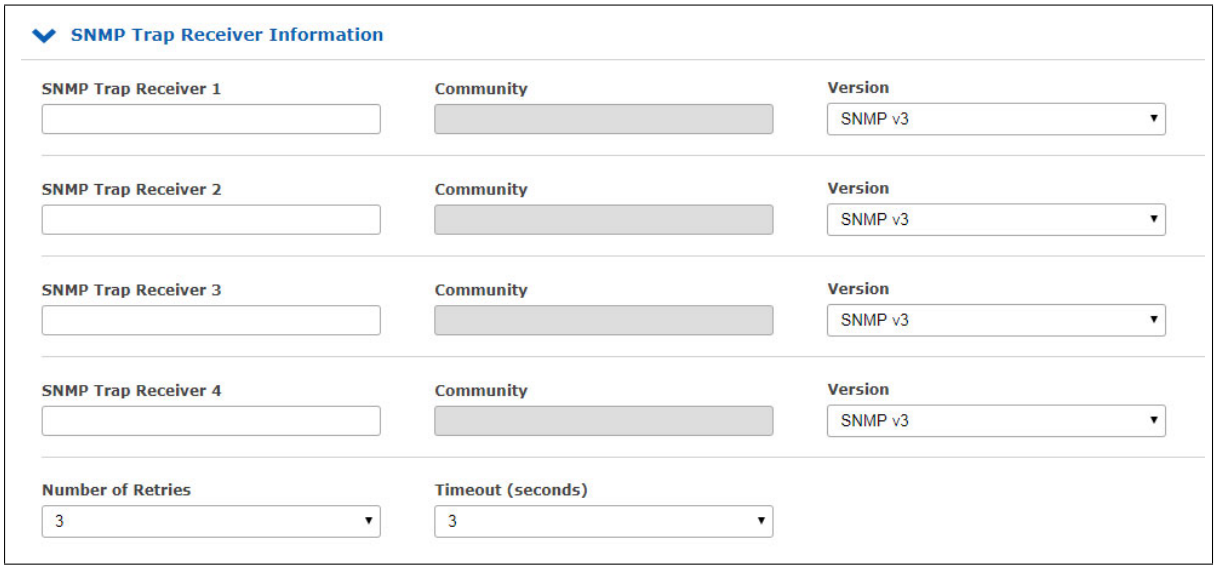
Activate Authentication: (Checkbox) Many mail servers require a valid authentication. Please check mark the box to activate it.

Username/ Password: Please enter a valid access for the e-mail server.

Additional E-mail Recipients: Configuration of additional e-mail recipients.

10.1.4.3 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: IP address or hostname of the SNMP trap receiver.

Community: SNMP Read Community of the Trap Receiver.

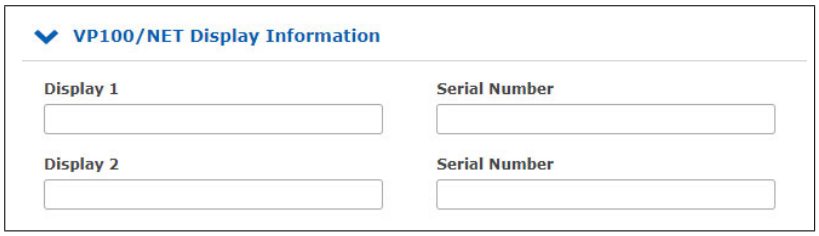
Version: SNMP version to use.

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

Timeout: Connection timeout value.

10.1.4.4 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 Addres 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.

10.1.4.5 User defined Notifications

Important!

The configuration of user-defined notifications requires advanced system administration knowledge and is therefore disabled by default.

To unlock this option, the entry **DISABLE SCRIPT** must be set to *NO* in the editor provided under "System → Services and Functions → Manual Configuration → Standard Configuration → Miscellaneous Configuration".

Alternatively, this option can be disabled or enabled by modifying the file */etc/mbg/msc.cfg* in the same way when accessing your IMS LANTIME over an SSH or serial terminal connection.

Regardless of the **DISABLE SCRIPT** setting, superuser permissions are always required to access the user-defined notifications editor.

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.

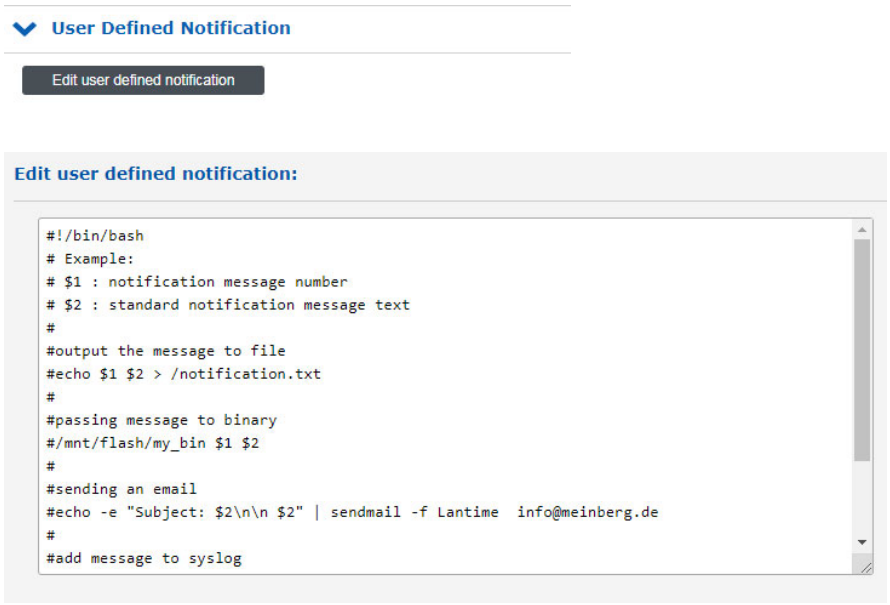


Figure: In the submenu "Edit user defined notification", you can select the system events on which the script should be executed.

10.1.4.6 Notification - Miscellaneous

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.

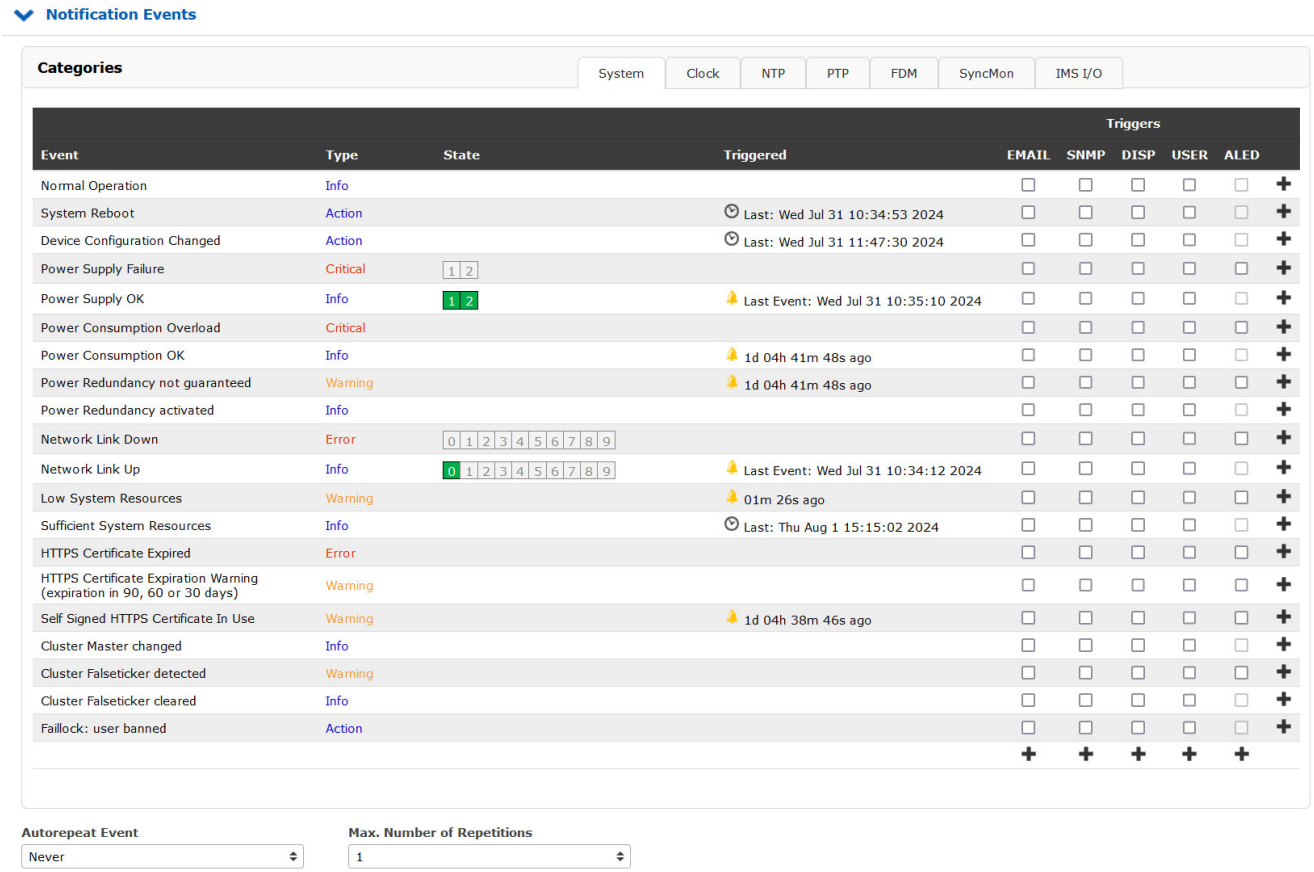
Only when using a PZF Clock

PZF: Delay Not Sync/Antenna Connection Fault Message (s)
To avoid unnecessary notifications, a time interval in seconds can be entered in this field. If 900 (seconds) is entered here, as shown in the illustration, the system waits 900 seconds or 15 minutes after a reception error occurs before sending a notification.

The DCF77 transmitter sends 59 bits of time and date information per minute. The PZF clock performs a plausibility check once a minute. If the transmission of just one bit fails, the clock goes into the “async state”. If the sync state is restored within the set time interval (900 seconds in the example), no notification is sent.

10.1.4.7 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:



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 (see chapter "Error Relays")

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

Categories

For a better overview, the events that can trigger notifications are sorted into categories. The following tabs are available in this menu to select the desired category:

System System notifications such as “System Reboot” on system restart.

Clock Notifications about the status of the clock in use, e.g. “Clock not Sync” if the reference clock is not synchronized.

NTP NTP status notifications, e.g. “NTP Stopped” when the NTP service is stopped.

PTP Status notifications of the PTP module, e.g. “PTP Link Down” if there is no network connection.

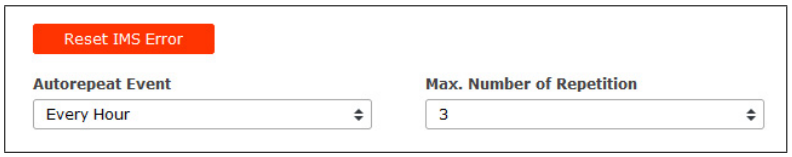
FDM Notifications about the FDM module in use, e.g. “FDM Error” if adjusted tolerance values for time or frequency are not met.

SyncMon Notifications from the Sync Monitor, e.g. “Sync Monitor Alert” if a network node is not accessible.

IMS/IO Status messages about the IMS I/O modules used, e.g. “IMS Error” if an error is detected in an IMS module.

A complete list of all notifications and the respective severity levels can be found in the chapter Overview for all Events.

Reset IMS Error



Removing an IMS module triggers a permanent error in the system. If modules are intentionally removed, the "**Reset IMS Error**" button at the bottom of the event table is available in the "Notifications" submenu. With this button all registered IMS errors can be reset.

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.

Example:
If the "Autorepeat Event" is set to "Every hour" and the "Max. number of Repetition" is set to the value 3, then the system will send a total of four notifications. The first one when the event occurs. Then one notification per hour for the next three hours.

10.1.4.8 Overview for all Events

Event	Severity Levels (according to X.733)	Description
System Events		
Normal Operation	Info	Indicates normal operation of the LANTIME
System Reboot	Action	The system has restarted
Device Configuration Changed	Action	Software configuration of the LANTIME has been changed
Power Supply Failure	Critical	Error detected on a power supply -> Safety During Operation
Power Supply OK	Info	Power supply ready for operation
Power Consumption Overload	Critical	Overload of the power supply unit(s). There are not enough power supply units in use -> Redundant Power Supply
Power Consumption OK	Info	The power supplies used provide sufficient power for the system
Power Redundancy not guaranteed	Warning	In case of failure of a power supply unit, trouble-free operation is no longer guaranteed -> Redundant Power Supply
Power Redundancy activated	Info	Normal operation is ensured even after the failure of a power supply unit
Network Link Down	Error	No network connection on one of the LAN ports -> Network Messages
Network Link Up	Info	Network connection detected on the LAN port
Low System Resources	Warning	Low system resources detected
Sufficient System Resources	Info	System resources restored
Fan Failure	Critical	An error has been detected on a fan -> Miscellaneous Messages
Fan OK	Info	No mistakes on installed fans
Certificate Expired	Error	HTTPS certificate has expired -> Certificates
HTTPS Certificate Expiration Warning (expiration in 90, 60 or 30 days)	Warning	HTTPS certificate expire in 90, 60 or 30 days -> Certificates

Table: All Notification Events

Event	Severity Levels (according to X.733)	Description
Self Signed HTTPS Certificate In Use	Warning	The certificate used is self-signed and does not come from an official certification authority -> Certificates
Cluster Master Changed	Info	The master of a LANTIME NTP cluster has changed -> Menu: Network
Cluster Falseticker detected	Warning	An NTP falseticker was detected in the cluster compound
Cluster Falseticker cleared	Info	Previously detected cluster falseticker is back in order
Faillock: user banned	Action	Failed login - user is temporarily locked
NTP Events		
NTP Not Sync	Error	NTP Service is not sync -> NTP Messages
NTP Sync	Info	NTP service is successfully synchronized
NTP Stopped	Critical	NTP service stopped -> NTP Messages
NTP Offset Limit exceeded	Error	Maximum NTP offset value has been exceeded -> SyncMon
NTP Offset Limit OK	Info	Maximum NTP offset not exceeded -> SyncMon
Clock Events		
CLK[NR] Not Responding	Critical	Receiver module is not responding -> Ref. Clock Messages
CLK[NR] Not Sync	Error	Receiver module is not sync -> Ref. Clock Messages
CLK[NR] Sync	Info	Receiver module is synchronous to its time source
Antenna Faulty	Error	No antenna or sufficient signal was detected -> Ref. Clock Messages
Antenna Reconnect	Info	Antenna / signal was detected by the LANTIME
Antenna Short Circuit	Error	Short circuit at the antenna connection -> Ref. Clock Messages
Leap Second Announced	Info	A leapsecond was announced

Table: All Notification Events

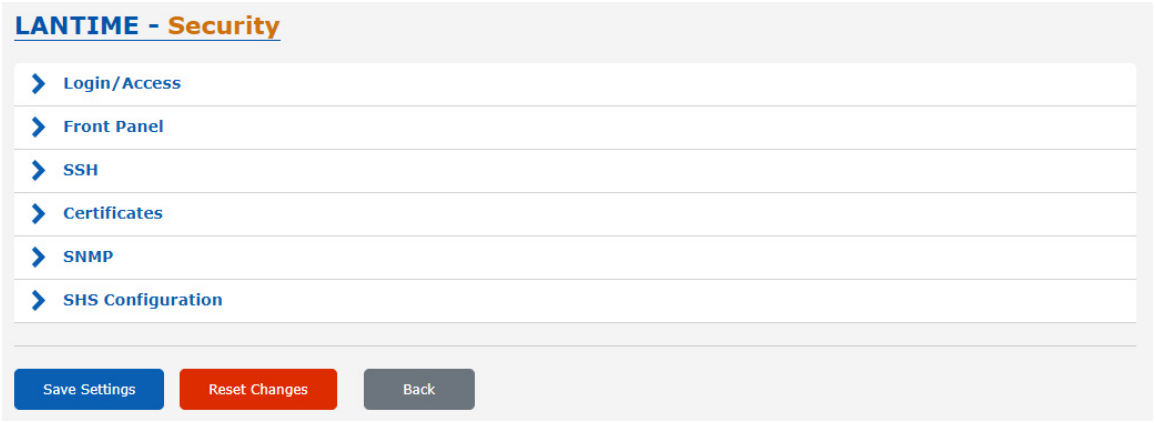
Event	Severity Levels (according to X.733)	Description
SHS Time Limit OK	Info	The set SHS time limit value has not been exceeded
SHS Time Limit Warning	Warning	The set threshold for an SHS warning has been exceeded
SHS Time Limit Error	Critical	The set threshold for an SHS error has been exceeded -> SHS Configuration
MRS Source: Limit Exceed	Error	Set MRS limits have been exceeded -> Ref. Clock Messages
MRS Source: No Signal	Warning	A configured MRS time source is no longer available -> Ref. Clock Messages
MRS Source: Signal Detected	Info	A configured MRS time source is available
MRS Source: Selected Signal Changed	Action	The active MRS source has changed
MRS Source: Invalid Signal	Warning	A configured MRS source provides an invalid signal
MRS Source: Signal OK	Info	The configured MRS source provides a valid signal
Oscillator Adjusted	Info	Internal oscillator runs stably and is completely adjusted
Oscillator Not Adjusted	Warning	Internal oscillator is not adjusted -> Ref. Clock Messages
Trusted Source OK	Info	The source selected as trusted is in the configured offset range -> Extended Options
Trusted Source Error	Error	Offset limit violation of trusted source used -> Extended Options
Sync Monitor Events		
Sync Monitor	Action	Sync Monitor limits were exceeded
Sync Monitor Alert	Error	SyncMon malfunction - monitored network node is unreachable -> Error Logs
Sync Monitor OK	Info	No malfunction detected in Sync Monitor
FDM Events (only if an FDM module is in use)		

Table: All Notification Events

Event	Severity Levels (according to X.733)	Description
FDM Error	Error	The deviation of the time or frequency of the monitored mains is outside the adjusted tolerance
FDM OK	Info	The monitored mains frequency and time deviation is within the adjusted tolerance range
PTP Events (only if an PTP module is in use)		
PTP Link Down	Error	No network connection on the PTP network port
PTP Link Up	Info	Network connection detected on the PTP network port
PTP State Changed	Info	The current PTP status has changed
PTP Error	Error	A PTP error has been detected -> PTP Global Status
IMS I/O Events (only for IMS systems)		
IMS Error	Error	An error has been detected on an IMS module -> Miscellaneous Messages
IMS OK	Info	IMS module is error-free
ESI: ITU limits violated	Error	Exceeding or falling below the recommendations defined by ITU-T -> IMS - LIU (Line Interface Unit)
ESI: ITU limits adhered	Info	ITU limits are complied with
Sync-E Input Quality Level Changed	Info	The quality factor of the SyncE reference has changed -> Option SyncE Configuration
Port Error	Error	E.g. short circuit at the input of an IMS-VSI reference card
Port Ok	Info	Signal at the port is OK (the card must support the port event - e.g. IMS-VSI).

Table: All Notification Events

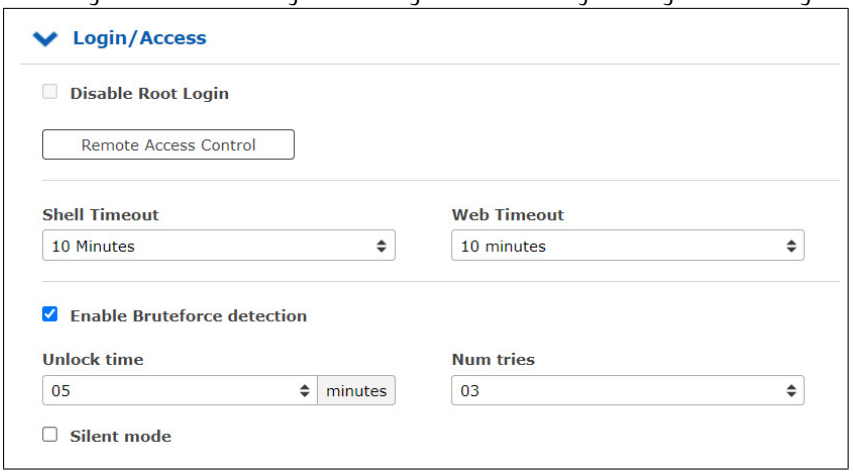
10.1.5 Security



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.

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 to be allowed to access the Web interface. After the first entry, access to all other clients is automatically blocked. Individual client IPs or entire subnets can be configured.

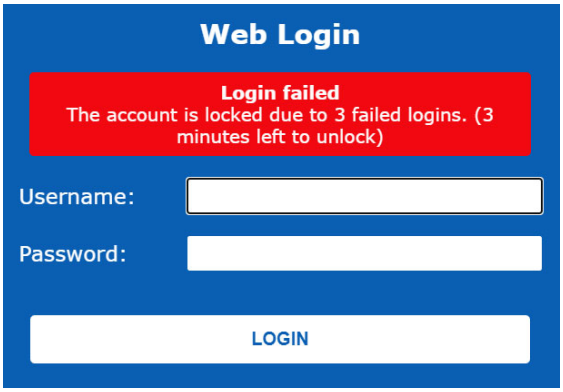
Shell Timeout:
Defines a timeout in seconds. After expiration of this period without any user interaction, the current session on the command line will be terminated for the logged-in user.

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.

Enable Bruteforce Detection:
When bruteforce detection is enabled, user accounts are temporarily locked after too many failed login attempts.

Unlock Time:
The unlock time, is the time until a locked user is unlocked again.

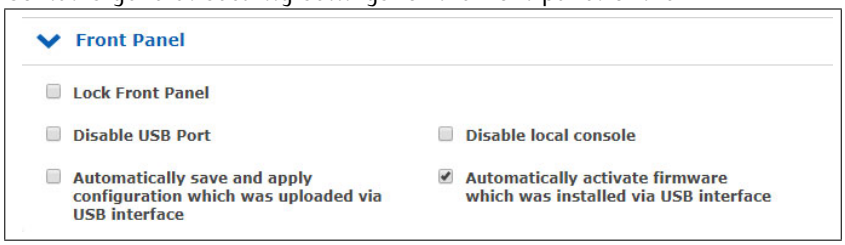
Number of Attempts:
The number of attempts, is the number of login attempts that must fail before a user account is locked.



Silent Mode:
Silent mode prevents the SSH and web interface from reporting a user's lock status. This also prevents the disclosure of valid user names to attackers, but reduces the traceability of users who have accidentally entered their login data incorrectly too often and cannot log in during the lockout period even with valid data.

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.

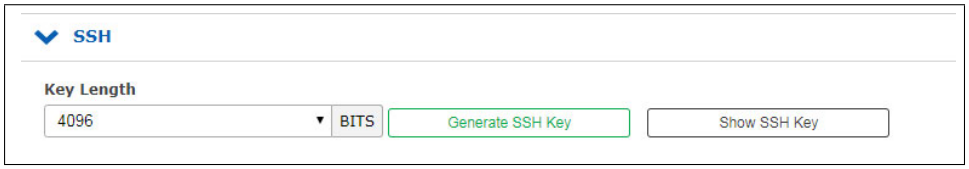
Checkbox "Automatically save and apply configuration which was uploaded via USB interface"
You can install a previously saved configuration on your LANTIME via the USB stick menu, if you have activated this check box, the uploaded configuration will be taken over directly as the start configuration.

Checkbox "Automatically activate firmware which was installed via USB interface"
By activating this checkbox, a firmware version loaded via the USB menu on the LANTIME will be directly taken over as active firmware.

Also see USB Stick Menu.

10.1.5.1 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 10.1.3.3 "Web GUI → Network → Network Services").

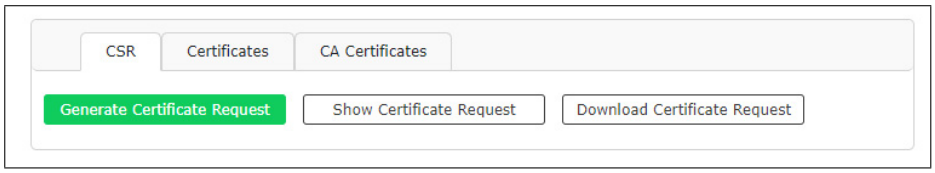


Key Length (Bits):
Determines the key length for a new key to be generated.

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.

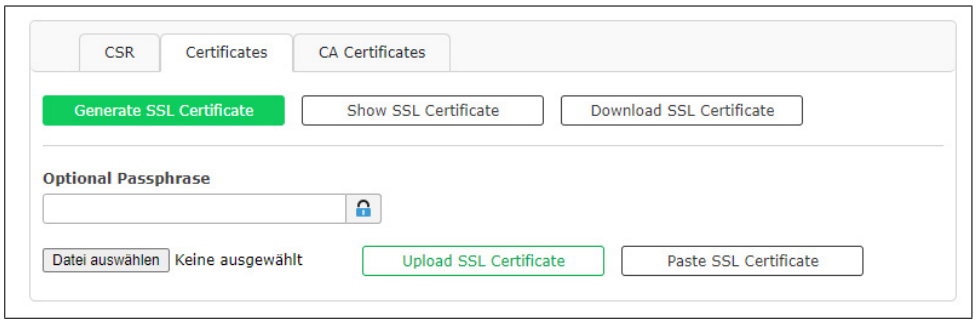
10.1.5.2 Certificates



HTTPS is a standard for enabling the encrypted transmission of data between a web browser and a web server. It relies on X.509 certificates and asymmetric cryptographic methods. The time server uses X.509 certificates to authenticate itself to a client (web browser). When a web browser connects to the HTTPS web server of your LANTIME system for the first time, you will be prompted to accept the certificate of the web server.

To verify that you are actually communicating with your time server, review the certificate and only accept it if it corresponds to the certificate stored on the LANTIME system. Upon each subsequent connection, the browser will compare the certificate with the one stored locally in your web browser.

Note: The LANTIME has a pre-installed default certificate that is self-signed, not signed by a Certificate Authority (CA). Some web browsers will react to this by reporting that the connection is not secure. If you wish to install a certificate that has been signed by a trusted Certificate Authority, you can use the "Upload SSL Certificate" below. More information on this is provided in the instructions below.



Generate SSL Certificate:
Generates a new self-signed SSL certificate.

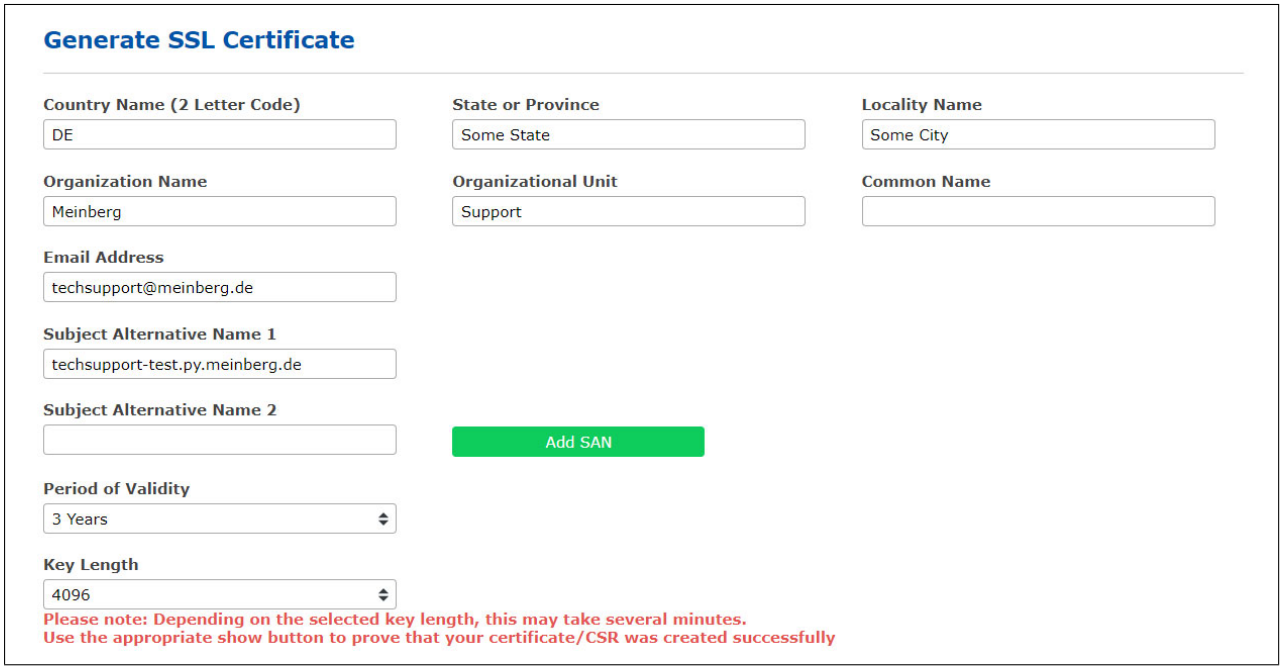
Show SSL Certificate:
Allows the currently installed SSL certificate to be reviewed.

Download SSL Certificate:
Downloads the currently installed SSL certificate.

Optional Passphrase:
If the private key uploaded with the SSL certificate is protected with a passphrase, this passphrase must be entered here. Without the passphrase, the web server will be unable to start automatically, as it will not be able to decrypt the uploaded key.

Upload SSL Certificate:
Allows a certificate signed by a trusted Certificate Authority to be uploaded. This certificate must be in PEM file format.

Generate Certificate Request:
This function generates a Certificate Signing Request (CSR) that can be sent to a Certificate Authority for the purpose of requesting a signed certificate. This process generates a certificate and a private key on the LANTIME system. The storage location of the CSR is */mnt/flash/data/https.req*", while the corresponding key is deposited at *"/mnt/flash/data/https.req.pk"*.



Subject Alternative Name
The "Subject Alternative Name" field can be used to specify additional hostnames (sites, IP addresses, common names, etc.) to be protected by a shared SSL certificate, such as a multi-domain certificate. Multiple SANs can be specified via the "Add SAN" button. The type of SAN, such as an IP address or DNS address, is determined automatically. The Common Name can be specified separately from the SAN.

Note:
If the certificate submitted to the Certificate Authority has been generated on the LANTIME system using the "Generate Certificate Request" function, the corresponding key for this certificate will be available under *"/mnt/flash/data/https.req.pk"*. Once the signed certificate is uploaded, this previously generated key will be used.

If the submitted and signed certificate was not generated on the LANTIME system, then the PEM file must contain both the private key and the certificate itself.

The private key starts with:
"—BEGIN RSA PRIVATE KEY—"
and ends with:
"—END RSA PRIVATE KEY—"

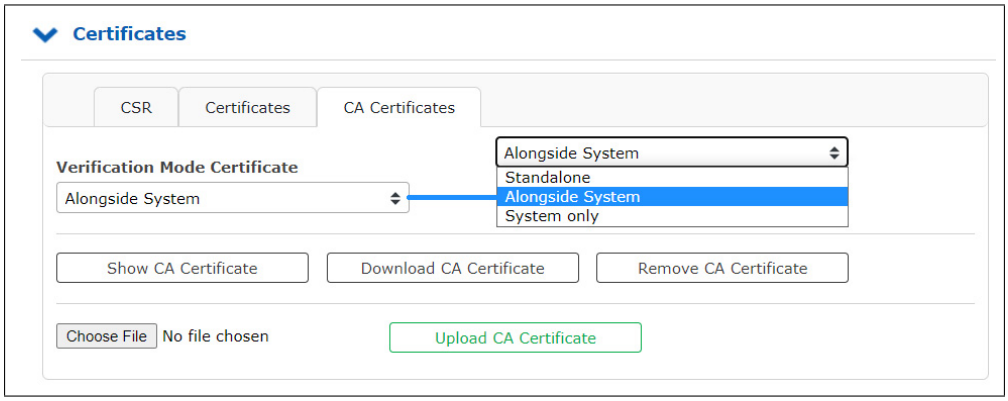
The certificate itself starts with:
"—BEGIN CERTIFICATE—"
and ends with:
"—END CERTIFICATE—".

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---
```

10.1.5.3 CA Certificates

The functions in the menu "Security → certificates → CA certificates" can be used to add an own, non-public root certification authority to the LANTIME. This allows programs and services which establish a TLS connection, e.g. the LDAP service, to uniquely identify the requested server, even though no (mostly paid) certificate of a public certification authority is used.



The Certificate Verification Mode can be selected as follows:

Standalone: The LANTIME uses only the uploaded own root certificate to verify connections.

Alongside System: The LANTIME uses the uploaded own root certificate and the system known public certification authority certificates.

System only: The LANTIME uses the system known public certification authority certificates.

10.1.5.4 Uploading Signed Multi-Level Certificates/Certificate Chains

Support is provided not only for SSL certificates but also multi-level certificates and certificate chains. Certificate chains can be uploaded together with the server certificate and private key in PEM format.

Certificate chains should be entered in the correct order to avoid potential problems. The first certificate must be the server certificate, followed by the intermediate certificates. The (optional) root certificate can be used to mark the end of the file. The key for the server certificate should be entered directly before or directly after the server certificate.

10.1.5.5 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.

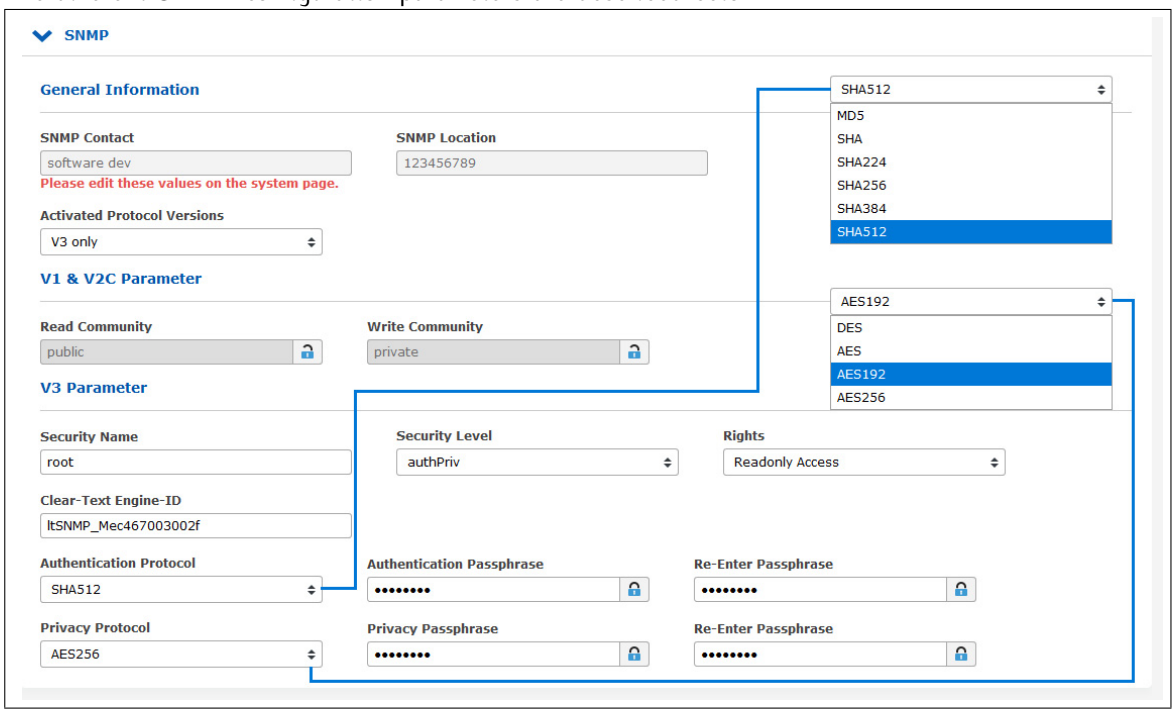
The Meinberg SNMP MIB Files can be downloaded on the "System" page → Services and Functions → Download SNMP MIB". The files named "MBG-SNM P-ROOT-MIB.mib" and "MBG-LANTIME-NG-MIB.mib" need to be used to monitor a LANTIME system.

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

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

(see also configuration chapter "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 an 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"

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):

- MD5
- SHA
- SHA224
- SHA256
- SHA384
- SHA512

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):

- DES
- AES
- AES192
- AES256

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

10.1.5.6 SHS Configuration

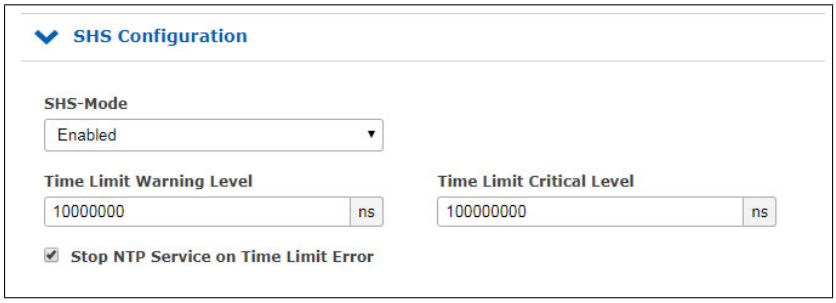
SHS is the abbreviation for Secure Hybrid System and is available on LANTIME systems with two reference clocks. When the SHS mode is enabled only the currently active clock is used for passing the timing signal on to the NTP service, the other clock is indicated as “no select” and used only for measuring 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 trigged 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.



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")

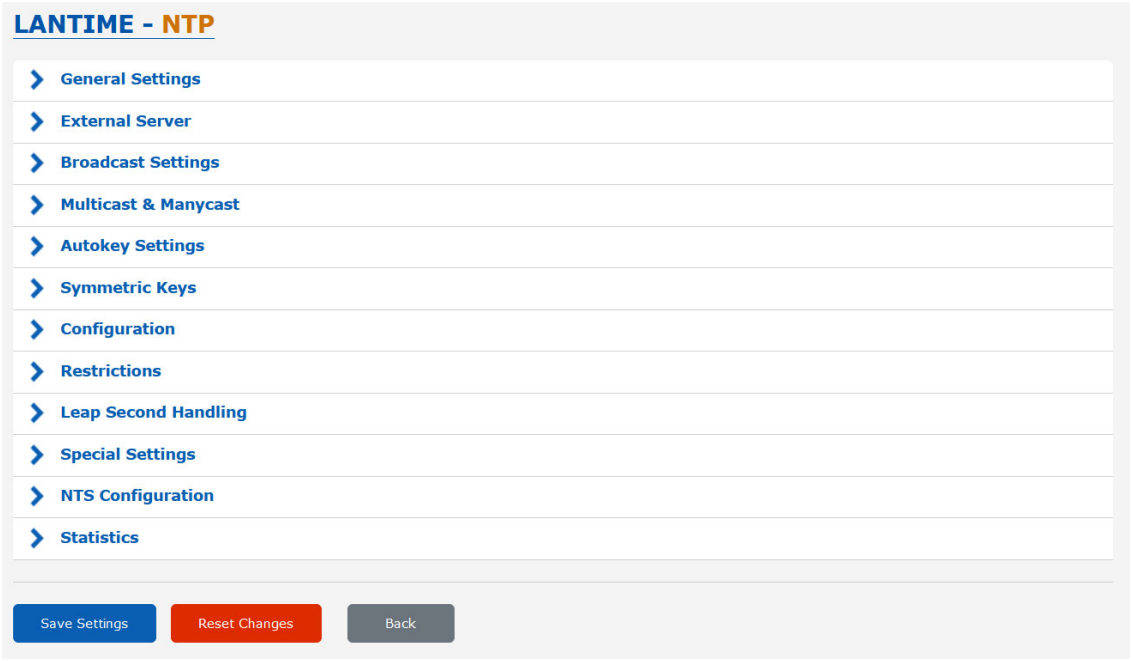
In LANTIME IMS systems with a built-in RSC, the parameter is configured in nanoseconds. For systems without an RSC in milliseconds.

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.

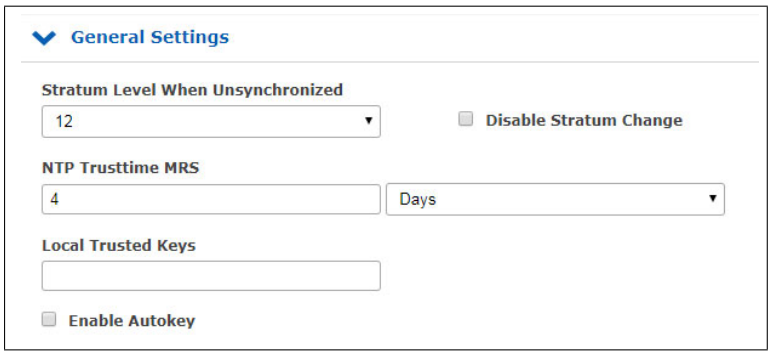
Stop NTP Service on Time Limit Error
Here you can decide if the NTP service is to be terminated at the Critical "TimeLimitError". In this case, requesting NTP clients would no longer receive a response from the time server.

10.1.6 NTP



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

10.1.6.1 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 Trustime 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 Trustime

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.

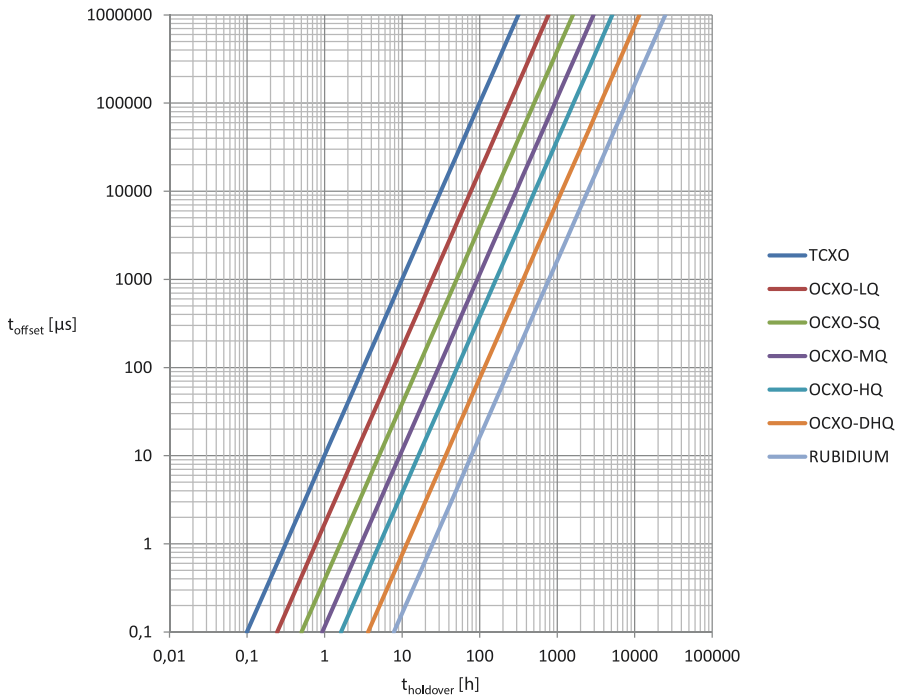


Figure: relation between holdover time (x) and offset (y) by using of built-in Meinberg oscillators

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.

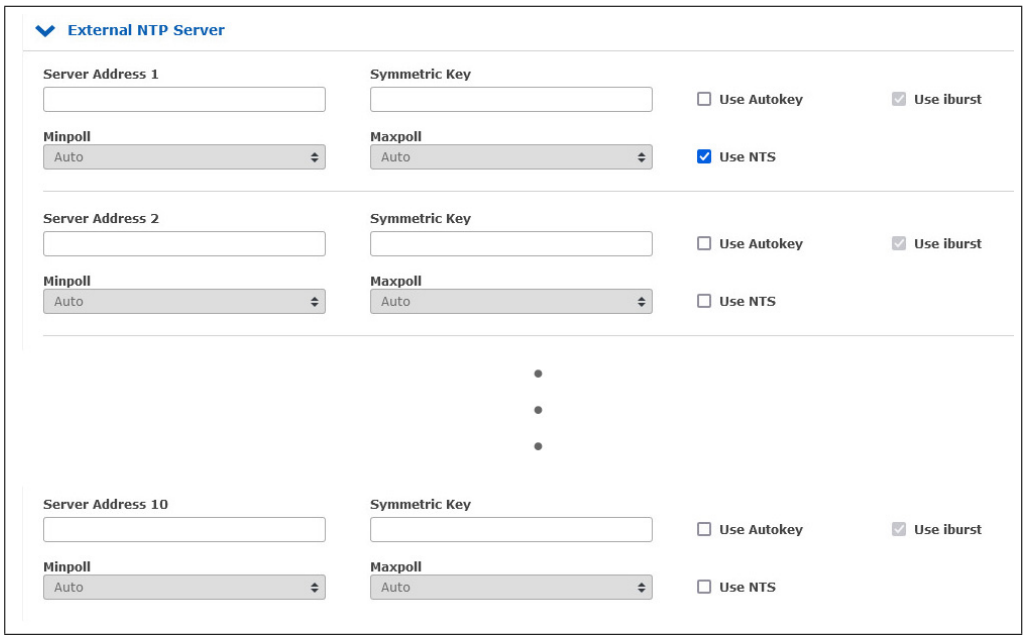
Procedure: First you should find out which oscillator is used. Go to the web interface menu "Monitoring and Management → Clock → Receiver Information → Oscillator Type". Then you can define an offset, from which the NTP should lose its stratum or the trust time.

A list of oscillators available for Meinberg reference clocks:
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.

10.1.6.2 External NTP Server

Via the configuration page you can enter up to 10 external NTP server as backup for the internal reference clock.



Server Address:
IP or 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.

The following must be considered, 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 "Local Trusted Keys" under "NTP → General Settings".

c) The same key with the same ID must be configured on the external server.

Minpoll and Maxpoll (not supported on devices which support the MRS feature):
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 (not supported on devices which support the MRS feature):
The iburst activation accelerates the initial synchronization with an external server.

Use NTS (only available on devices that support the MRS function)
This option activates Network Time Security for the respective external NTP server. If NTS is activated, no further authentication procedure can be used for this server. The configuration of symmetric keys or autokey is thus ignored for this server.

For NTS authentication to work, the following points must be taken into account:

- The server address entered must correspond to that of the NTS-KE server.
- To be able to verify the NTS-KE server, a corresponding root certificate must be available on the LANTIME (see CA Certificates).

Particularity LANTIME/MRS:
All external NTP servers are requested for statistical purposes only and are never directly selected as synchronisation peers by the time service. Normal NTPv4 servers are added as "noselect" in the NTPD configuration file */etc/ntp.conf* for this purpose.

Since NTPD currently does not support Network Time Security, external NTS servers are requested via a separate Chrony time service.

The LANTIME MRS logic then selects the best server among all servers. The selection algorithm for the best external NTP server is separated in the following steps:

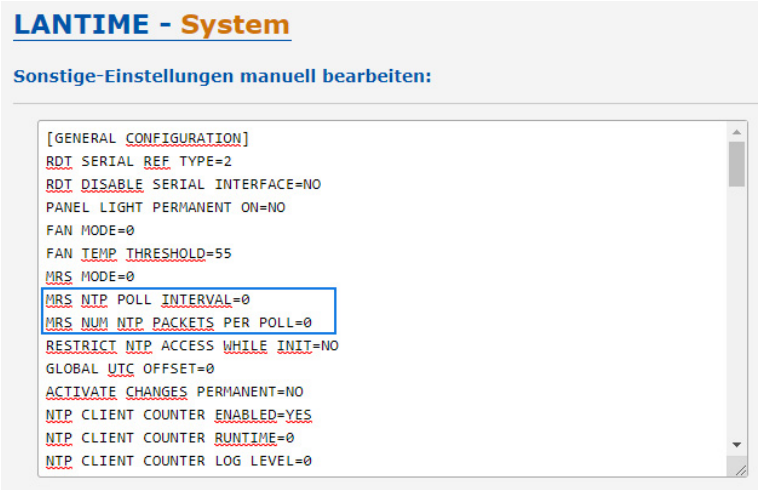
- select which server is accepted
- create groups of different offsets
- select the biggest group
- check for outliers and remove them from that group
- use the median as best-server
- check if last_best_external_NTP_server can be used - to reduce clock hopping

The best server can be checked in the Web Interface under "Statistics → NTP Status" and under "Clock → Status & Configuration → MRS Status". The determined offset is then used to discipline the internal oscillator in case no other reference source with a higher priority is available.

Due to this particularity, the configuration possibilities for external NTP server are different. The parameters Minpoll, Maxpoll and Iburst cannot be configured on a LANTIME/MRS.

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:

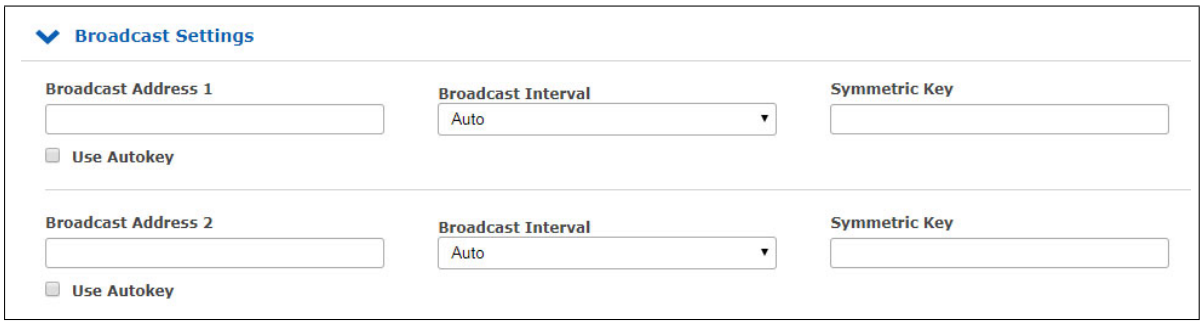
Web Interface - "System Page → Services and Functions → Manual Configuration → Standard Configuration → Miscellaneous Configuration"



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.

10.1.6.3 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.

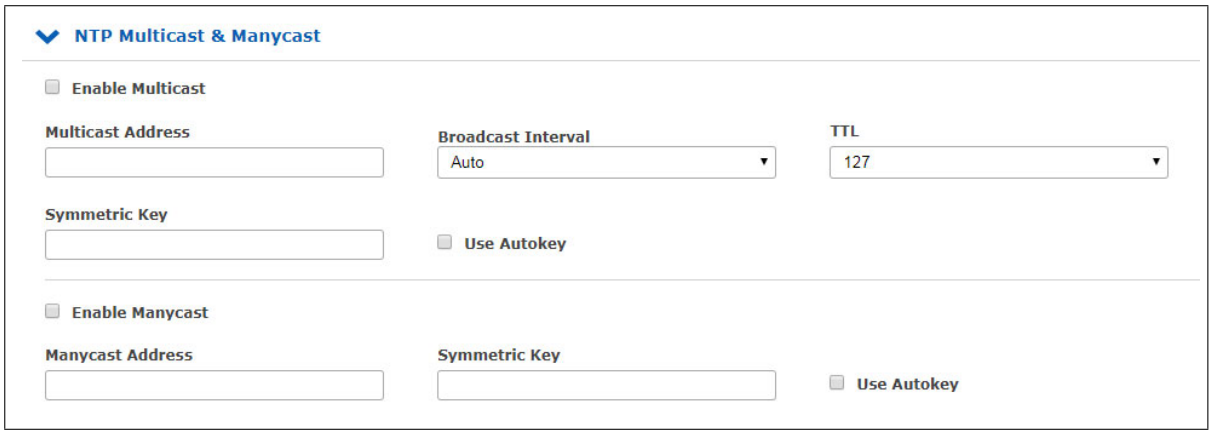
b) Additionally you must enter the ID into the field "Trustable Keys" under "NTP → General Settings".

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
```

10.1.6.4 NTP Multicast and Manycast



10.1.6.5 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:

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 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
```

10.1.6.6 NTP Manycast

NTP Manycast 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 mutlicast IP. The Manycast 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 Manycast: It activates the Manycast-Feature

Manycast Address: Address field for entering the manycast address (mutlicast 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 Manycast, 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:

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".

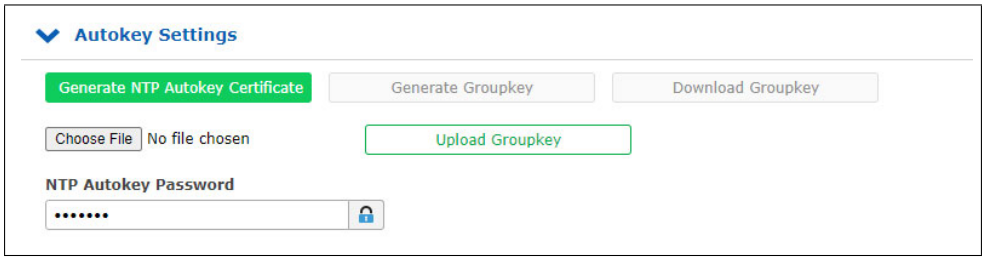
c) The same key with the same ID must be configured on the NTP client.

The following is an excerpt from the NTP configuration of a client,
which is configured as a 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
```

10.1.6.7 NTP Autokey Settings

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



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

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

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

b) Host
One or more NTP servers, which do not own a "trusted" certificate, but only a self-signed certificate without this "trusted" mark.

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

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

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

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

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

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

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

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

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

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

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

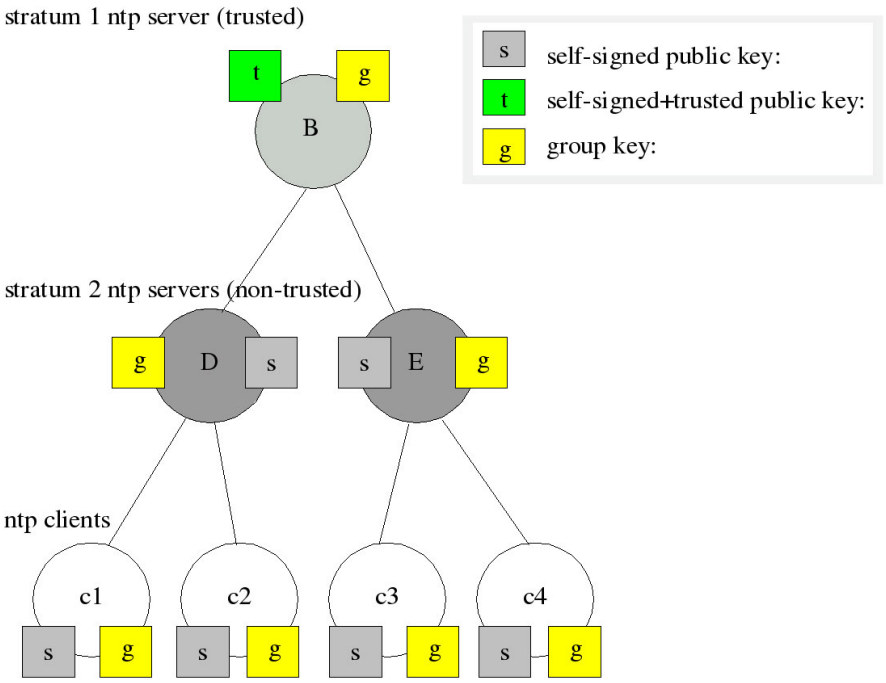
```
LantimeGpsV4:/etc/ntp # ntp-keygen -q cryptosecret
```

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

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

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

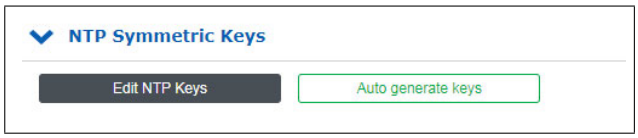
Example:
This autokey group is formed by one Stratum-1-server (B), two Stratum-2-servers (D and E) and a number of clients (in the diagram there are 4 clients shown, c1 – c4). B is the trusted host, he holds the group key and a self-signed certificate marked as "trusted".



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

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

10.1.6.8 NTP Symmetric Keys



Since NTP version 3, NTP has been providing an authentication method using symmetric keys. The "NTP 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 Keys" button allows keys to be generated automatically.

Figure: Menu "NTP → NTP Symmetric Keys → Edit NTP Keys"

Attention:
If symmetric keys are already in use and should be kept, the contents of this file must be cached before a new block is automatically generated. The contents of the "old" file must then be re-inserted into the field **Edit NTP Keys** together with the "new" keys.

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

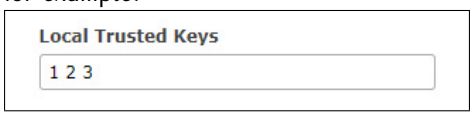
```
1    MD5        BtdW/<gj2*2M;!'~qAIN                        # MD5 Key
2    SHA1       094c533b614d9e4bcb6e18a97a7b0e4d459025bd    # SHA1 Key
3    SHA256     bb48079a17b370fb0ae48bc1a09d5e0ab1ce59fc    # SHA256 Key
4    SHA512     56b98e4d4f57d415bebbb1a0ff72c625a57d865c    # SHA512 Key
5    AES128CMAC 02eb9a63710dda360d181d9582056a504d965700    # AES128-CMAC Key
```

The first column contains a unique key ID (value range 1 - 65535). The second column contains the key type ("MD5" for an MD5 key, "SHA1" for a SHA1 key, AES128CMAC for a AES128-CMAC key etc.). The third column contains the key string, which may be between 1 and 40 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 as shown in the excerpt of an NTP key file.

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.

10.1.6.9 NTP Configuration

Important!

Editing the additional NTP parameters requires advanced system administration knowledge and is therefore disabled by default.

To unlock this option, the entry **DISABLE SCRIPT** must be set to *NO* in the editor provided under "System → Services and Functions → Manual Configuration → Standard Configuration → Miscellaneous Configuration".

Alternatively, this option can be disabled or enabled by modifying the file */etc/mbg/msc.cfg* in the same way when accessing your IMS LANTIME over an SSH or serial terminal connection.

Regardless of the **DISABLE SCRIPT** setting, superuser permissions are always required to access the additional NTP parameters editor.

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.

10.1.6.10 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 here. Client IP addresses, which are not covered in the allowed IP address ranges, will no more receive NTP responses from the LANTIME.

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.

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
```

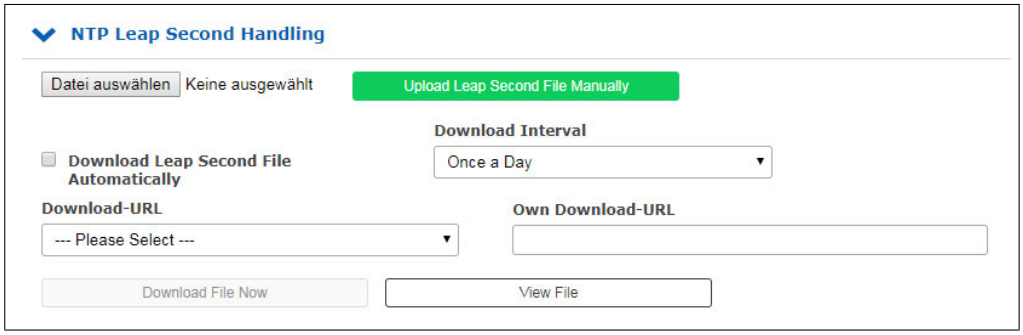
These settings cause that the server no longer responds to NTP requests. In the submenu "Configure NTP Restrictions" you can configure a “white list” of client IP addresses or even entire subnets whose requests are allowed to be answered by the server.

10.1.6.11 NTP Leap Second Handling

Most of the world's local time zones have their basis in Coordinated Universal Time (UTC). This timebase is derived from many atomic clocks distributed throughout the world in various countries. The rotation of the Earth is not constant and varies over time; the average speed of the Earth's rotation is declining gradually. This is why 'leap seconds', which account for the changing relation between UTC time and the physical rotation of the Earth, are introduced into the UTC timebase. A leap second is always added at 23:59:59 (UTC), either on December 31 or June 30. While other dates are theoretically possible, leap seconds have never been practically applied on dates other than these.

Some time information protocols and transmission technologies, among them GNSS, NTP, PTP, DCF77, and IRIG, support leap second announcements to allow receivers to prepare ahead of time for the application of a leap second. The GPS satellite system, for example, announces a leap second six months before the actual event. Meinberg LANTIME time servers with GPS receivers receive this announcements automatically via the GPS signal. This is noted in the log file of a LANTIME with the entry "Leap Second Announced" when the date of the leap second application is received.

Other synchronization methods do not support this pre-announcement approach, which can result in a second time jump. In these cases, it is necessary to keep the NTP leap second file up to date so that the leap second is correctly applied at midnight (UTC).



The menu "**NTP Leap Second Handling**" shows the currently stored leap second file, which can be uploaded manually or downloaded automatically from one of the following sites:

Available download sources for leap second files:

1. NIST Leap Second File:
   - ftp://ftp.boulder.nist.gov/pub/time/ (Directory Listing)
   - ftp://ftp.boulder.nist.gov/pub/time/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 Leap Second File)

3. Meinberg Leap Second File (Mirror of the IERS Leap Second File):
   - https://www.meinberg.de/download/ntp/leap-seconds.list
   - https://www.meinberg.de/download/ntp/leap_second

Information:

For more information on the application of leap seconds, please visit:

https://kb.meinbergglobal.com/kb/time_sync/ntp/leap_second_smearing/start

10.1.6.12 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.

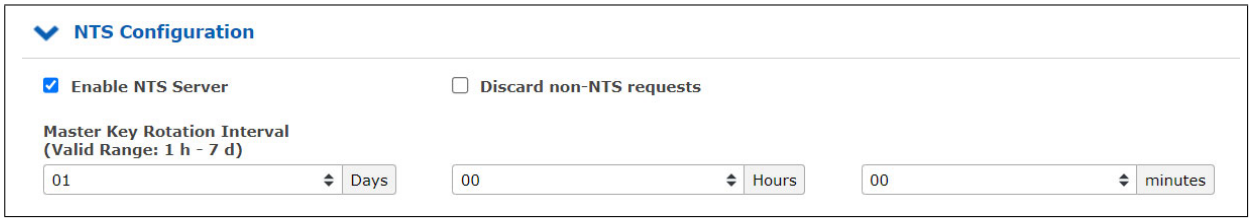
Pass-through MRS Stratum
This feature only comes into effect if you synchronize a LANTIME with MRS feature primarily via NTP. If "Pass-through MRS Stratum" is not activated, the LANTIME presents itself as Stratum 1 server in the network. If "Pass-through MRS Stratum" is active, the stratum of the external NTP server is considered. For example, if the external server is a Stratum 1 server, the MRS LANTIME would appear as Stratum 2 server in the network.

10.1.6.13 NTS Configuration

Information:

This option is not available on LANTIME systems with CPU module type "C05F1".

The NTS server mode requires an SSL certificate to be configured; see the chapters Optimizing Management Access Security and Certificates).



Enable NTS Server
This option enables the NTS server mode. In this mode, the LANTIME system will operate not only an NTP server but also an NTS key establishment server that provides NTS clients with cryptographic keys via a TLS-secured connection.

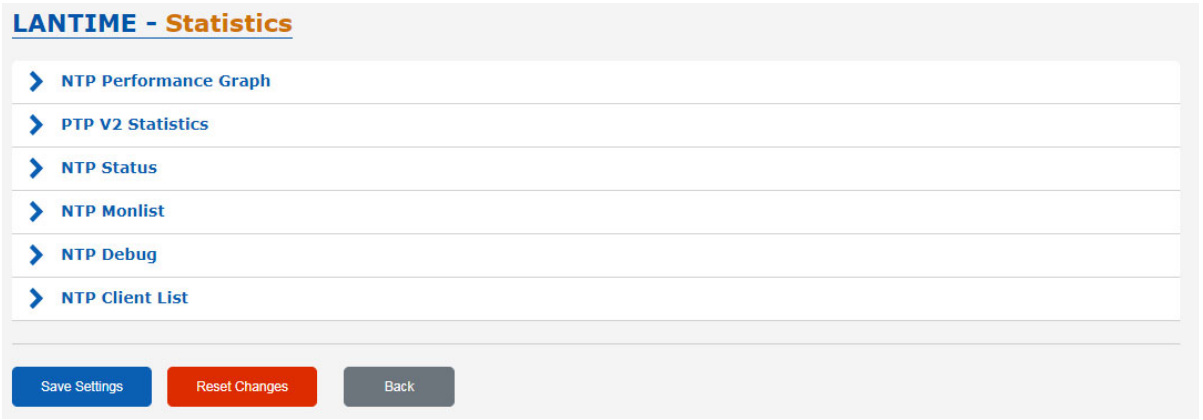
Because *NTPd* currently does not yet support NTS, all NTP requests in this case will be answered by a special, NTS-capable NTP server implementation. Autokey is not supported by this implementation.

Discard NTP Requests that are Not Protected by NTS
This option causes the NTS server to reject and ignore any NTP requests not secured by NTS. This option has no effect if the NTS server is not enabled.

Master Key Rotation Interval
This option determines the duration of validity of the internal, private master key used for the encryption of the NTS cookies. At this end of this period, the NTS server will generate a new key to be used from that point on. The oldest key will then be deleted.

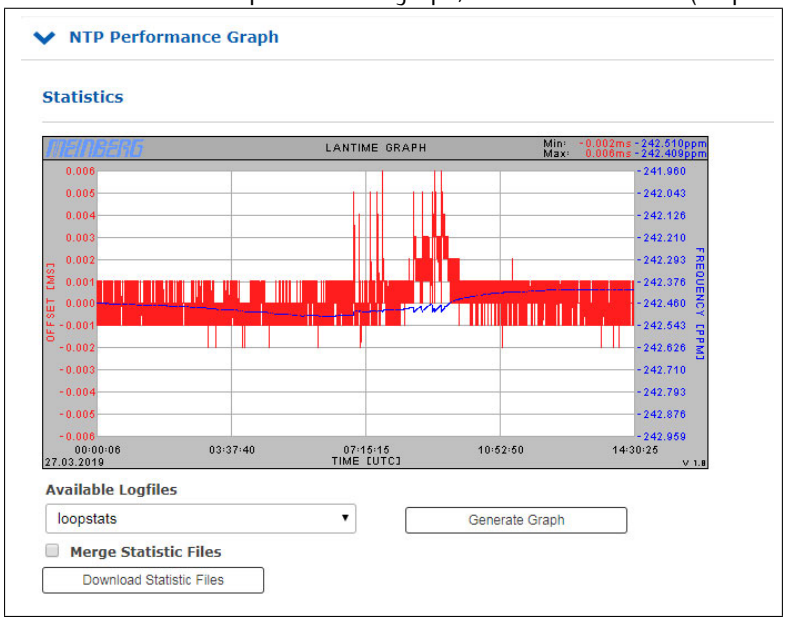
The NTS server stores up to three legacy keys to enable it to continue responding to requests from NTS clients using cookies from a previous rotation interval.

10.1.6.14 NTP Statistics



10.1.6.15 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.

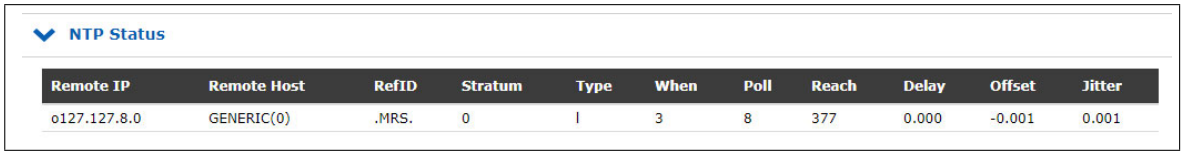
Available Log Files:
You can select the available log data via the dropdown menu. The ntpd creates a new loopstats file for each day.

Merge Statistic Files:
After activating the checkbox and clicking on "Generate Graph", all available log files are merged and displayed as one graph.

10.1.6.16 NTP Status

This menu lists the current states of all reference time sources (peers) available to the NTP service. For integrated reference clocks as well as normal external NTPv4 servers, this corresponds to the output of the command *"ntpq -p"*. For external NTS servers, this display also includes status information from a Chrony time service, in which case there may be minor differences in how the information is displayed.

The following example shows the NTP status output of a LANTIME with an integrated GNSS reference clock and two external NTP time servers configured:


NTP Status

Remote IP	Remote Host	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
o127.127.8.0	GENERIC(0)	.MRS.	0	l	3	8	377	0.000	-0.001	0.001

Remote IP:
IP address of the NTP peer. Alternatively, if it is a hardware time reference (e.g., a radio clock or a GPS receiver), this will show 127.127.x.x.

Codes may be displayed alongside each of the NTP peer IP addresses. These have the following meanings:

'*'	This server has been selected for synchronization.
'o'	The system is synchronized on the basis of 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 is not suitable for synchronization.
'#'	The server is a survivor, but not among the first six servers.
' '	The peer is rejected due to being unreachable or is itself synchronized by this server (sync loop).

Remote Host:
The resolved DNS name of the NTP peer or, for NTS servers, the address of the associated NTS-KE server.

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
c:	NTS server

When:
Value in seconds. Indicates when the NTP peer was last queried.

Poll:
Interval in seconds. Specifies the time between queries to the NTP peer.

Reach:
Octal value. Indicates the status of the last 8 queries. The value *"377"* (binary value *11111111*) means that the last eight queries were successful.

Delay:
Value in ms. Displays the transmission time of the NTP packet.

Offset:
The NTP software compares its own system time with its reference time sources at regular intervals, a process that is referred to as "polling". After each polling operation, the packet round trip time is determined, calculated, and the current time difference ("offset") is calculated and displayed in milliseconds.

Jitter:
The packet round trip time will vary depending on network conditions when "polling" external NTP sources upon each time comparison, and so the calculated time offset will also vary. Because of this, the results of multiple successive time comparisons are filtered by calculating weighted mean values for packet transmission time and time offset. Variations in the individual values relative to these mean values are referred to as "jitter"; the higher the jitter value, the less accurate the calculated time offset is likely to be. On the other hand, if the mean time offset gradually rises, this is indicative of the system time drifting away from the reference time. The value is displayed in milliseconds.

10.1.6.17 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
https://www.ntp.org/documentation/4.2.8-series/ntpq/

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

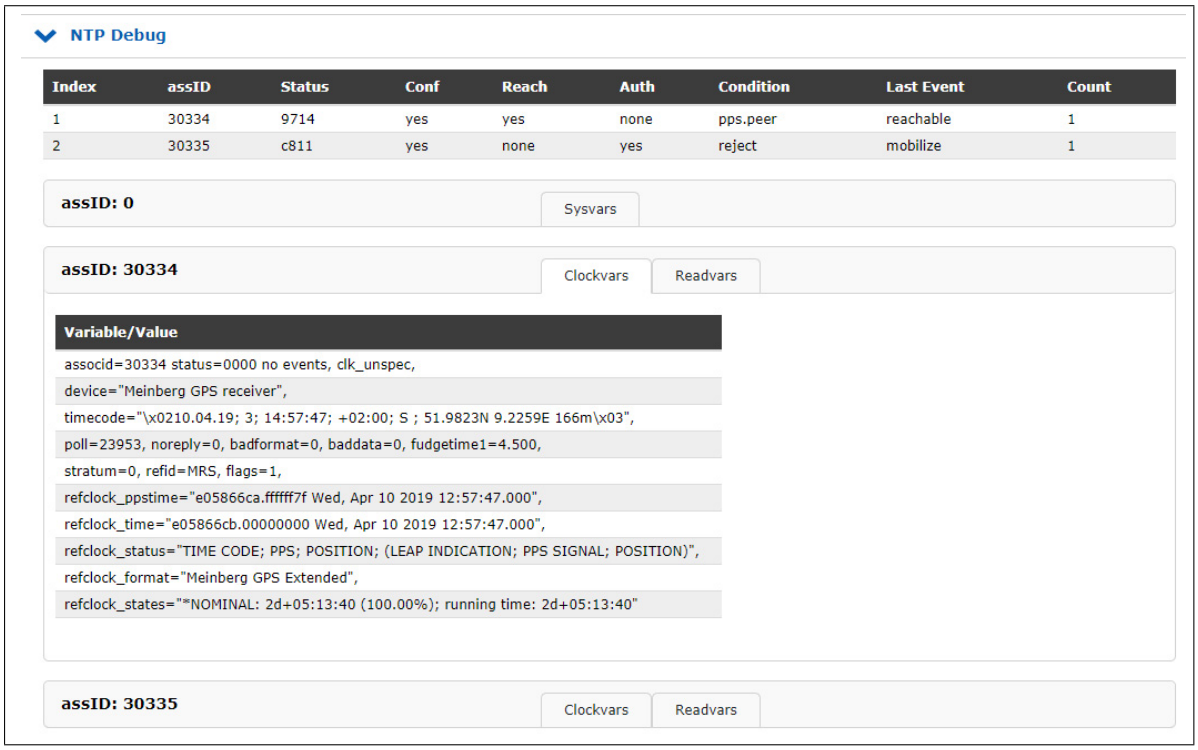
V:
NTP Version

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

10.1.6.18 NTP Debug



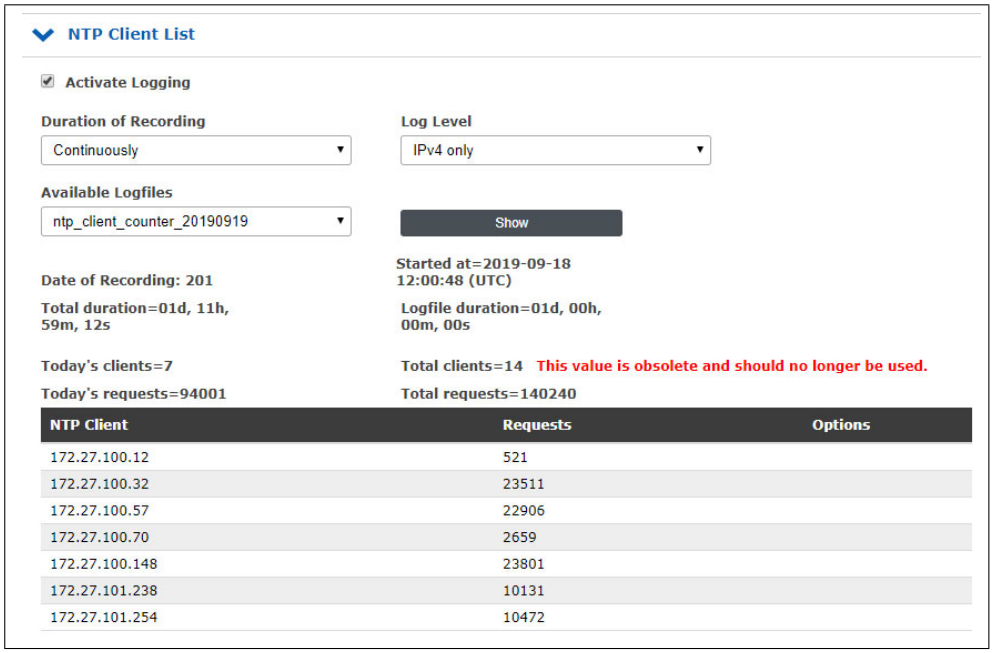
The NTP Debug submenu displays NTP debug information queried by the LANTIME using the NTP Query Tool (ntpq). The "ntpq" is executed with the following parameters:

- "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

10.1.6.19 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.



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.

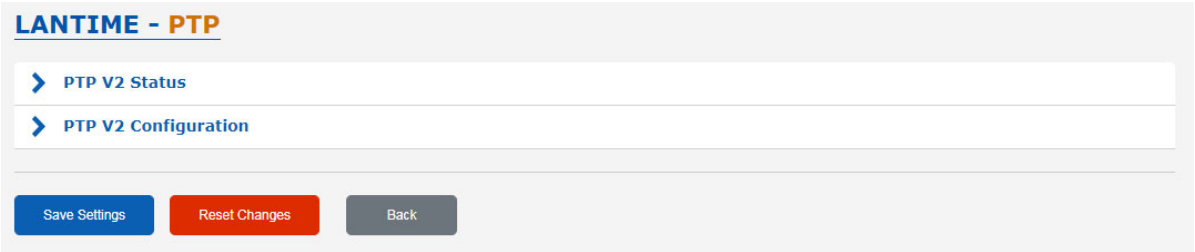
Available Log Files:
If the client logging is activated, log files for display are provided at this point. Select the desired daily statistics from the selection box and use the "Show" button to display the statistics. You will then receive a list of clients as well as other statistics.

NTP Client	Anfragen	Optionen
172.16.100.172	1214	Details
172.27.101.162	569	Details

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

10.1.7 PTP



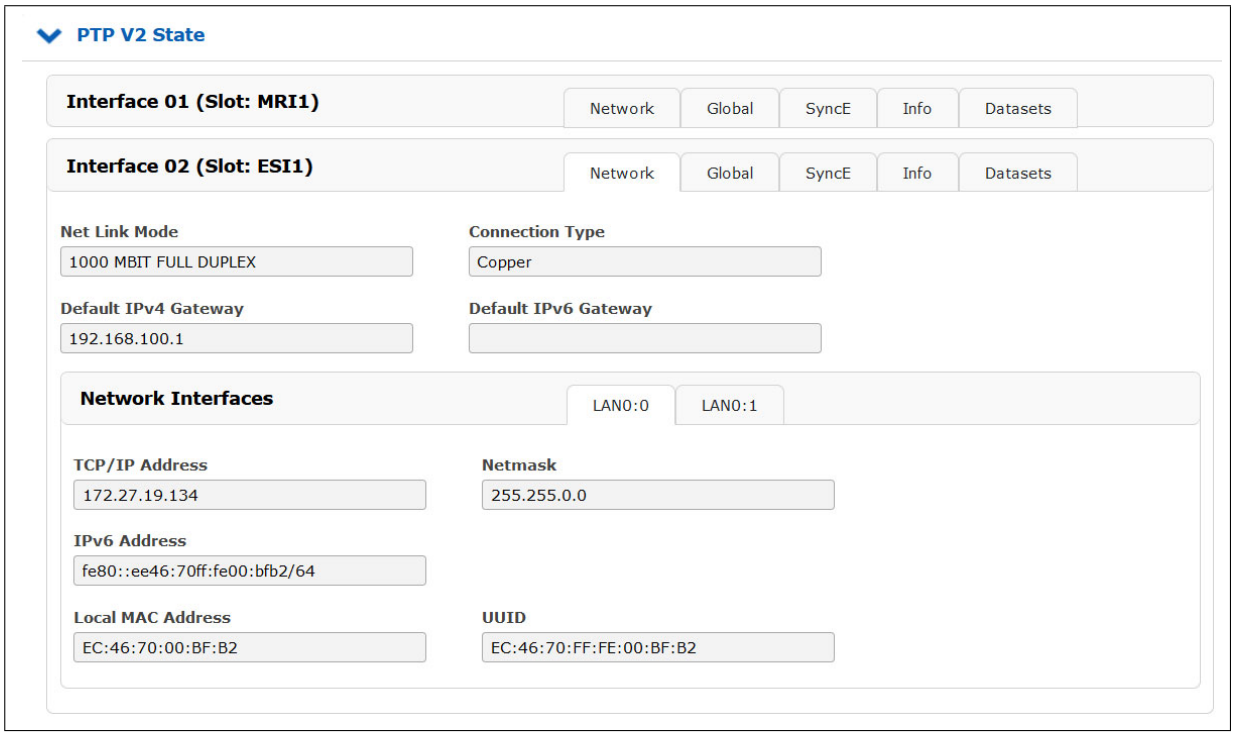
All parameters for proper PTP functionality can be configured in a clear and user friendly Web GUI. The set of parameters which can be configured in the Web GUI corresponds to the PTP card version currently installed in the system. Some features are available with TSU-GbE cards and above only and these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

- PTP Status
- PTP 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.

10.1.7.1 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.

10.1.7.2 PTP Network Status

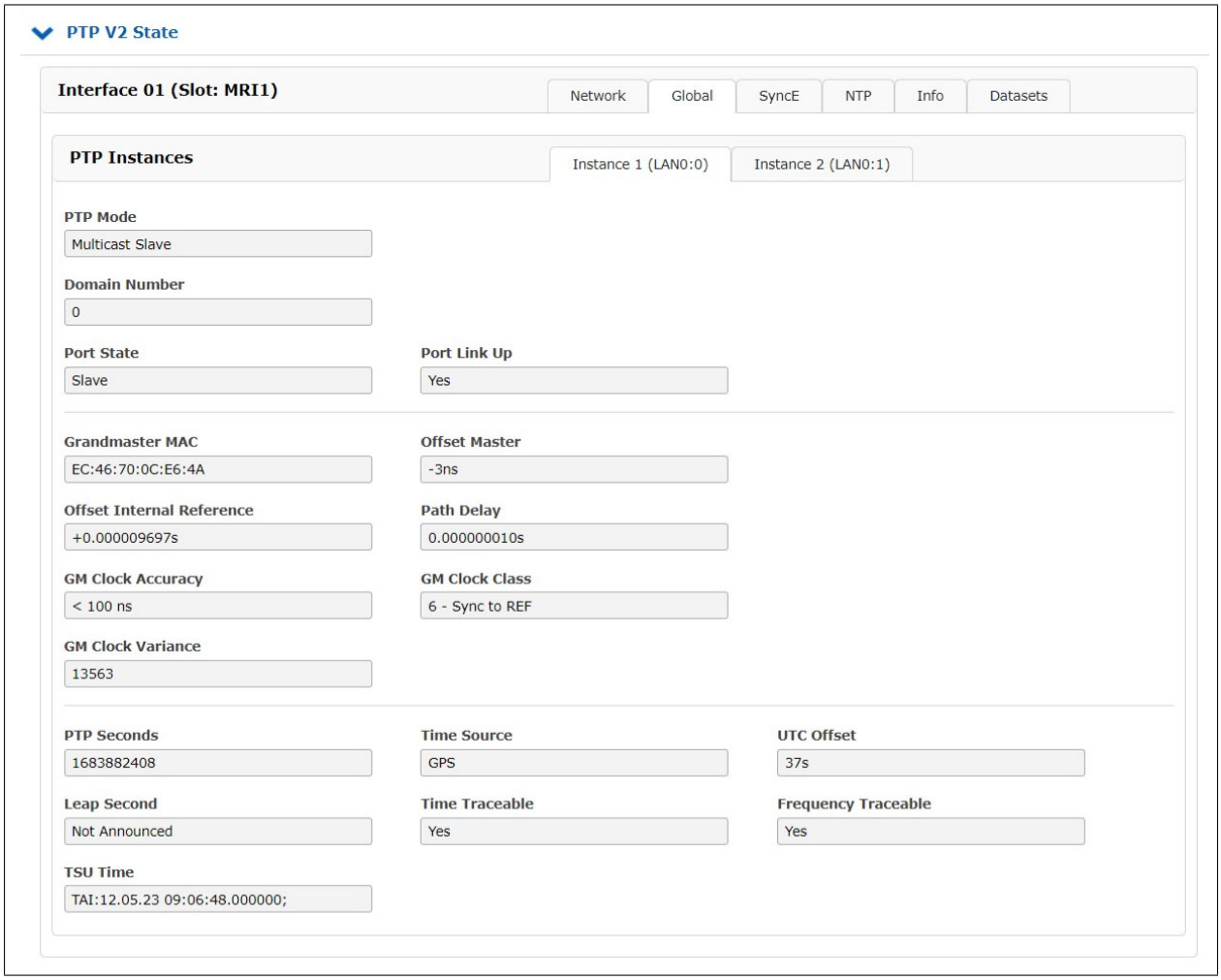
In the Network tab you can check if network settings of the PTP card are valid.

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.

10.1.7.3 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.



Port States

Uninitialized The PTP module 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.

Stopped 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.

Disabled Not defined in LANTIME systems.

Listening The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.

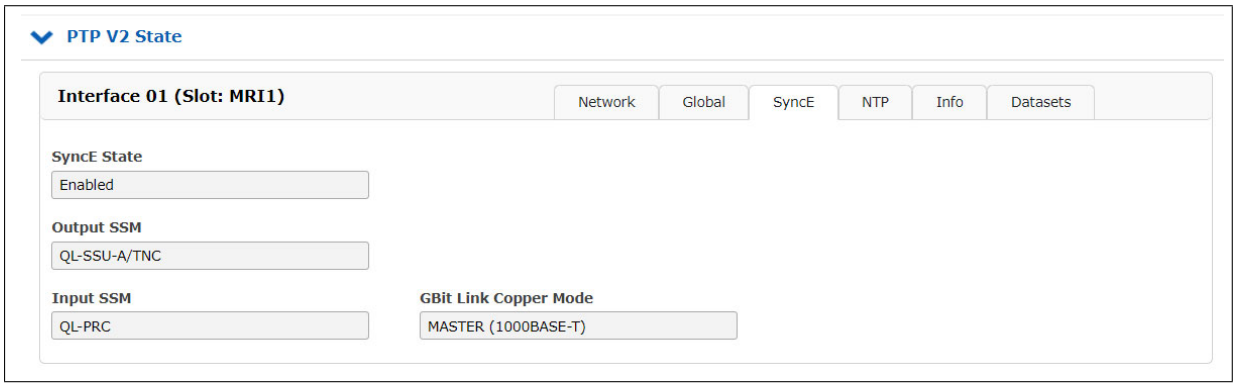
preMaster A short transitional state while the port is becoming a master.

Master The port is a current master.

Passive The port is in passive mode, meaning there is another master clock active in the PTP

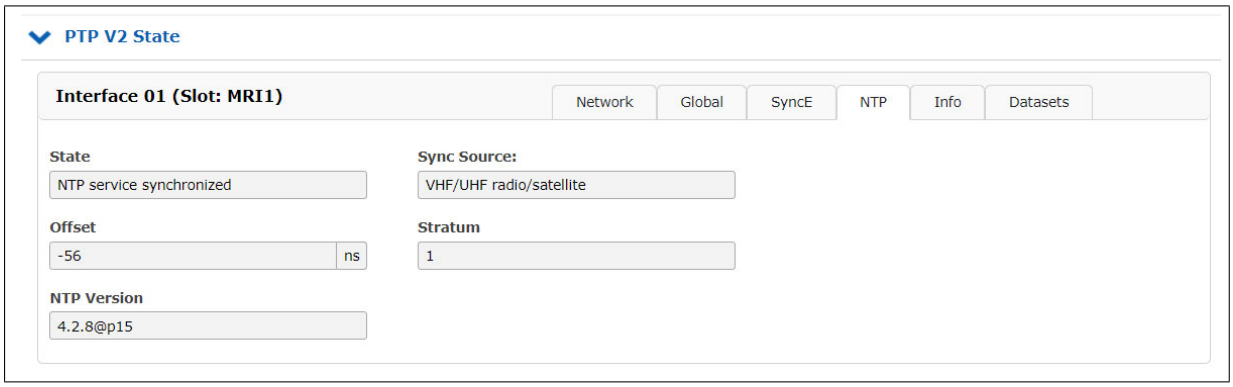
	domain. The port can enter master state when it wins the BMCA (Best Master Clock Algorithm) due to a failure/service degradation of the current master.
Uncalibrated	The port wants to become a slave in the PTP domain and has already detected a suitable grandmaster. The TSU is waiting to calculate the path delay to a Grandmaster.
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.
Grandmaster MAC	The MAC Address of the current Grandmaster.
Clock Accuracy	The clock accuracy of the active grandmaster. This value is used in the Best Master Clock Algorithm to select the best master.
PTP Seconds	Current value of the raw PTP seconds value (seconds since 1970).
UTC Offset	This value represent the current Offset to the PTP time based on TAI to calculate UTC.
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.
Port Link up	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.
Delay Asymmetry	If a static asymmetry offset in the network is known, this value may be entered (in ns) to compensate it before the PTP start.
Clock Class	PTP Clock class of the currently selected PTP grandmaster. This value is used in the Best Master Clock Algorithm.
Time Source	The type of a time source as used by the Grandmaster (informative only).
Leap Second	Leap second announcement flag, set up to 24 hours prior the leap second event, depending on the GM implementation.
TSU Time	Displayed time of day in the selected PTP timescale.

10.1.7.4 SyncE Status



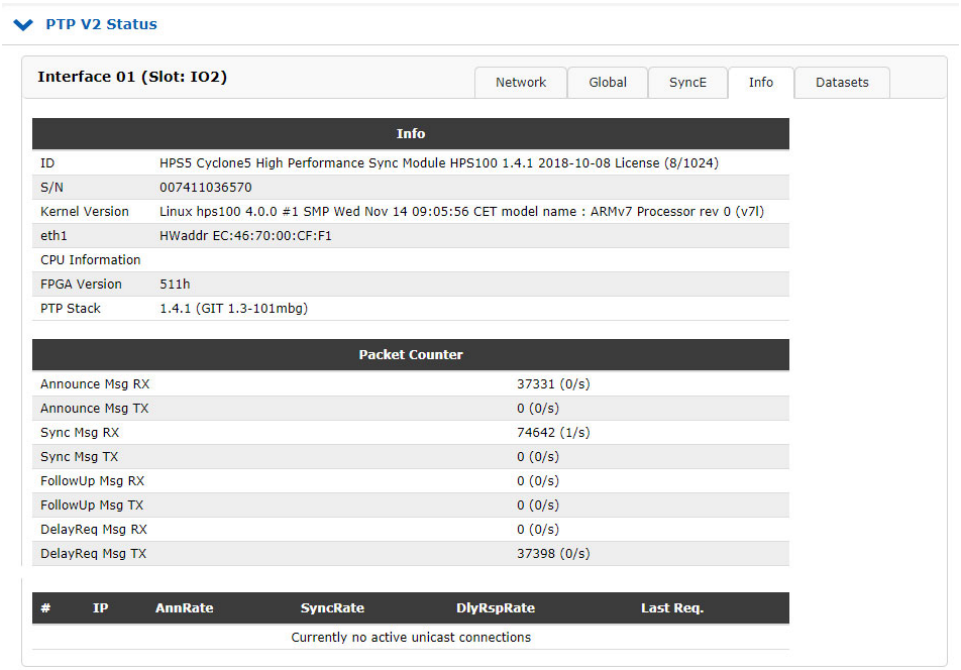
You can check if SyncE functionality is activated on the card or not (if supported by the PTP module).

10.1.7.5 Status NTP



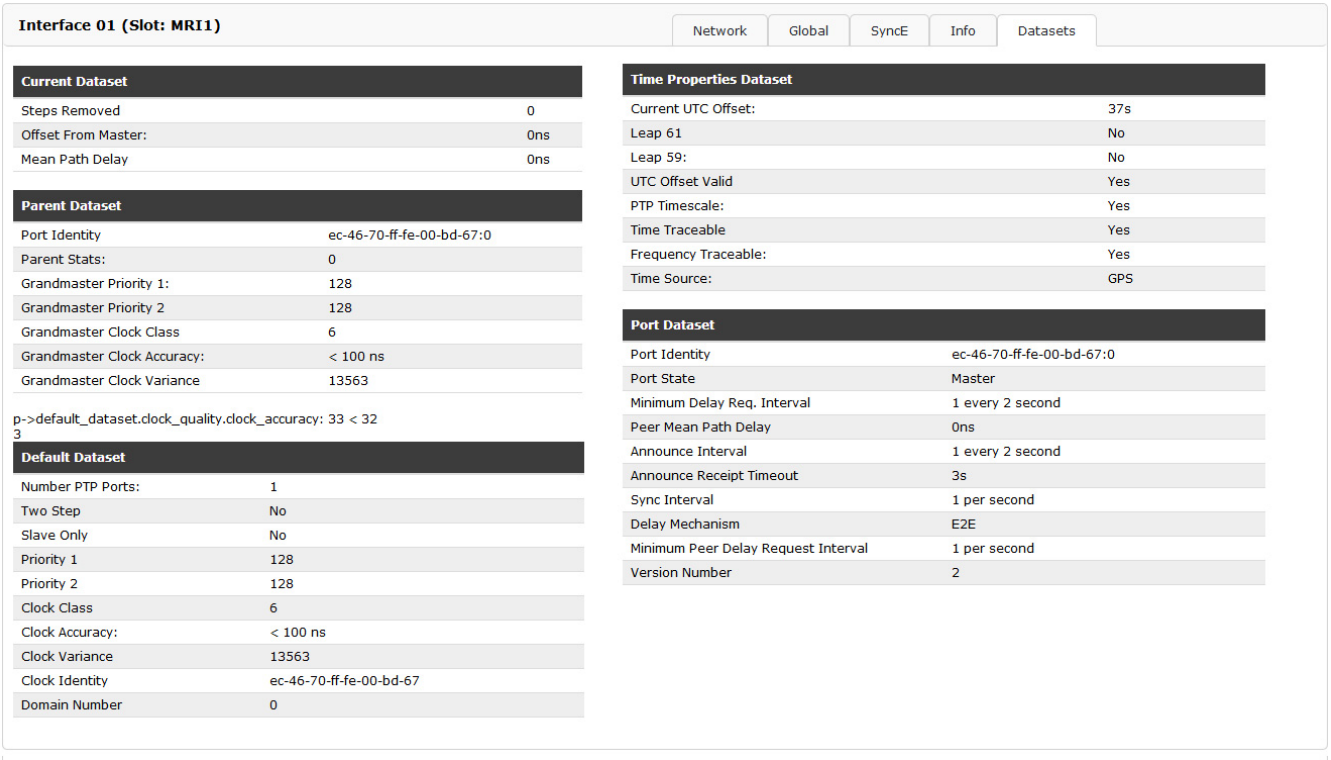
The "NTP" tab is only visible if the **Software NTP service** was previously activated in the "PTP V2 Configuration" menu. Here the values for Status (synchronized or not-synchronized), Sync Source (e.g. the integrated receiver), NTP offset from the reference receiver (in nanoseconds), the stratum value of the time server and the NTP version used are displayed.

10.1.7.6 Menu PTP Status Info



Under this menu item you will find information about the used PTP module, about the packets sent and received (Packet Counter) as well as information about active unicast connections.

10.1.7.7 Menu PTP Status Datasets



Clock Variance:
This a log scaled statistic which represents the jitter and wander of the clocks oscillator over a Sync message interval.

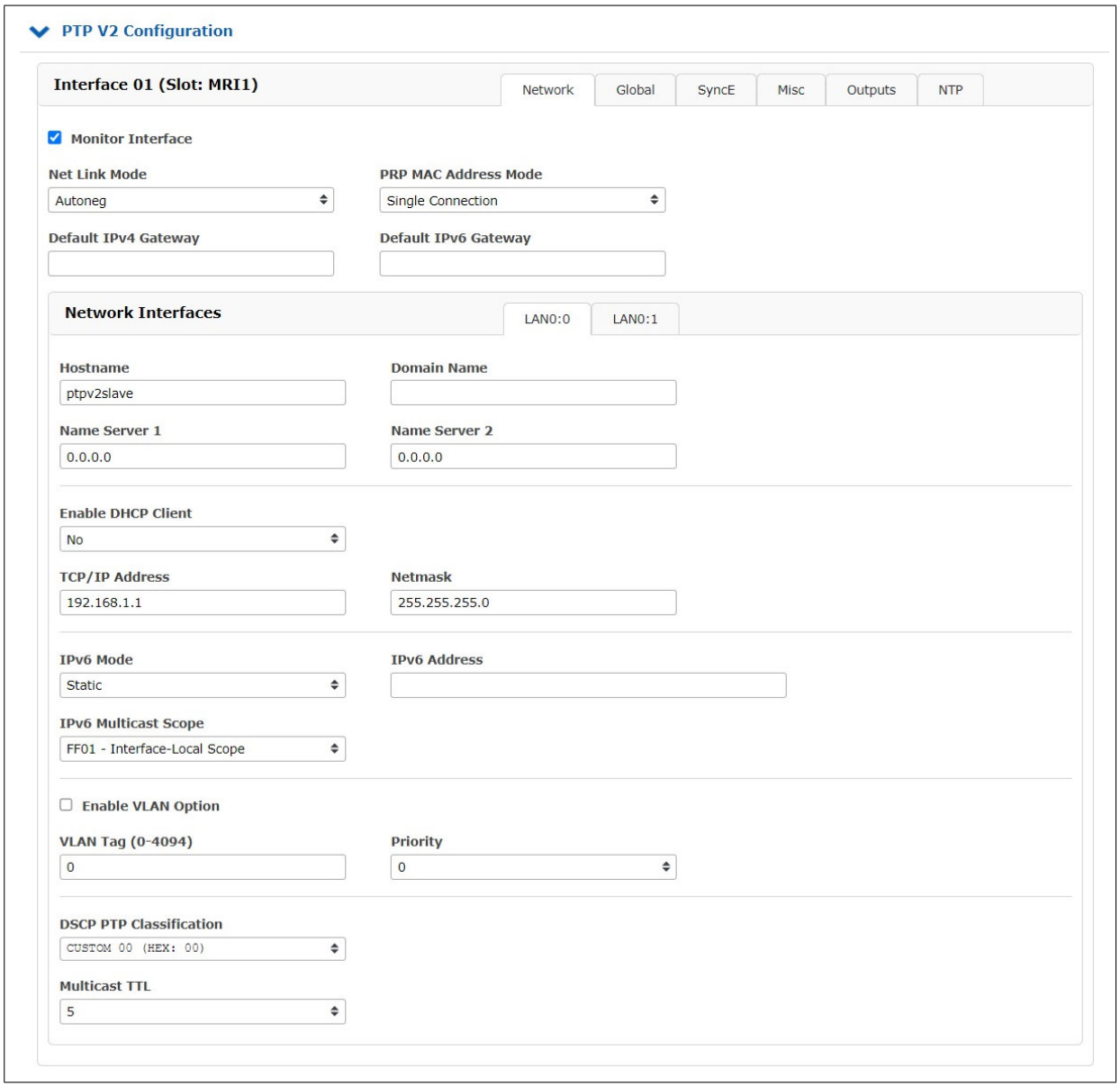
10.1.7.8 PTP Configuration Menu

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 on HPS100 or TSU-GbE modules only (the tabs marked with ** only on HPS100).

- Network
- Global
- SyncE*
- Misc*
- Outputs*
- NTP** (Software NTP Service)

10.1.7.9 PTP Network Configuration



Monitor Interface

Monitors the link state of the network port. A "PTP Link Down" event is triggered as soon as the selected PTP network interface ceases to detect a link. These events are documented in the menu "Notification → Notification Events".

If the PTP module is no longer required and is therefore not connected to the network, the "Monitor Interface" checkbox can be unchecked to deactivate it. Once deactivated, these error events will no longer be logged.

NET Link Mode

The following values are available:
Autonegotiation
100 MBIT HALF DUPLEX
100 MBIT FULL DUPLEX
1000 MBIT HALF DUPLEX
1000 MBIT FULL DUPLEX

PRP MAC Address Mode

PRP is a network redundancy protocol that is used to safeguard the availability of a network. PRP is implemented in the form of two independent network paths for the transmission of data packets, providing a redundant transmission path for data packets even if the other path fails for any reason.

A LANTIME system with two or more PTP interfaces can operate as a DAN ("Dual Attached Node")—a device connected to two independent networks.

PRP groups can be created using the menu "PTP → PTP V2 Configuration → Network". Select the same PRP group in the drop-down menu "PRP MAC Address Mode" for at least two interfaces.

Note:
A PRP group requires at least two PTP modules (HPS100) accordingly.

Hostname

A hostname—a unique alphanumeric label that allows the selected PTP port to be uniquely identified in a network—can be entered here.

Domain Name

The domain name for the selected PTP interface can be assigned here.

Name Server 1

This can be used to enter the first name server, if one is used in the network.

Name Server 2

This can be used to enter a second name server if a redundant name server is used in the network.

Enable DHCP Client

Enables or disables the DHCP service. If the DHCP client is enabled, the field for the static IP configuration will be disabled. The static IP configuration field will conversely be enabled if the DHCP client is disabled.

IP Address from DHCP

If a DHCP server has been found in the network, a valid IP address will be automatically assigned to a PTP port and displayed here.

Netmask from DHCP

If a DHCP server has been found in the network, a valid netmask will be automatically assigned to a PTP port.

Gateway from DHCP

If a DHCP server has been found in the network, a valid gateway will be automatically assigned to a PTP port.

TCP/IP Address

If the DHCP client is disabled, this field can be edited to define a valid static IP address for the selected PTP interface.

Netmask

If the DHCP client is disabled, this field can be edited to define a valid netmask for the selected PTP interface.

Default Gateway

If the DHCP client is disabled, this field can be edited to set a Default Gateway for the selected PTP interface.

IPv6 Mode

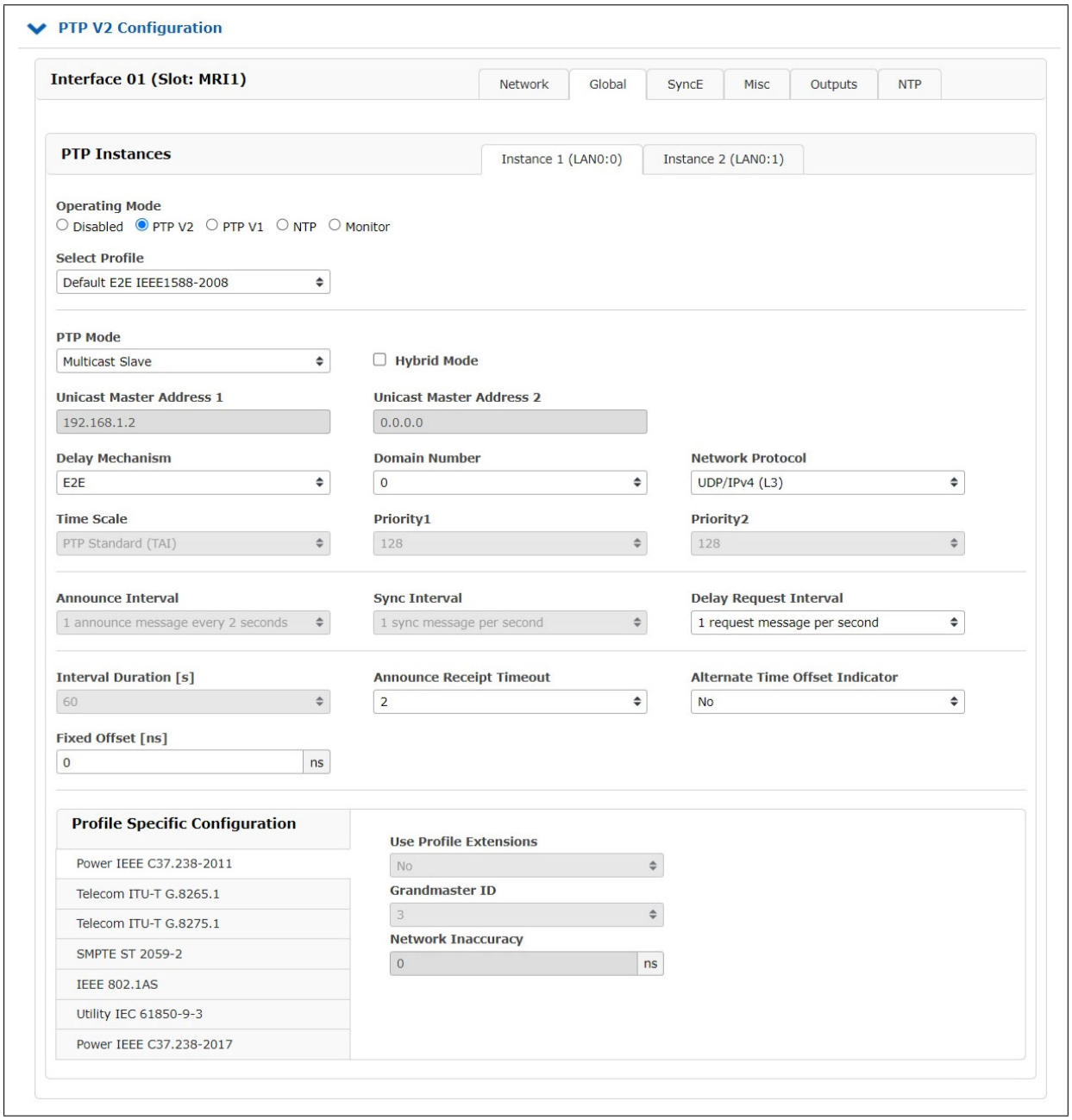
Enables IPv6 addressing via DHCPv6 / router advertisement or allows a static IPv6 address to be set.

IPv6 Address

IPv6 address assigned to the selected PTP port. If the option "Static" is enabled

	for IPv6 mode, this field can be used to define a valid static IP address.
IPv6 Multicast Scope	The prefix of an IPv6 multicast address determines the multicast scope. This field can be used to define the scope for IPv6 multicast.
Enable VLAN Function	Enables/disables the Virtual LAN (IEEE 802.1Q) service on the PTP interface.
VLAN Tag (1–4094)	A 12-bit value that specifies the VLAN ID to which the PTP port is assigned.
Priority	A value from 0 (default, lowest priority) to 7 (highest priority) that allows network traffic for various data types to be prioritized.
Disable SSH Service	If checked, this option disables SSH access for this PTP port. This option is only available with a TSU-GbE module.
DCSP PTP Classification	Differentiated Services Code Point. This is a QoS parameter integrated into the IP header of the classified PTP packet for the purpose of traffic prioritization.
Multicast TTL	Time-To-Live. By default, PTP multicast traffic is not routed and the PTP standard establishes this value to be "1". However, this field can be used to customize the TTL configuration to a value other than the default standard.

10.1.7.10 PTP Global Configuration



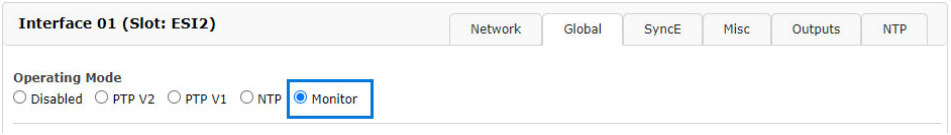
Operating Mode

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)



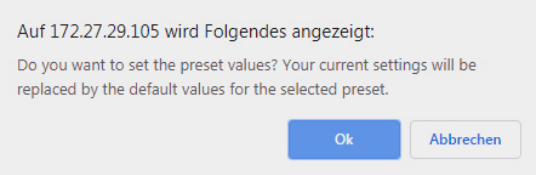
To monitor PTP network elements and generate statistics, a HPS100 can operate in monitor mode. Only if this mode is activated, it is possible to monitor PTP-nodes in the network via the HPS100.

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:

Please note: When you switch to another profile, your current settings are overwritten with the default values of the selected profile.



Example: When selecting the Telecom ITU-T G.8275.1 profile, SyncE is automatically activated and the GBit Link Copper mode in the the tab **SyncE** is set to "Automatic".

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)“
- 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-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.

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.

Network Protocol:
Three options for network protocol are possible:
ETH-IEEE 802.3 / Ethernet (Layer 2): Ethernet frames including MAC addresses of a slave and master.
UDP/IPv4 or UDP/IPv6 (Layer 3): User Data Protocol one of the main protocols used for the Internet.

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.

Arbitrary:
If "Arbitrary" is selected, the time sent over PTP will be UTC and not TAI. Consequently, the timestamps in the PTP messages will also be based on UTC instead of TAI. Also, the UTC_OFFSET field in the announce messages will be changed from 37 (current number of leap seconds as of 12/2021) to 0.

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, clock-Accuracy 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.

Interval Duration [s]:
Requested duration until timeout / renewal.

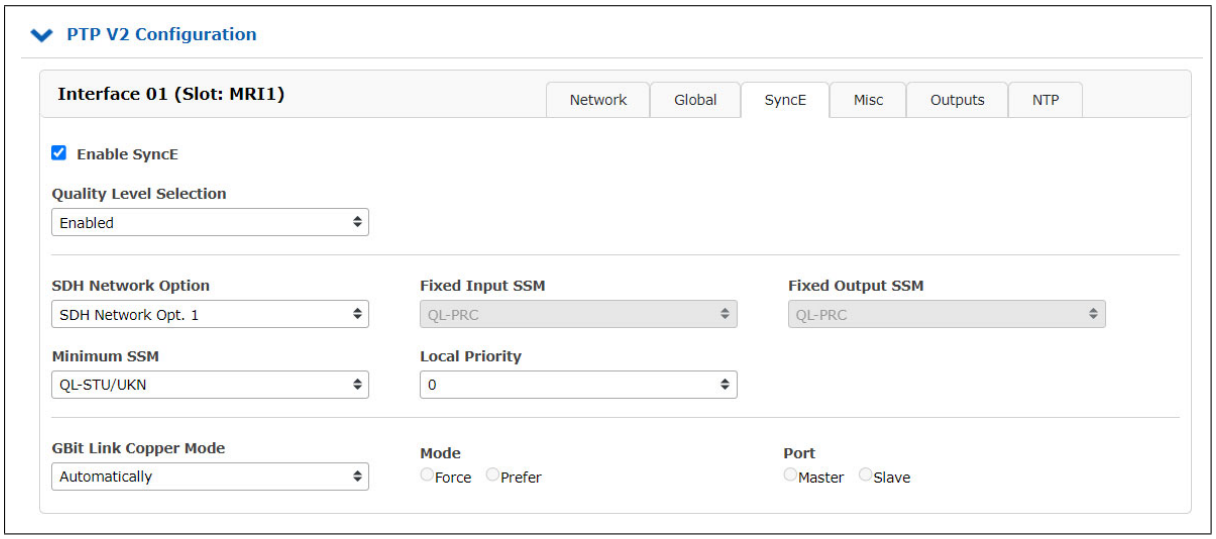
Announce Receipt Timeout:
Specifies the rate for announce receipt timeout messages which is generally 2-10 times the Announce Interval rate, with a default value of 3. In this time the BMCA procedure should select the current Grandmaster.

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.

Profile specific Settings
Only if the custom profile has been selected can this option be used. It is possible here to select profile-specific parameters simply for your own "custom profile". To do this, the "Use Profile Extensions" select field must first be set to **Yes**.

Grandmaster ID
In Power Profile C37.238-2011, a 1-byte ID must be assigned to the Grandmaster. Choose an ID between 3 and 254.

10.1.7.11 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 mode 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. Missconfiguration 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.

10.1.7.12 Misc. Configuration

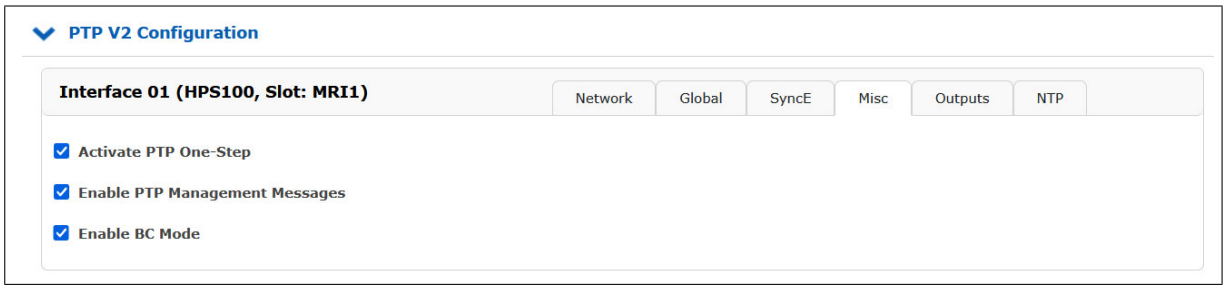


Figure: PTP Configuration - Misc. with HPS100 module and performance level A or B

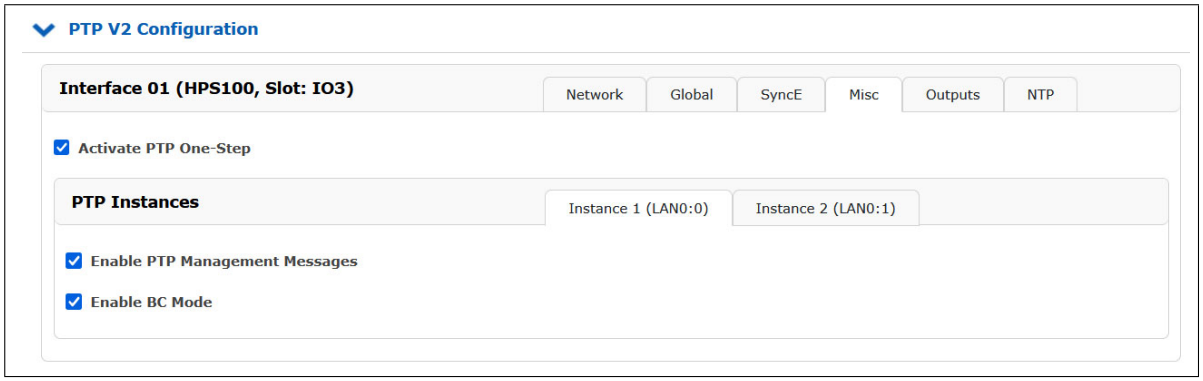


Figure: PTP Configuration - Misc. with HPS100 module: Dual PTP stack, performance level C, D or E

Activate PTP One Step:
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: Where two-step mode employs a Sync and Follow-Up message to account for processing latency in message generation, one-step operation uses the accurate timestamp generated in the Sync message and omits the Follow-Up message.

Enable PTP Management Messages
If this checkbox is enabled, PTP management messages will be sent to other PTP clocks. Management messages are requests sent to other clocks in the network to provide information about themselves.

BC Mode
This setting is intended for IMS systems operating as boundary clocks with multiple PTP instances.

If *enabled*, this HPS100 module will transfer its parent dataset to any other PTP clocks on the system operating as Masters. This allows any downstream Slave clocks to identify the upstream top-level grandmaster of the wider PTP network with its clock ID, clock class, etc.

If *disabled*, this HPS100 module will transfer its own clock ID, clock class, etc. to slave clocks, identifying itself as the grandmaster of the PTP network.

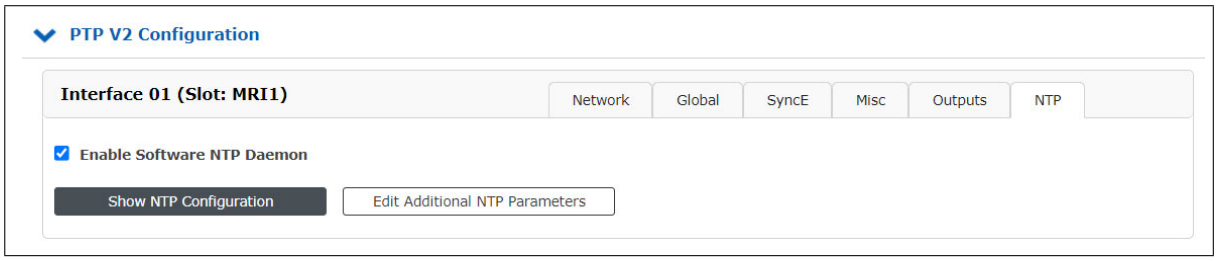
10.1.7.13 Option: Output Configuration

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

- PPS (generated locally on the TSU)
- 10 MHz (generated locally on the TSU)
- 2048 kHz (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.

10.1.7.14 Configuration NTP



Software NTP Daemon
This feature is only supported by PTP modules of type HPS100 with HPS firmware version ≥ 1.4.1. The type and firmware version of a built-in PTP module can be checked under "PTP → PTPv2 Status → Info".

Enable Software NTP Daemon:
If activated, a Software NTP Daemon *"**ntpd**"* is also started on the PTP module. This service works in the same way as the NTP software service on the LAN-CPU and can be parameterized accordingly. The Software NTP Daemon can be used in parallel with all other operating modes of the PTP module that can be set in the "Global" tab. Symmetric keys configured on the main system under "NTP → NTP Symmetric Keys" are automatically included in the NTP configuration of the PTP module. If the PTP module has been configured as an NTP server in the "Global" tab, all NTP requests without symmetric key authentication will continue to be answered by the hardware NTP responder of the PTP module. NTP requests with symmetric key authentication are answered by the Software NTP Daemon.

Display NTP configuration:
This button can be used to display the current NTP configuration. The initial configuration is generated automatically when the Software NTP Daemon is activated.

Editing Additional NTP Parameters:
This button can be used to configure additional NTP parameters, such as Restrictions or Trusted Keys. The syntax must follow the standard configuration syntax of the *ntpd*. After saving, configured lines are automatically appended to the NTP configuration generated by the PTP module.

10.1.7.15 PTP Dual Stack Mode

Starting with HPS100 firmware version 2.0.3 with PL-C as the minimum performance level, two independent PTP instances per port can be configured. The LANTIME firmware 7.04 supports the configuration of these two PTP instances and can display the status of the two PTP instances separately.

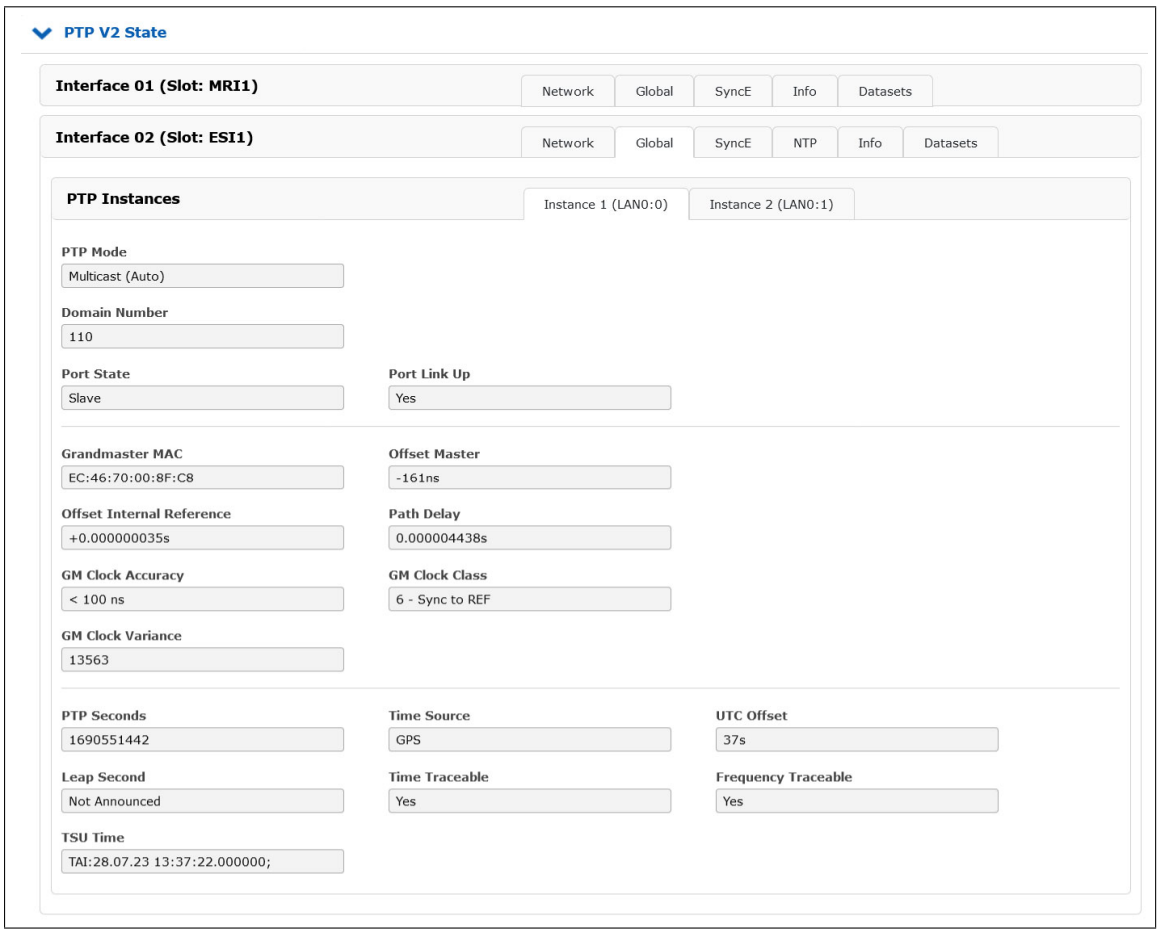
For example on one PTP card, two PTP Grandmaster instances can be started for both IPv4 and IPv6 mode or for Layer 2 and Layer 3 operation in parallel.

If a PTP slave instance is configured then a second instance is not possible. More constraints on possible configuration options can be found below.

Performance Notes
There are different client capacities available between the two PTP instances. The first instance (Instance 1) has the full capacity of PTP clients or DelayRequests per second as the Performance Level grade allows (ie: 1024 unicast clients with PL-D).

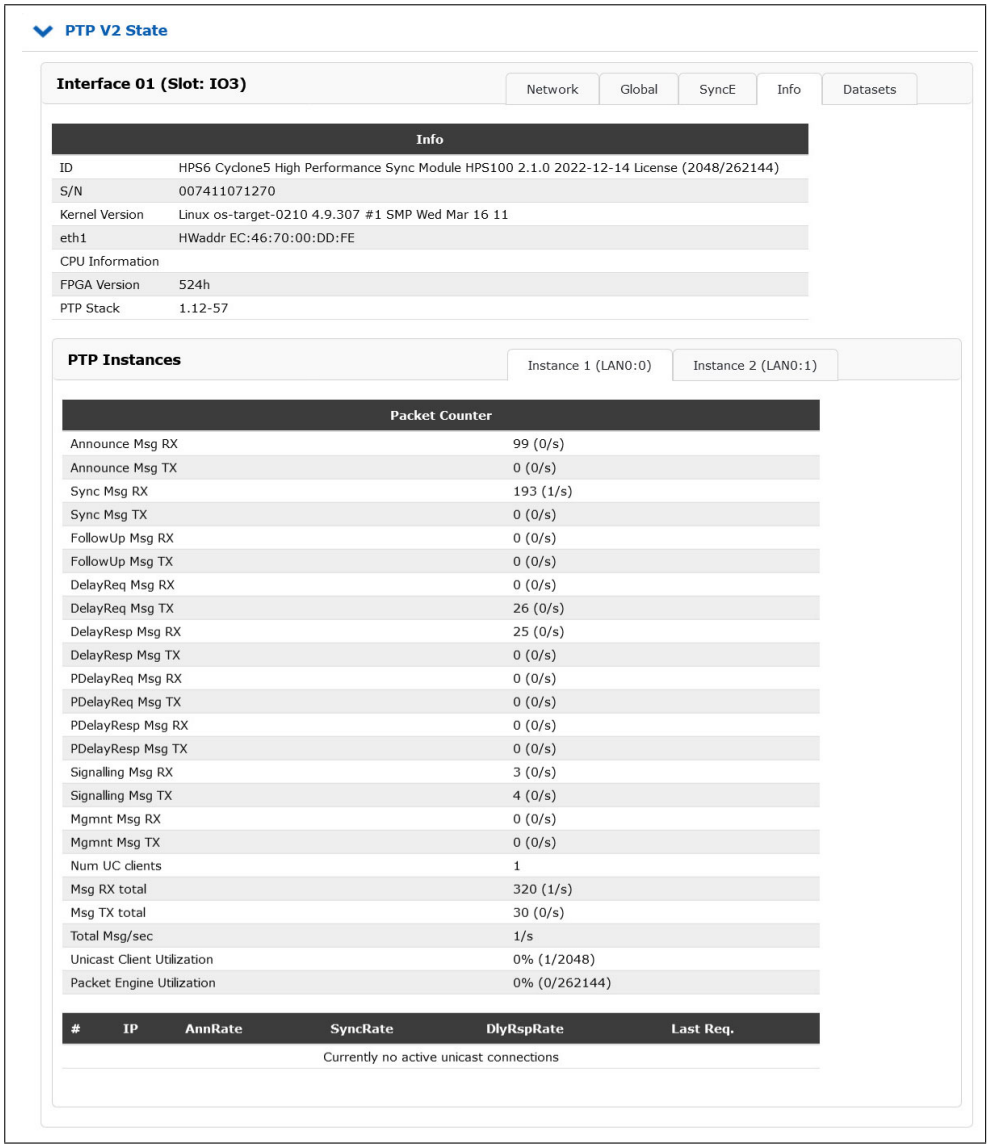
However, the second PTP instance that is running in parallel to the first one has the CPU power as the limiting factor. The total capacity of the PTP packet engine is approx. 15.000 PTP transactions per second.

Webinterface: PTP → Status → Global
In case the feature is provided by the HPS card, the Web UI shows the status of the two PTP instances on two independent tabs on the Network, Global, Info and Datasets page:

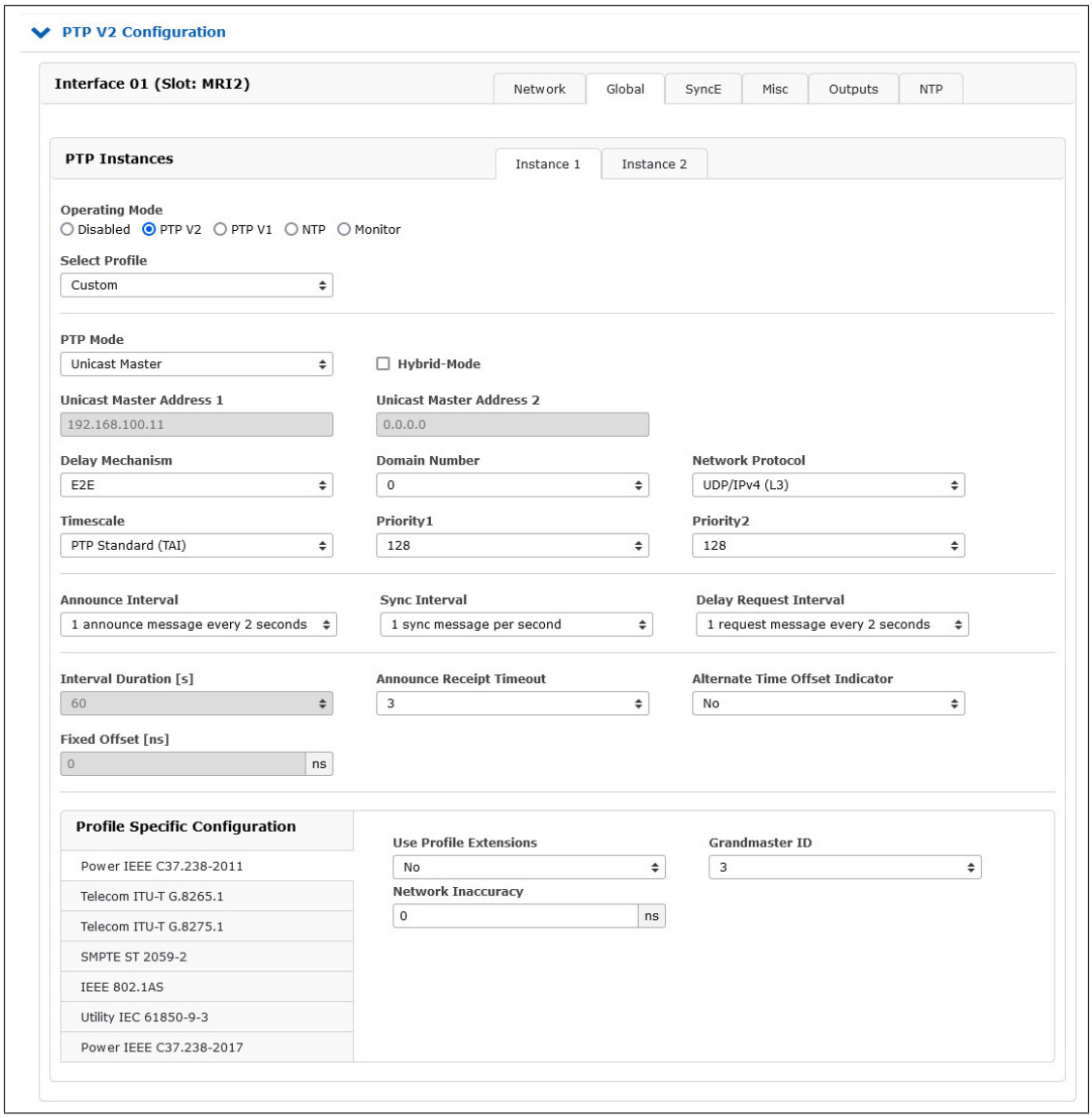


Webinterface: PTP → Status → Info

The PTP Packet Counter for both instances can be shown independently.



Webinterface: PTP → Configuration → Global
On the PTP Configuration page, the two instances of the PTP deamon can be configured independently, however, some constraints have to be kept in mind (see below).

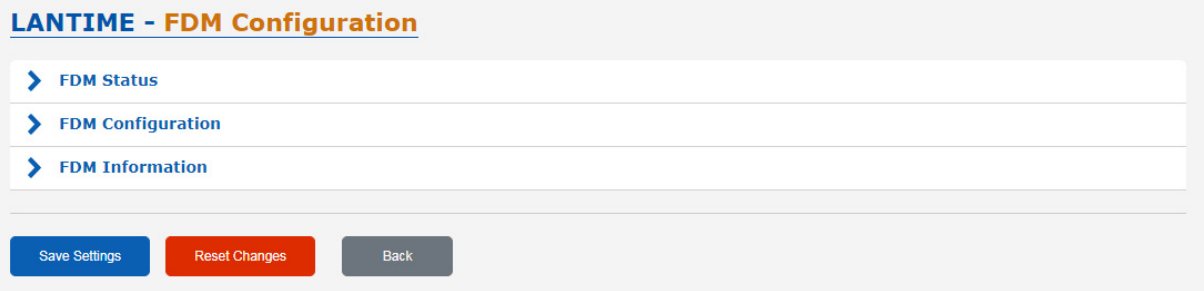


Constraints and rules when configuring a PTP card in Dual Stack Mode

(two active PTP instances)

- Both instances must be PTPv2 (as of HPS100 firmware 2.0.4, PTPv1 can be selected for Instance 1 and PTPv2 for Instance 2).
- Both instances must be Master Only.
- 1-step clock operation is mandatory for both instances (this setting is automatically deactivated when configuring PTPv1/PTPv2 mixed operation).
- The configuration parameters of the two PTP instances must differ at least for one of the following parameters:
  - Domain Number
  - Network protocol (L2 or L3)
  - VLAN tag enabled

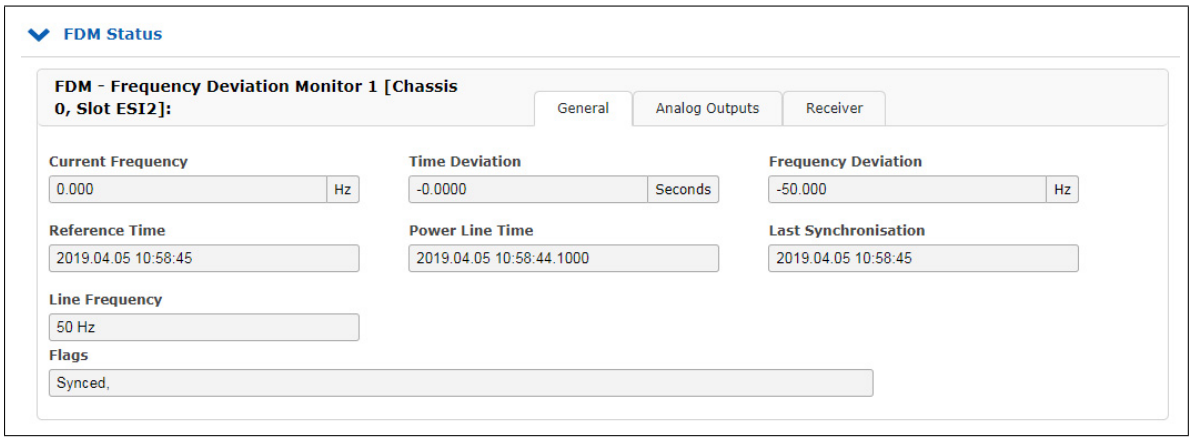
10.1.8 FDM - Frequency Deviation Monitoring



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.

10.1.8.1 FDM Status



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: 50 Hz or 60 Hz

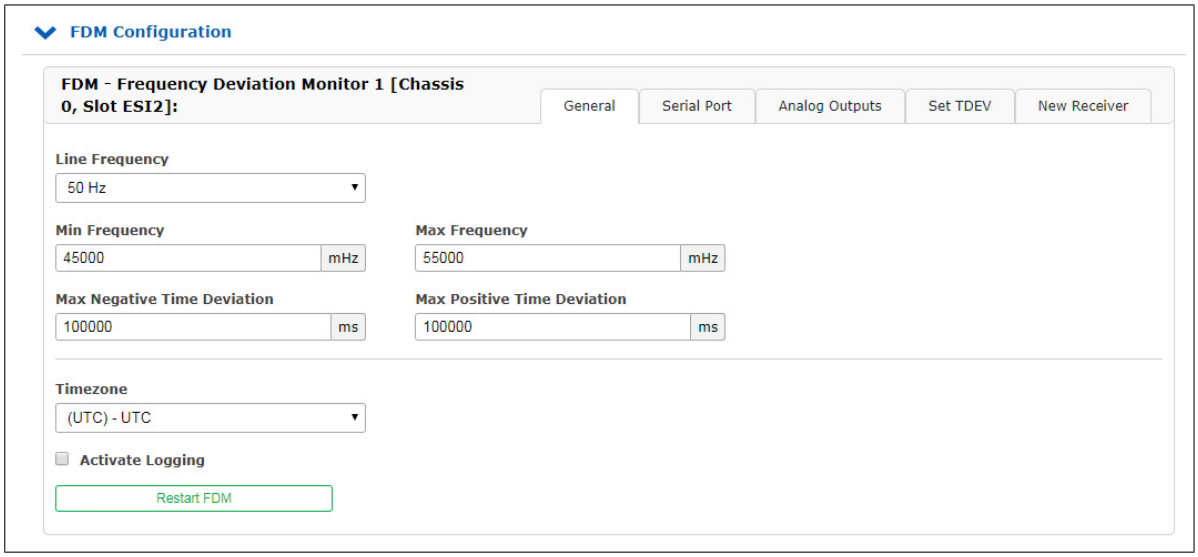
Flags: Transmitted Flags by FDM (Error Bits)

Receiver State

All receivers previously added in the FDM configuration are displayed in the TAB "Receiver".

10.1.8.2 FDM Configuration

Automatic Monitoring of Power Line Frequency
An upper and lower limit can be defined for the Power Line Frequency for the purpose of triggering alarm messages (by email, syslog, SNMP traps) whenever the LANTIME detects that the measured frequency is outside of an acceptable range.



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

Line Frequency: Establishes the rated frequency of the monitored power line.

Min Frequency: The lower threshold, specified in Millihertz, at which an alarm is triggered if the frequency drops below it.

Max Frequency: The upper threshold, specified in Millihertz, at which an alarm is triggered if the frequency exceeds it.

Max Negative Time Deviation: The lower threshold at which an alarm is triggered if the time deviation TDEV drops below this negative value in milliseconds.

Max Positive Time Deviation: The upper threshold at which an alarm is triggered if the time deviation TDEV exceeds this positive value in milliseconds.

Timezone: Local timezone used for Reference Time and Power Line Time.

Activate Logging: Enables logging for FDM in XtraStats.

Reset FDM: This is used to restart the FDM module only without having to manually remove the module or reboot your LANTIME.

Configuration of Serial Ports

Baud Rate: Specifies the transmission rate for serial time strings:
600, 1200, 2400, 4800, 9600, 19200

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

String Type: Type of generated serial time string:
Standard, Short, Areva (TTM1), TPC (TTM2),
Standard 2, Computime, Fingrid, FDM III

The Standard FDM string 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 (+-SS.mmm) (+-SSS.mmm if TDEV $\geq$ 99.999 ms)

Mode: Per second, per minute, or on request

Analog Outputs

The FDM180 provides two analog outputs (A1/A2), which are passed through a 3-pin MSTB connector, depending on the system. These outputs have a voltage range of -2.5V to + 2.5V, with 65,536 discrete values available in this range (16-bit resolution).

It is possible to select whether the displayed value should be the frequency deviation or the time deviation at each analog output.

Mode:

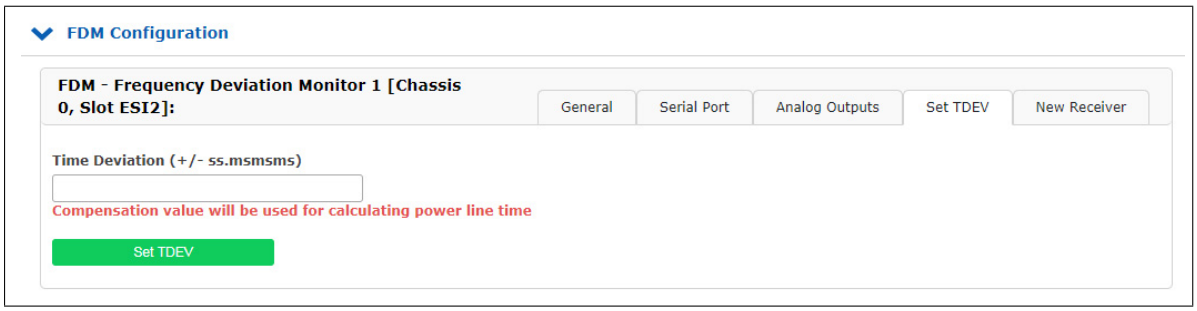
Time Deviation: The output voltage is governed by the minimum and maximum limits defined for the time deviation.

For example, if min = -100 s and max = +100 s, and the time deviation falls to -100 s, the analog output delivers a voltage of -2.5 V, while with a deviation of +100 s, the output provides +2.5 V with a DAC resolution of 16 bits.

Frequency Deviation: The output voltage is governed by the min and max limits defined for the frequency deviation.

For example, if min = 45 Hz and max = 55 Hz with a mains frequency of 50 Hz, and if the frequency deviates by 45 Hz, the analog output delivers a voltage of -2.5 V, while if the frequency deviates by 55 Hz, the output provides +2.5 V with a DAC resolution of 16 bits.

Submenu Set TDEV

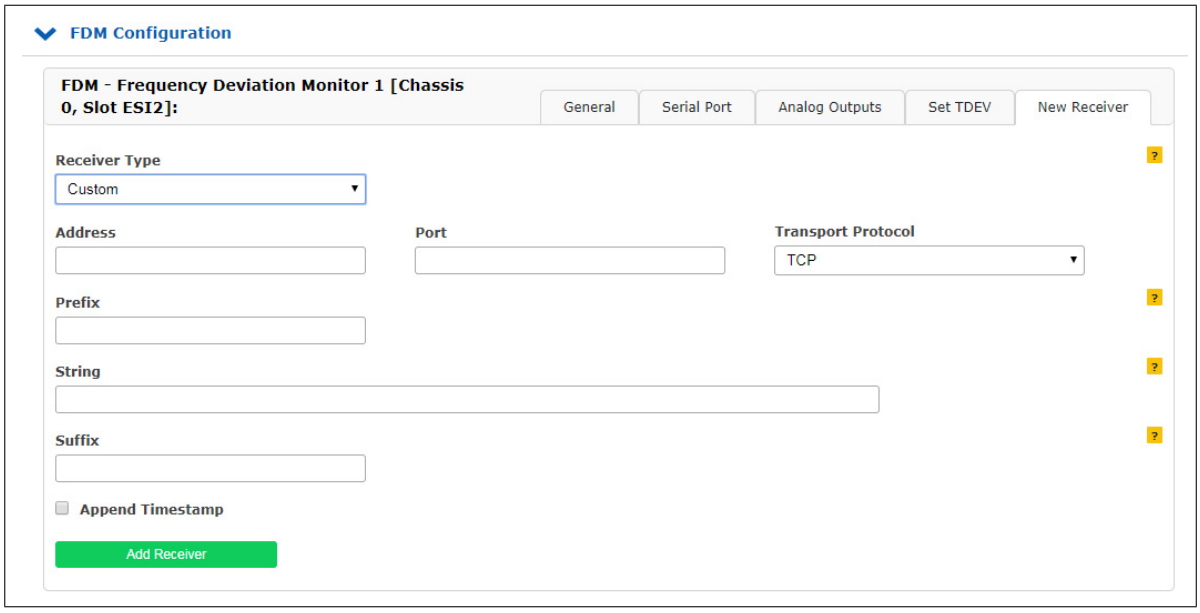


Time Deviation: A value can be entered into this field (with a preceding negative sign if necessary) to override the current time deviation value.

This field can also be used to reset the current TDEV to zero at any time by simply entering a value of 0 and clicking on **Set TDEV**.

The new or reset time deviation will be applied as soon as the FDM180 is synchronized and a voltage is detected by the module (or will be applied immediately if the FDM180 is already synchronized and a voltage is already present at the module input).

Submenu New Receiver



This section can be used to add a new receiver for FDM strings. It is possible to add an arbitrary number of receivers (network displays and/or PCs for analysis and display of status messages or frequencies) to be connected to the same network.

Receiver Type: String type for network transmission
Standard: Standard FDM time string
Sent once per second
e.g., "F:50.016 FD:+00.016 REF:15:17:57 PLT:15:17:57.056 TD:+00.056"

Extended: Extended FDM time string with interim measurements and sequence ID
Sent once per second
e.g., "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 string with intermediate measurements
Sent once every 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 string, comprising prefix, string, and suffix
Sent once per second

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

Port: TCP/UDP port used for string transmission

Transport Protocol: Protocol used for string transmission (TCP/UDP)

Only if receiver type "Custom" is selected:

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

String: Customized time string, which may consist of any text and the following variables (identified by the prefix '%'):

PLFRQ	Power Line Frequency (e.g., 50.023)
FRQDEV	Frequency Deviation (e.g., +00.023)
REFTIME	Reference Time (e.g., 15:17:23)
POWERLNTIME	Power Line Time (e.g., 15:17:22.550)
PLTDEV	Power Line Time Deviation (e.g., -00.450)
IDX	Intermediate Measurement Index (e.g., 1)
IMMFRQ1	Intermediate Measurement Frequency with Index 1 (e.g., 50.034)
IMMFRQ2	Intermediate Measurement Frequency with Index 2 (e.g., 50.034)
...	
SEQID	Sequence ID (e.g., 0000000061)
SYSTIME	System Time (e.g., 15:17:23)
SYNCSTATE	Synchronization Status (" " = synchronized, "*" = not synchronized)
SYNCTEXT	Synchronization Text ("OK" = synchronized, "NO" = not synchronized)
TIMESTAMP	Current Timestamp (e.g., 2016-03-15 16:03:10.042)
TIMESTRING	Time string to set the display time (e.g., S16:04:37;15.03.16S)

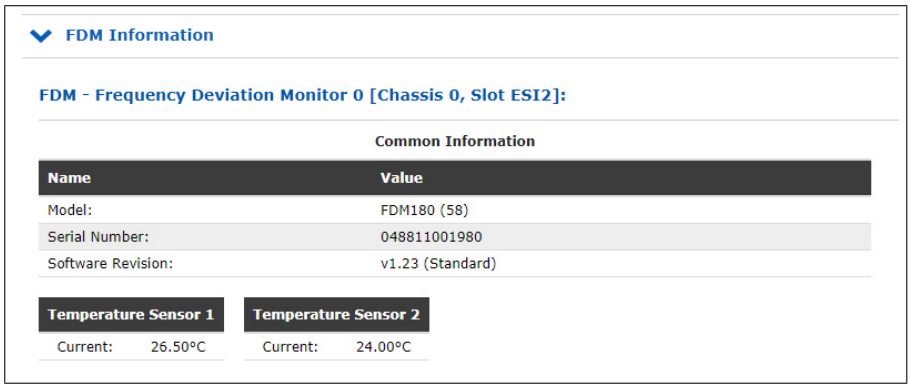
An auto-toggle feature allows a sequence of formats to be defined by configuring comma-separated format strings. Additionally, the duration of a format string can be defined using the *FORMATSTR@DURATION* format.

The example below displays the Power Line Frequency for 20 seconds, then the Reference Time for 30 seconds, then the Frequency Deviation for 10 seconds. It then restarts the sequence from the beginning with the PLF display again:
PLF %PLFRQ Hz@20,REF %REFTIME@30,FDV %FRQDEV@10

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

Append Timestamps: Specifies whether a timestamp should be appended to the message.

10.1.8.3 FDM Information



10.1.8.4 Serial FDM Telegrams

10.1.8.5 Standard FDM String

The Standard FDM String is a sequence of 62 ASCII characters containing the frequency *F*, the frequency deviation *FD*, the reference time *REF*, the power line time *PLT*, and the time deviation *TD*. Each field is separated by a space character (ASCII code 20h). The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements 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 each value is described below:

F:*49.984*	The measured power line frequency, resolution: 1 mHz.
FD:*-00.016*	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz.
REF:*15:03:30*	The reference time from the upstream reference clock (hours:minutes:seconds)
PLT:*15:03:30.378*	The power line time, based on the mains frequency, (hours:minutes:seconds.milliseconds) Time jumps such as changes between daylight saving and standard time or leap seconds are **not** applied to power line time!
TD:*+00.378*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms, maximum: +-99.999 s

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each reference time second.

10.1.8.6 Standard 2 FDM String

The Standard 2 FDM string is identical to the Standard FDM string, but varies in the frequency of transmission, depending on the configured transmission mode.

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second and at each 500 ms interval between each second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	Not supported.

10.1.8.7 Short FDM String

The Short FDM String is a sequence of 23 ASCII characters containing simplified information about the frequency deviation *FD* and time deviation *TD*, separated by a space character (ASCII code 20h). The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

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

The meaning of each value is described below:

FD:*-00.016*	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz, maximum: +-09.999 Hz
TD:*+00.378*	The time deviation of the power line time relative to the reference time, resolution: 1 ms, maximum: +-99.999 s

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each reference time second.

10.1.8.8 Areva (TTM1) FDM String

The Areva FDM String is a sequence of 71 ASCII characters containing the frequency *020*, the frequency deviation *021*, the time deviation *022*, the power line time *023*, and the reference time *024* (preceded by the three-digit day of the year). Each of these items is separated by a Carriage Return (<CR>, ASCII code 0Dh) followed by a Line Feed (<LF>, ASCII code 0Ah).

Each of the five fields is prefixed with a unique three-digit address (020–024).

The string as a whole is prefixed with the Start of Text character (<STX>, ASCII code 02h) and terminated with an End of Text character (<ETX>, ASCII code 03h).

The characters displayed in italics represent the measured values, while the other characters are unalterable elements 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 each value is described below:

02049.984	The measured power line frequency, resolution: 1 mHz.
021-0.016	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz.
022+00.378	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms.
02315_03_30.378	The power line time, based on the mains frequency, (hours_minutes_seconds.milliseconds) Time jumps such as changes between daylight saving and standard time or leap seconds are **not** applied to power line time!
024068_15_03_30	The reference time from the upstream reference clock, (day-of-year_hours_minutes_seconds). A space (ASCII code 20h) is appended to the time prior to the terminating <CR><LF>.

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	Not supported.

10.1.8.9 TPC (TTM2) FDM String

The TPC FDM string is a sequence of 29 ASCII characters containing the reference time (with the three-digit day-of-year), the time deviation, and the frequency deviation *F*. The string starts with the Start of Header character (<SOH>, ASCII-Code 01h) and is terminated by the characters Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

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

The meaning of each value is described below:

288:10:11:29	The reference time from the upstream reference clock, (day-of-year:hours:minutes:seconds).
?	If the reference clock is not synchronized, this character will be ? (ASCII code 3Fh). If it is synchronized, a space will be output at this point (ASCII code 20h).
-00.03	The frequency deviation of the measured frequency relative to the nominal frequency, resolution: 1 mHz.
F*+50.01*	The measured power line frequency, resolution: 10 mHz.

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	Not supported.

10.1.8.10 Computime Extended FDM String

The Computime Extended FDM String consists of a sequence of 42 ASCII characters containing the reference time (with date and day of the week), the time deviation D and the frequency F. The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

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

The meaning of each value is described below:

T:*10:03:09:02*:	The date from the upstream reference clock, (year:month:day:day-of-the-week / Monday = 01, Sunday = 07)
15:03:30	The reference time from the upstream reference clock, (hours:minutes:seconds).
D:*+000.378*	The time deviation between reference time and power line time, signed (+/-), resolution: 1 ms, maximum: +-99.999 s (always with a leading zero!)
F:*49.984*	The measured power line frequency, resolution: 1 mHz.

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each reference time second.

10.1.8.11 Fingrid FDM String

The Fingrid FDM String is a sequence of 34 ASCII characters containing the reference time, the time deviation *T*, and the frequency deviation *F*. The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

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

The meaning of each value is described below:

079:08:13:55.000	The reference time from the upstream reference clock, (day-of-year:hours:minutes:seconds:milliseconds).
T*+6.780*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms.
F*+0.012*	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz.

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) or "T" (ASCII code 54h) at RxD.
Per second, <CR> on second change	Not supported.

10.1.8.12 FDM III String

The FDM III String is a sequence of 52 ASCII characters containing the reference time (with three-digit day-of-year), the time deviation *T*, the frequency deviation *F*, the measured power line frequency *SF*, and the power line time *ST*. The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

068:12:17:55?T*-1.537*F*+0.123*SF*+60.095*ST*12:17:53.463*<CR><LF>

The meaning of each value is described below:

068:12:17:55	The reference time from the upstream reference clock, (day-of-year:hours:minutes:seconds).
?	If the reference clock is not synchronized, this character will be ? (ASCII code 3Fh). If it is synchronized, a space will be output at this point (ASCII code 20h).
T*-1.537*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms.
F*+0.123*	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz.
SF*+60.095*	The measured power line frequency, resolution: 1 mHz.
ST*12:17:53.463*	The power line time, based on the mains frequency, (hours:minutes:seconds.milliseconds). Time jumps such as changes between daylight saving and standard time or leap seconds are **not** applied to power line time!

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) or "T" (ASCII code 54h) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each reference time second.

10.1.8.13 FDM III XLi String

The FDM III XLi String is a sequence of 52 or 56 ASCII characters (depending on transmission mode, see below) containing the reference time (with three-digit day-of-year), the time deviation *T*, the frequency deviation *F*, the measured power line frequency *SF*, and the power line time *ST*. The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

It differs from the standard FDM III string in that it features an additional leading zero in the time deviation field *T* while the frequency field *F* is unsigned here.

If the transmission mode is set to *per second*, *per minute*, or *per second <CR> on second change*, the string will be as follows:

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

If the transmission mode is set to *on request '?' only*, the string will include the reference time with millisecond precision as follows:

068:12:17:55.000?T*−01.537*F*+0.123*SF*60.095*ST*12:17:53.463*<CR><LF>

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

The meaning of each value is described below:

068:12:17:55	The reference time from the upstream reference clock, (day-of-year:hours:minutes:seconds). If the transmission mode is set to *on request '?' only*, the format of this field will be (day-of-year:hours:minutes:seconds.milliseconds).
?	If the reference clock is not synchronized, this character will be ? (ASCII code 3Fh). If it is synchronized, a space will be output at this point (ASCII code 20h).
T*−01.537*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms.
F*+0.123*	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz.
SF*60.095*	The measured power line frequency, resolution: 1 mHz.
ST*12:17:53.463*	The power line time, based on the mains frequency, (hours:minutes:seconds.milliseconds). Time jumps such as changes between daylight saving and standard time or leap seconds are **not** applied to power line time!

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) or "T" (ASCII code 54h) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each reference time second. The reference time is output with millisecond precision instead of second precision in this case.

10.1.8.14 SIE-TSF-FDM String

The SIE-TSF String is a sequence of 32 ASCII characters containing the reference time *R*, the time deviation *D*, and the measured power line frequency *F*. Each field is terminated by a Line Feed (<LF>, ASCII code 0Ah) followed by a Carriage Return (<CR>, ASCII code 0Ah).

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

R:*13:11:19*<LF><CR>D:*+000.575*<LF><CR>F:*49.981*<LF><CR>

The meaning of each value is described below:

R:*13:11:19*	The reference time from the upstream reference clock, (day-of-year:hours:minutes:seconds).
D:*+000.575*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms.
F:*+0.123*	The measured power line frequency, resolution: 1 mHz.

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each are received at the start of each reference time second.

Information:

The SIE-TSF string uses the sequence <LF><CR> as a terminating sequence for each of the fields instead of the standard <CR><LF>.

However, if *per second, <CR> on second change* is configured with this string type, the string as a whole (after the *F* field) is terminated by the conventional termination sequence <CR><LF>, such that the first two fields are still terminated with <LF><CR>, but the last field is terminated with <CR><LF>. As a result, the complete string in this case would be as follows (as an example):

R:13:11:19<LF><CR>D:+000.575<LF><CR>F:49.981<CR><LF>

10.1.8.15 Vorne Display String

The Vorne Display String is a sequence of 90 ASCII characters containing the reference time, the frequency deviation, the time deviation (in two different formats), the power line time, and the power line frequency. Each field is terminated by a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah), and the string as a whole is terminated by a Bell character (<BEL>, ASCII code 07h).

The Vorne Protocol is employed by a proprietary phasor measurement unit, and the implementation in the FDM is therefore aimed at enabling the continued use of existing receivers. Please note, however, that the FDM is not a full phasor measurement unit, and while the phase and magnitude fields are preserved in the time string to maintain compatibility, these fields in the string as provided by the FDM will always be set to zero.

The Vorne Protocol also includes an "out-of-lock" field that specifies how long the reference clock has been isolated from the upstream reference source. This is also not used by the FDM; if your Meinberg system loses lock with its reference source and falls back to holdover, the FDM will suspend string output; the "out-of-lock" field will remain at 0 even after this time, even if the reference clock is set to simulation mode.

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements of the string:

1100<CR><LF>44*101103*<CR><LF>22*+00016*<CR><LF>33*+015*<CR><LF>34*+ 0156*<CR><LF>
66*101103*<CR><LF>77*50016*<CR><LF>8800000<CR><LF>8900000<CR><LF>55*164*<CR><LF><BEL>

The meaning of each value is described below:

1100	A notional "out-of-lock" time that would specify how long the clock had been disengaged from its reference source on original devices. This is always 11 (the field code) followed by 00 (the placeholder time) on a Meinberg system.
15:03:30	The reference time from the upstream reference clock, (HoursMinutesSeconds)
22+00016	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz. The first two digits are the integer value, the last three digits represent the three decimal places.
33*+ 015*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 10 ms. The first two digits are the integer value, the last three digits represent the three decimal places. If the deviation exceeds a value of *+9.99* or is less than *-9.99*, this overflow this overflow will be represented by the last two decimal places being represented by spaces (i.e., +9.<SP><SP><CR><LF>). Please note that no rounding is performed, i.e., a value of +089 may represent any value between *+0.890* or *+0.899*.
34*+ 0156*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms. This is represented as a six-digit value; the first three digits after the sign are the integer value, the last three digits represent the three decimal places. Any leading zeroes in the integer segment will be substituted with spaces (i.e., 34+1500<CR><LF> represents 1 second and 500 milliseconds. If the deviation exceeds a value of *+999.999* or is less than *-999.999*, this overflow will be represented by all numerical characters being substituted with spaces (i.e., +<SP><SP><SP><SP><SP><SP><CR><LF>). The direction of the overflow will remain indicated by the +/- sign.
66101103	The power line time, based on the mains frequency, (HoursMinutesSeconds) Time jumps such as changes between daylight saving and standard time or leap seconds are **not** applied to power line time!

77*50016*	The measured power line frequency, resolution of 1 mHz. The first two digits are the integer value, the last three digits represent the three decimal places.
88*00000*	A notional phase value for the power line waveform that would specify the phase of the AC wave at the time of measurement. This is always 88 (the field code) followed by 00000 (the placeholder value) on a Meinberg system.
89*00000*	A notional magnitude value for the power line waveform that would specify the the AC wave at the time of measurement. This is always 89 (the field code) followed by 00000 (the placeholder value) on a Meinberg system.
55*164*	The day-of-year value from the upstream reference clock (1– 366).

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating character <BEL> is received at the start of each reference time second.

10.1.8.16 Old Standard FDM String

The Old Standard FDM String is a sequence of 62 ASCII characters containing the frequency *F*, the frequency deviation *FD*, the reference time *REF*, the power line time *PLT*, and the time deviation *TD*. Each field is separated by a space character (ASCII code 20h). The string is terminated with a Carriage Return (<CR>, ASCII code 0Dh) and Line Feed (<LF>, ASCII code 0Ah).

The current "Standard FDM" string format replaced the old format at the end of 2023, but remains supported in order to preserve compatibility with appropriate receivers. The only difference is that the hours, minutes, seconds, and milliseconds of the reference time and power line time are separated by periods in the current string format, whereas they were previously separated by a colon in the old format.

The letters displayed in italics below represent the measured values, while the other characters are unalterable elements 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 each value is described below:.

F*+49.984*	The measured power line frequency, resolution: 1 mHz.
FD:*-00.016*	The frequency deviation of the measured frequency relative to the nominal frequency, signed (+/-), resolution: 1 mHz.
REF:*15:03:30*	The reference time from the upstream reference clock (hours:minutes:seconds).
PLT:*15:03:30:378*	The power line time, based on the mains frequency, (hours:minutes:seconds:milliseconds). Time jumps such as changes between daylight saving and standard time or leap seconds are **not** applied to power line time!
TD:*+00.378*	The time deviation of the power line time relative to the reference time, signed (+/-), resolution: 1 ms, maximum: +-99.999 s

Transmission Mode Behavior

Per second	The transmission of the string is initiated at the start of each reference time second.
Per minute	The transmission of the string is initiated at the start of each reference time minute.
On request '?' only	The transmission of the string is triggered by receipt of the character "?" (ASCII code 3Fh) at RxD.
Per second, <CR> on second change	The transmission of the string is initiated in advance of a new reference time second so that the terminating characters "<CR><LF>" are received at the start of each reference time second.

10.1.8.17 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.

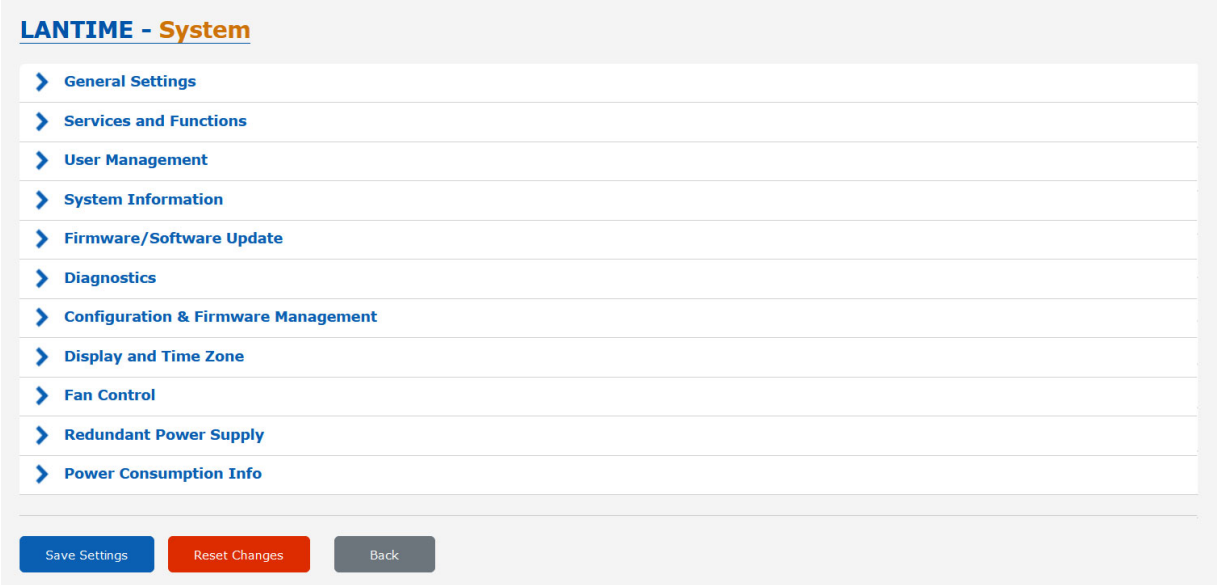
The displayed value has the format: *X8 X7 X6 X5 X4 X3 X2 X1*

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

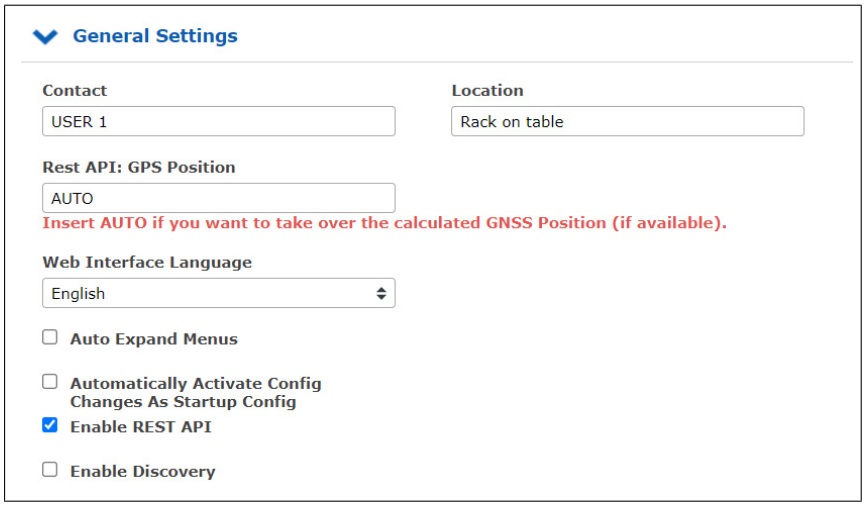
The error bits can be read out serially on request by an "E" (ASCII code 45h) via the interfaces COM 0/1.

The format of the response string is:
ERROR:X8X7X6X5X4X3X2X1<CR><LF>

10.1.9 System



10.1.9.1 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.

Rest API: GPS Position
The entered value will be output as GPS position of the LANTIME via the REST API.

Web Interface Language:
Language setting 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.

Each configuration change can then be saved as start configuration by confirming with "Save as startup configuration now" button.

REST API Support

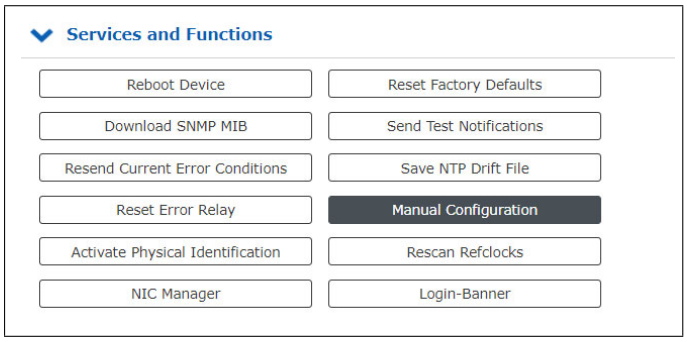
In the 7.04 release, a REST API interface is offered for the first time to retrieve status information and make configuration adjustments from external management systems over a secure HTTPS connection. The available objects are stored in a JSON-based syntax as a tree structure. The REST API can be enabled and disabled as a service by configuration.

A description of all available objects is available in an online help, which can be downloaded as a ZIP archive here: http:mbg.link/clihelp

Enable Discovery

The LANTIME provides information for a better mapping in the Meinberg Network Management System (mbgNMS).

10.1.9.2 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 V7 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. If your LANTIME system does not have function keys and a display, then the beep mode can also be terminated via a console connection with the command **'fpc'**. In the start menu that appears, simply press the F2 key on your keyboard. For a terminal connection you need your access data (user and password).

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.

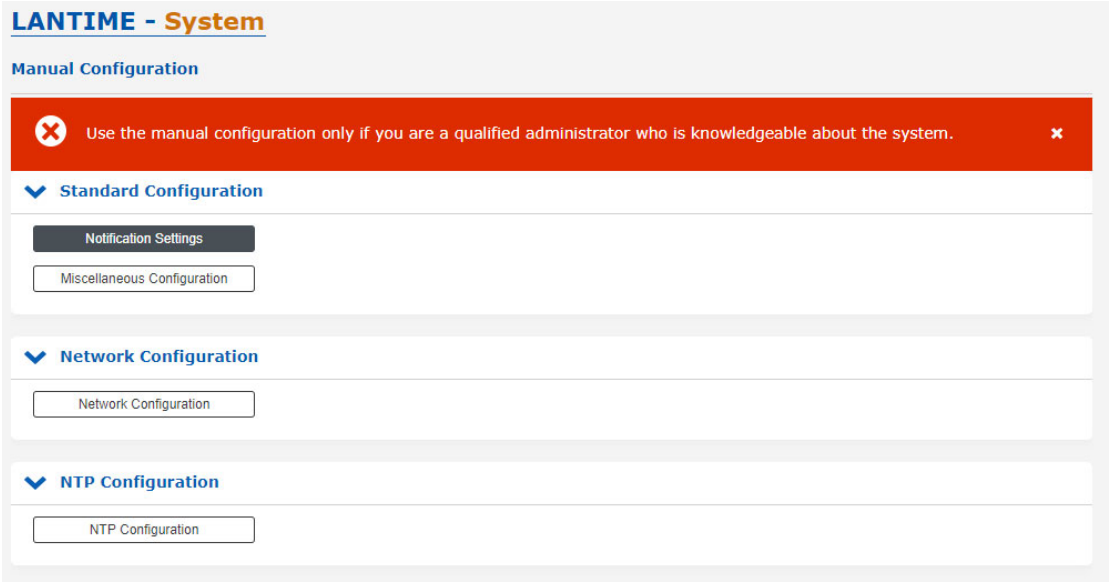
NIC Manager
The NIC Manager checks the system for physical network interfaces. This applies to the additional interfaces that can be added to the system via LNE modules. After the installation and initialization of an LNE card, the function must be executed so that the file "etc/mbg/net.cfg" is rewritten. The network port status can then be displayed on the start page of the web interface.

The NIC Manager function should also be executed after removing or replacing an LNE. The system uses the MAC addresses of the individual network ports to check whether they exist, whether their position (slot) in the system has changed or whether new interfaces exist.

Rescan Refclocks
This function must be executed if a second clock is subsequently installed in IMS systems in order to obtain a redundant receiver configuration. After start-up, the system remembers the serial connection of the reference clock used. If, for example, an M3000- or M1000 system with built-in RSC a second clock will be installed during operation (hot-plug), the "Rescan Refclocks" button must be pressed to register the new clock so that the serial connection of the second clock will be saved on the system.

Login Banner
The Login Banner button opens a dialogue to create your own login banner. The banner is integrated on the login page. Thus, a user can be shown a hint on how to use the device before logging in. It is possible to enter HTML (to a limited extent) and text in the text field.

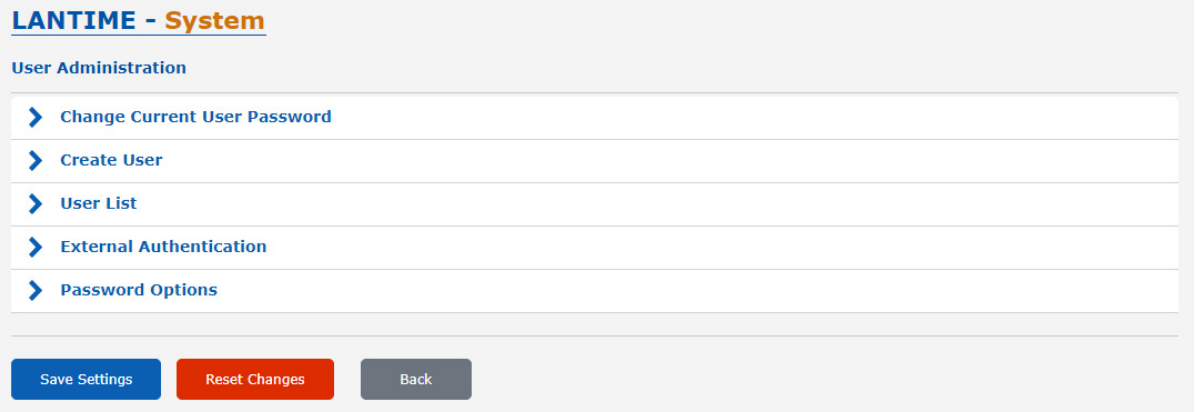
10.1.9.3 Manual Configuration



- 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.).

10.1.9.4 User Management



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.

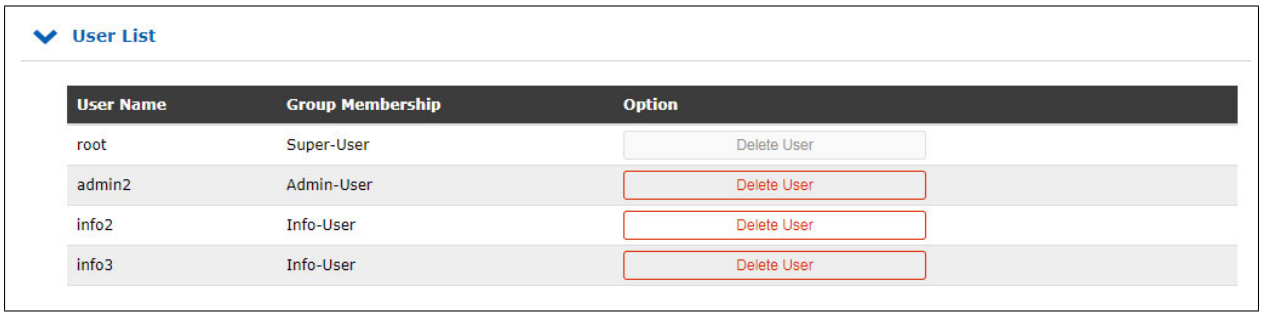
The table below illustrates the user-rights of each access level in detail.

	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 a Firmware Update	✓		
Create a diagnostic file	✓		
Create a new super user account	✓		
Review all webinterface configuration values	✓	✓	✓

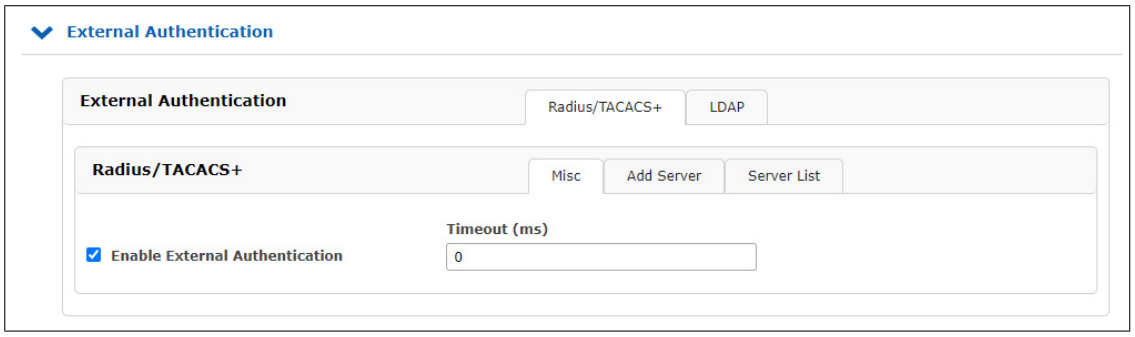
*Additional Network Configuration, Additional NTP Configuration, User defined notifications

User List

This submenu gives you an overview of all configured LANTIME users. By clicking "Delete User" a single user can be deleted.



10.1.9.5 External Authentication Options



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 Authentification Methods:
1. LDAP
2. RADIUS
3. TACACS+

10.1.9.6 LDAP / LDAPS

Lightweight Directory Access Protocol
LDAP is based on the client-server model and is used for so-called directory services. LDAP describes the communication between the LDAP client and the directory server. Object-related data, such as personal data or computer configurations, can be read from such a directory.

10.1.9.7 LDAP Setup

Example LDAP setup in connection with the Microsoft Active Directory (AD)

This chapter describes an example for setting up an LDAP connection with the Microsoft Active Directory with non-standard attributes of an admin user. Please note that this is an example only and may not be directly applicable to your directory structure. Please contact your directory service administrator to identify any discrepancies and make any necessary adjustments.

The ADSI editor of the Microsoft Active Directory is used to adjust the following attributes of an LDAP user in this example:

- gidNumber = 4
- sAMAccountName = ldap-ad
- uidNumber = 10020
- unixHomeDirectory = /home/ldap-ad
- loginShell = /bin/false

The name of the user (ldap-ad) the uidNumber and the "HomeDirectory" name are freely selectable. These are only example values. Also the attributes (e.g. sAMAccountName) can be freely chosen by the mapping. It is only important that a mapping of the attribute selected in the directory service is defined by the attribute provided for this purpose in the RFC ("shadow uid sAMAccountName" for this example).

The **gidNumber** can also be specified in a group of the directory service (Secondary Group Support). The user then still needs a primary group, but it has no meaning for a LANTIME. For this purpose, the user can map the **gidNumber** to the AD attribute **primaryGroupID**, for example.

After specifying "LDAP User", "LDAP Password", "Search Scope" and "Search Base", the filters and mappings can be defined. The LDAP user/binddn is required to read information from the AD, and is not normally a user to log into this machine afterwards.

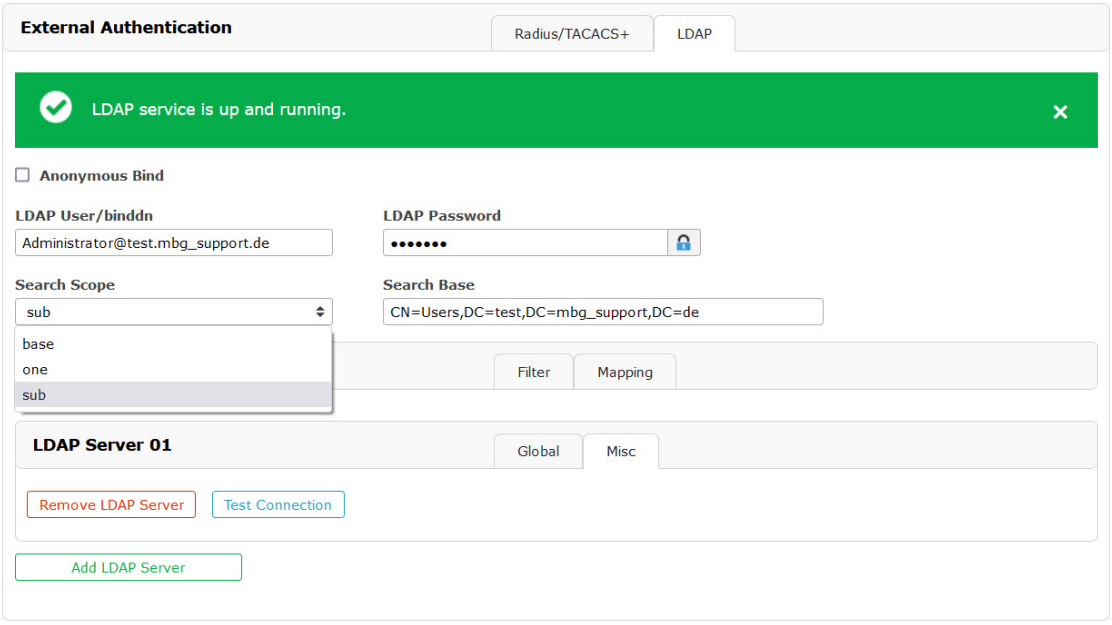


Figure: Web interface menu "System → User Administration → External Authentication → LDAP"

In the sample domain test.mbg.de the "Search Base" "CN=Users,DC=test,DC=mbg" was selected and the "Search-Scope" was set to "sub".

The following filters and mappings must be added to this sample configuration via the web frontend of LTOS.

Filter:
- passwd (&(objectClass=user)(unixHomeDirectory=*))
- shadow (&(objectClass=user)(uidNumber=*)(unixHomeDirectory=*))

Figure: LDAP sub menu "Advanced LDAP Configuration → Filter"

Mappings:
- passwd uid sAMAccountName
- passwd homeDirectory unixHomeDirectory
- shadow uid sAMAccountName

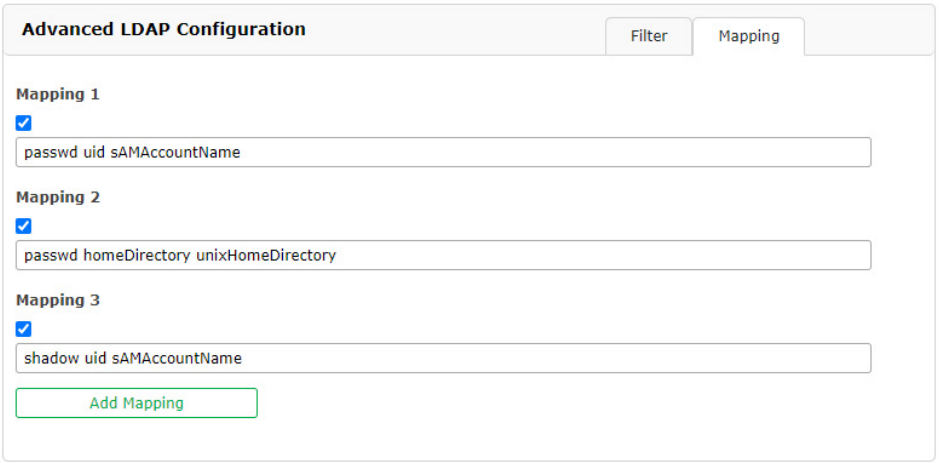
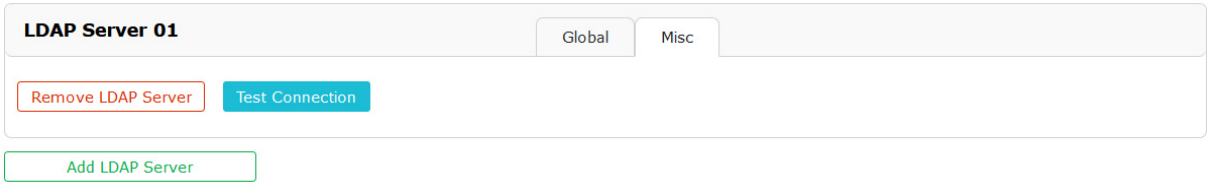


Figure: LDAP sub menu "Advanced LDAP Configuration → Mapping"

The gidNumber can sometimes conflict with group membership on other systems. Ask your directory service administrator for possible avoidance strategies.

After the URI of the LDAP server is assigned, the settings can be saved. If LDAP is selected as the protocol, the configured LDAP users can log in via the web frontend (and the CLI if a loginShell has been assigned for the super user). If LDAPS is selected as protocol, the rootca certificate that uniquely identifies the LDAP server (see CA Certificates) must be added beforehand.

In case of problems, the connection can be tested under "Misc" of the respective LDAP server entry. Here the basic connectivity is checked with the mandatory values URI, bind dn and search base. The status of the LDAP functionality is shown in the banner of the LDAP tab.



10.1.9.8 RADIUS

Radius stands for Remote Authentication Dial In User Service and provides centralized authentication for LANTIME 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.

10.1.9.9 TACACS

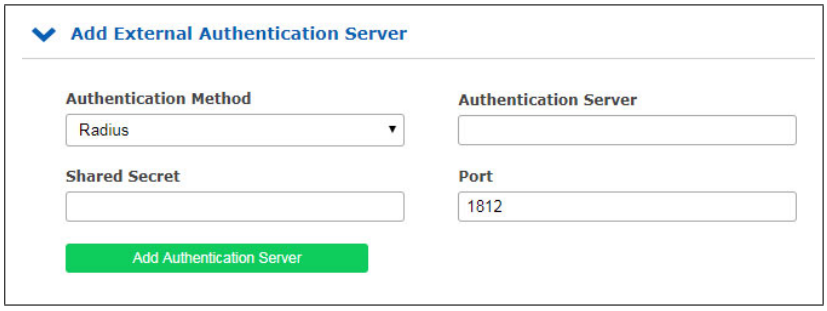
Terminal Access Controller Acc-Control System is a remote authentication protocol that gives the LANTIME the possibility to communicate with a TACACS authentication server.

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.

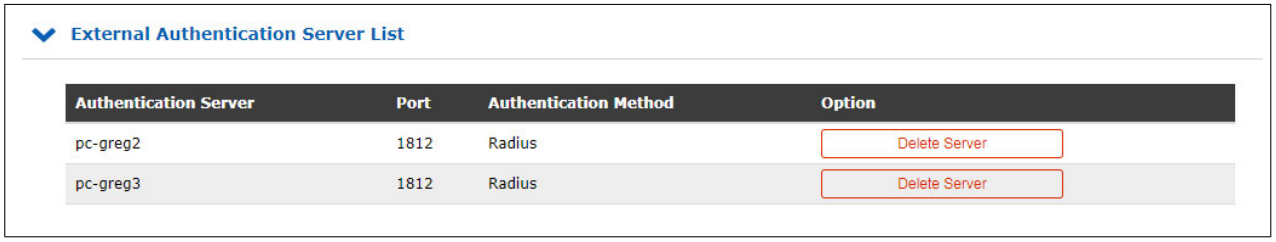
Authentication Method:
Configuration of the authentication method to use, either Radius or TACACS+. More detailed information on both methods can be found in the upper part of this chapter..

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")

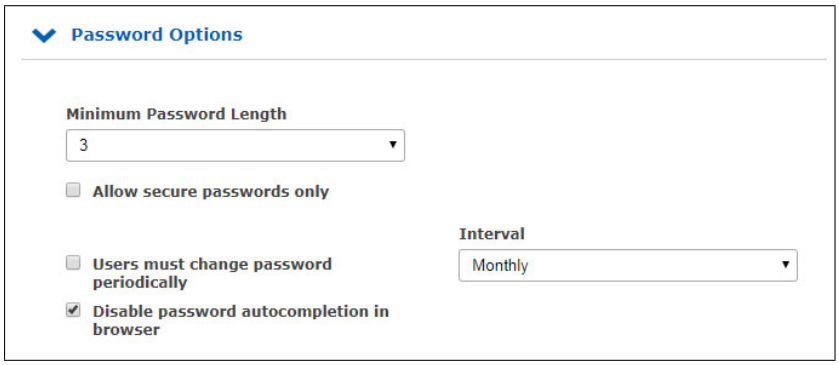
Port:
Depending on the authentication method, the default port is already configured here. If needed, the port can be changed.

External Authentication Server List



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.

10.1.9.10 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

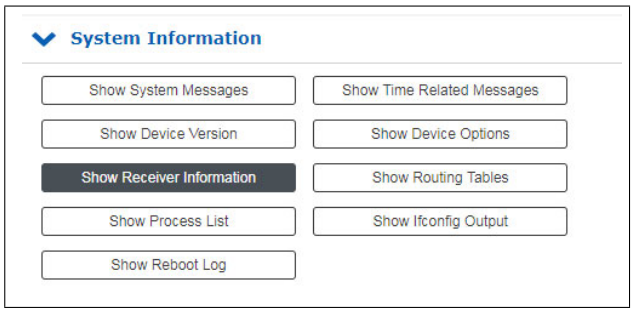
A list of allowed signs which can be used as special characters you can find in the chapter "Before you Start → Text and Syntax Conventions")

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.

10.1.9.11 System Information



The "System Information" menu offers the possibility to view important log files and setups of the LANTIME.

Show System Messages: Displaying the LANTIME SYSLOG file stored in /var/log/messages

Show Device Version: Displaying the additional device information (model, firmware, serial number, built-in hardware components, etc.)

Show Receiver Information: Displaying the additional status information on the built-in reference clock.

Show Process List: Displaying of all currently running processes.

Show Reboot Log: Displaying the reboot logs stored in /mnt/flash/data/reboot.log. The log file contains information about past system reboots.

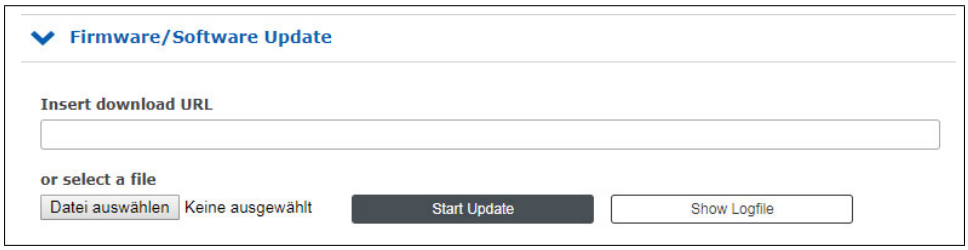
Show Time Related Messages: Displaying the file /var/log/lantime_messages.

Show Device Options: Displaying additional system parameters.

Show Routing Tables: Displaying the network routing table.

Show Ifconfig Output: Displaying information for all network interfaces (output of the command "ifconfig -a")

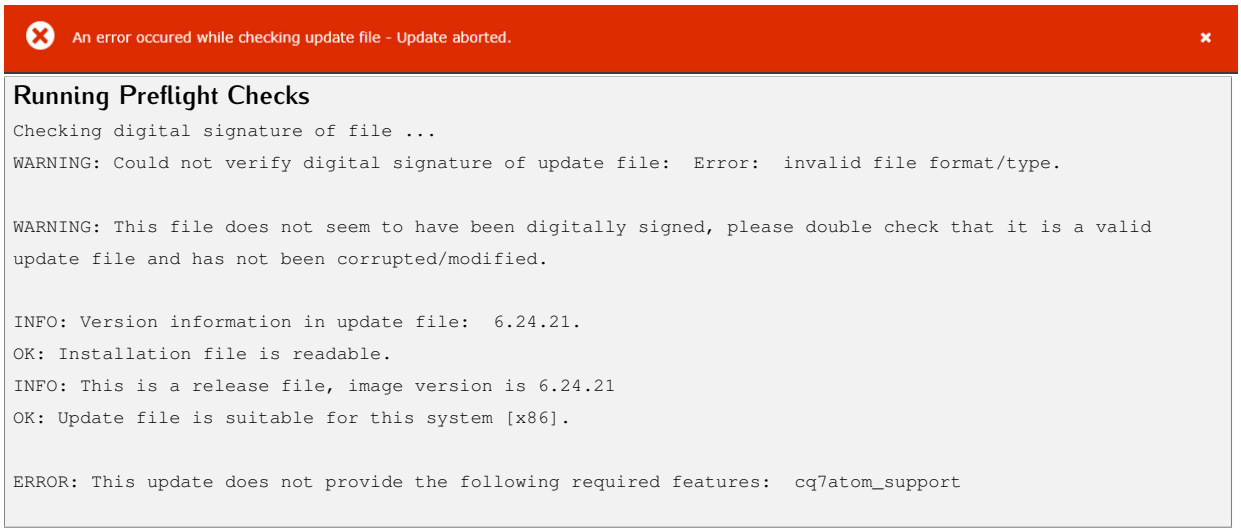
10.1.9.12 Firmware/Software Update



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.

Errors may be detected during installation, such as an unusable update package or a missing signature of the update file. For security reasons, some information is displayed during installation. The following is an excerpt of possible warning or info messages:



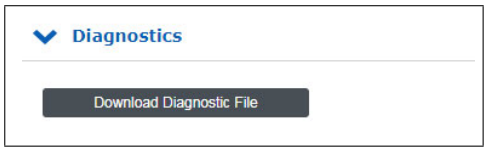
This example shows the attempt to install an update package that does not support the CPU's Q7 processor.

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

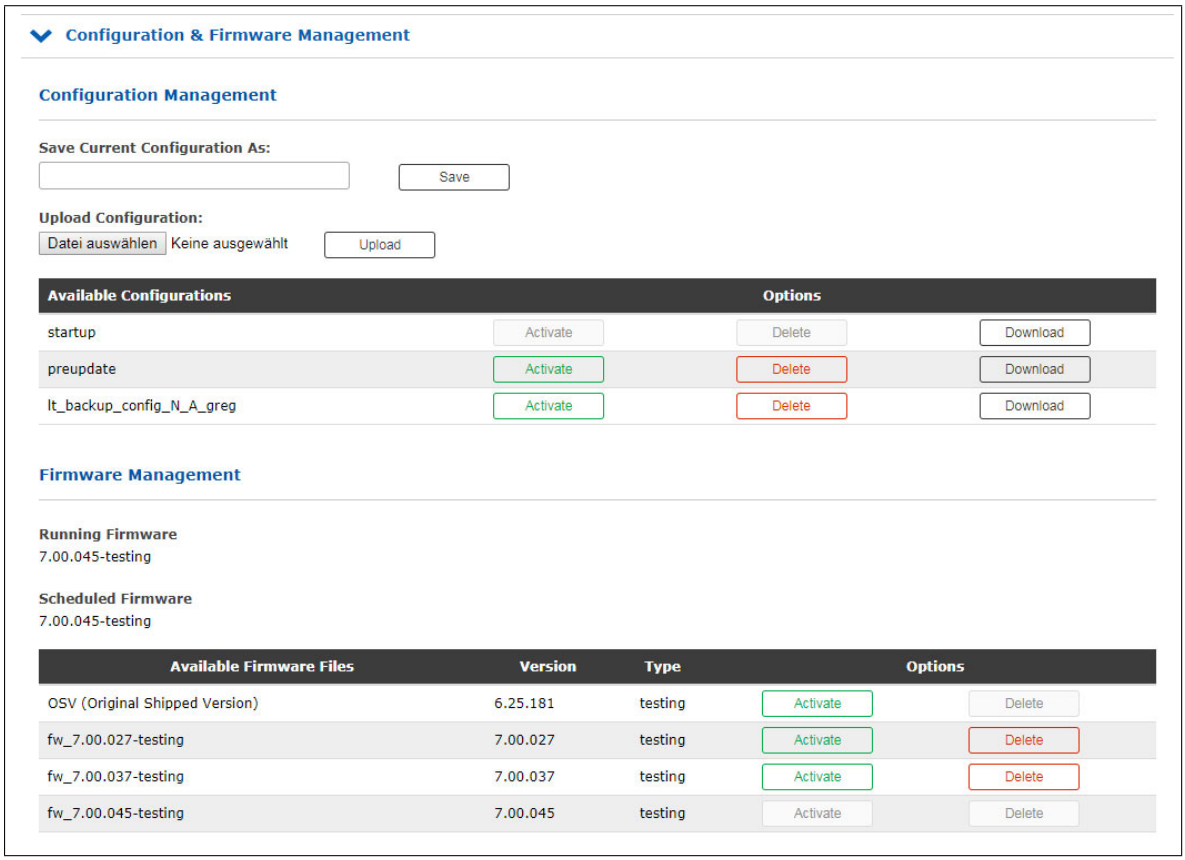
Note: No new firmware revision number will be displayed under Firmware Management after a module update is installed. Refclock and HPS100 updates are enabled immediately after a reboot.

10.1.9.13 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.

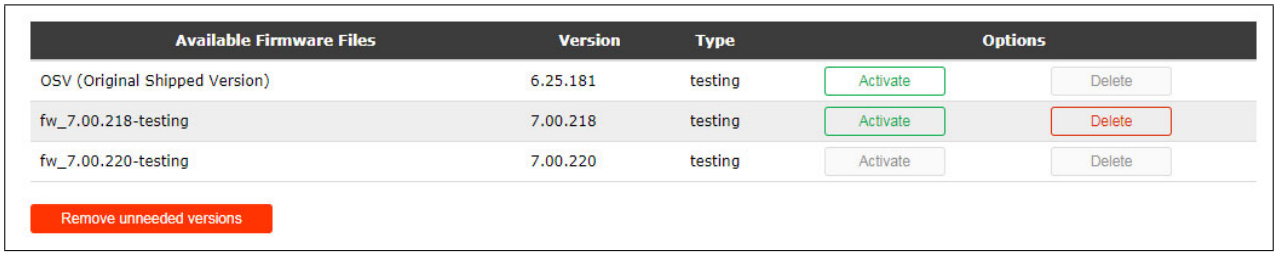
10.1.9.14 Configuration and Firmware Management



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.

Remove unneeded Versions



With this button all unused firmware versions can be deleted. Only the active firmware and the OSV (Original Shipped Version) remain on the system.

LANTIME Updates for reference clocks and HPS modules

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.

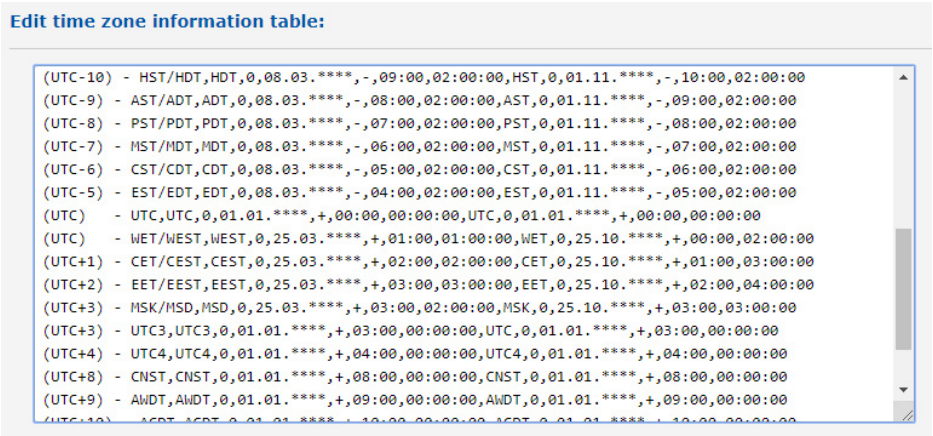
10.1.9.15 Display

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.)

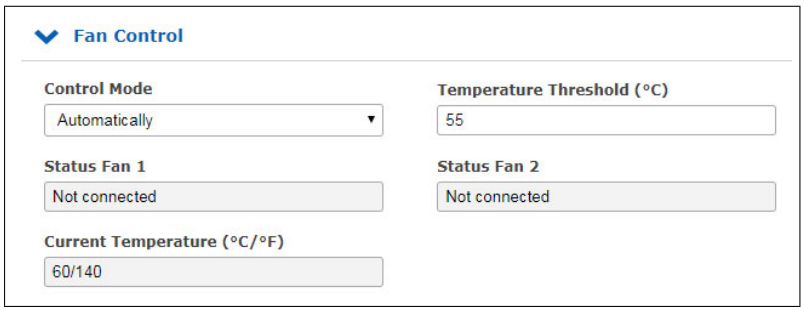
11. Field: Sign (+ or -) Add or subtract offset from UTC → +

12. Field: UTC offset (hh:mm) → 01:00

13. Field: Time of changeover → 03:00

10.1.9.16 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 (°/°F): Displaying the current temperature in degrees Celsius and Fahrenheit.

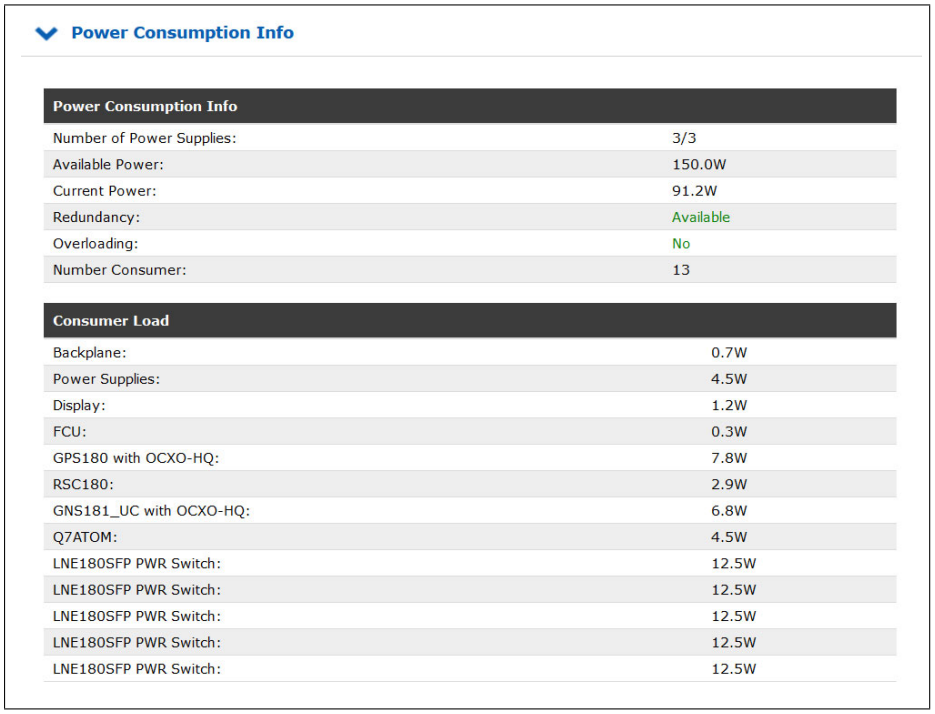
10.1.9.17 Redundant Power Supply

If your LANTIME is an IMS system, the status of the available power supply units is displayed in this submenu.

Redundancy Monitoring
If "Enable Redundancy Monitoring" is activated, a notification is sent via the configured channels if a redundant power supply is no longer ensured in this system (e.g. by disconnecting the power line of a power supply unit). See also chapter Notification.

10.1.9.18 Power Consumption Info

If your LANTIME is an IMS system, all integrated power consumer are displayed and evaluated in this submenu.



Power Consumption Info
The available power depends on the number of used power supply units. In the example we have three power supply units, each with 50W of power - this results in a total of 150W when all power supply units are in active state.

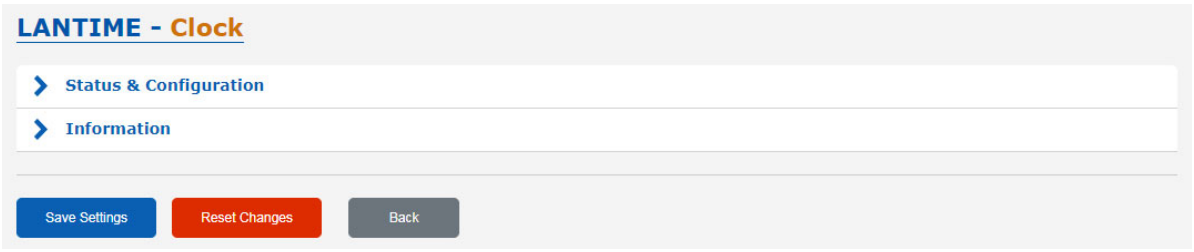
As long as, as in this example, a value below 50W is displayed in the field "Current Power", only one power supply is sufficient to supply this system. If the value is greater than or equal to 50W, two power supply units are required for supply or three active power supply units are required to ensure redundancy.

The "Redundancy" field is set to "Available" if the "Available Power" minus the "Current Power" is greater than or equal to 50W. The "Overload" field always displays "No" as long as the "Current Power" is less than or equal to "Available Power".

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.

10.1.10 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.

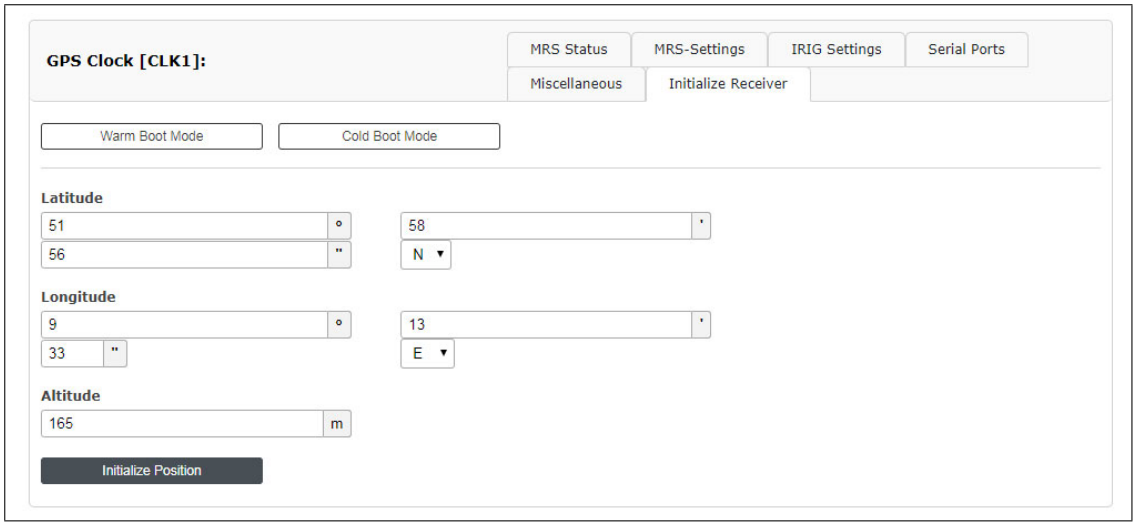


Figure: Menu "Clock" in case of a single receiver

10.1.10.1 Synchronization with GNSS (GXL Clock Module)

This chapter describes how to quickly set up the GXL reference clock for synchronization to GNSS services.

Information:

This function is available as from LTOS firmware version 7.08.007.

Step 1: Connection of the GXL receiver with the GNSS Multi-Band Antenna

Ensure that the GXL is connected to a correctly installed GNSS Multi-Band Antenna.

Step 2: Selecting the Satellite Constellations

The GXL receiver is capable of receiving signals from the GPS, Galileo, BeiDou, and GLONASS satellite constellations simultaneously.

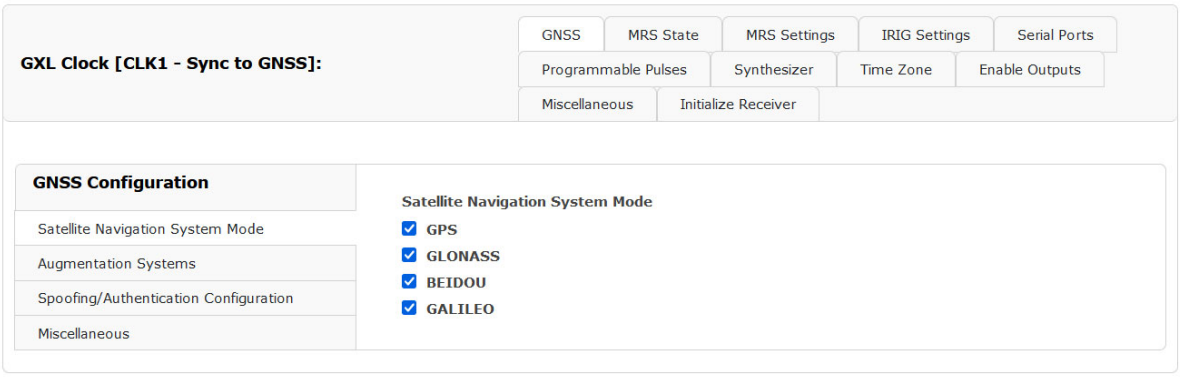


Illustration: Specifying the satellite constellations to be used

The GXL reference clock also supports the Japanese QZSS constellation and a number of national satellite-based augmentation systems (SBAS). The following augmentation systems are supported:

- European Geostationary Navigation Overlay Service (EGNOS) – Europe
- Wide Area Augmentation System (WAAS) – United States, Canada, Mexico
- GPS Aided Geo Augmented Navigation (GIGAN) – India
- Multi-functional Satellite Augmentation System (MSAS) – Japan
- System for Differential Corrections and Monitoring (SDCM) – Russia

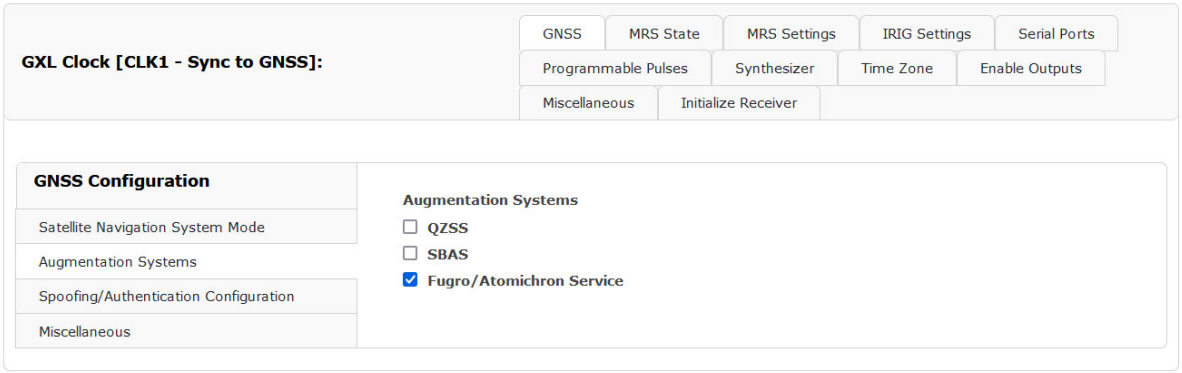


Illustration: Enabling support for the Japanese QZSS constellation and national SBAS constellations.

You may specify which constellations should be used and which should be excluded by logging into the Web Interface of your LANTIME system and proceeding as follows:

1. Open the menu "**Clock**" → "**State & Configuration**".
2. Select the corresponding clock module.
3. Click on the "GNSS" tab.
4. Select the constellations using the checkboxes under "**Satellite Navigation System Mode**".
5. If desired, enable support for regional augmentation systems under "**Augmentation Systems**".

Information:

If you intend to use Fugro NMA spoofing detection, ensure that "**Fugro AtomiChron® Service**" is enabled under "**Augmentation Systems**".

Step 3: Configuring the Signal Propagation Time

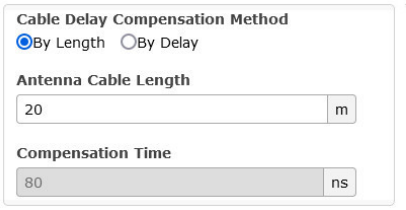
The signal propagation time for the satellite signal is influenced by the length of the cable and can cause a delay in signal reception of approx. 4 ns/m cable length (when using H155 antenna cable).

To enable the connected reference clock to compensate for the cable-induced propagation delay of the signal, you must either specify the length of the antenna cable in meters (antenna –> Meinberg system) or enter the offset time in nanoseconds under the configuration settings for your reference clock.

To do this, proceed as follows:

1. From the same page as Step 1 above (**Clock –> State and Configuration**), ensure that the "**Miscellaneous**" tab under the corresponding clock module is selected.

2. Under "**Cable Delay Compensation Method**" select the compensation method and enter the appropriate value.



Information:

The default value set in this field is 20 m or 80 ns. LANTIME OS supports a maximum value of 2000 m or 8000 ns respectively.

The delay time can be estimated automatically as the cable length multiplied by 4; this is done on the assumption that you are using H155 antenna cable. This will provide a reasonable estimate of the propagation delay.

If you are using a different cable type or transmission method, the propagation delay must be calculated manually and entered in nanoseconds. A manual specification of the propagation delay is also recommended if you wish to further improve time accuracy relative to a time standard such as UTC.

Step 4: Position Lock Behavior Configuration

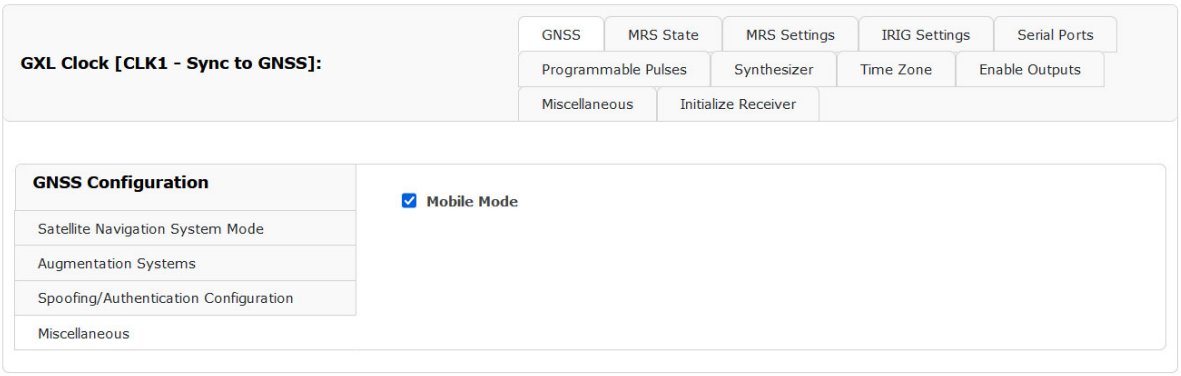


Illustration: Enabling mobile mode

If your GXL reference clock is intended to be operated in a mobile capacity (i.e., aboard a moving vehicle), you should enable "**Mobile Mode**" under "**Miscellaneous**". Mobile mode allows the position of the receiver to remain dynamic at the expense of some clock accuracy and spoofing detection reliability.

If your GXL will be used in a fixed location, ensure that this option is *disabled* in order to maximize clock accuracy and the reliability of spoofing detection.

Step 5: Navigation Message Authentication Configuration

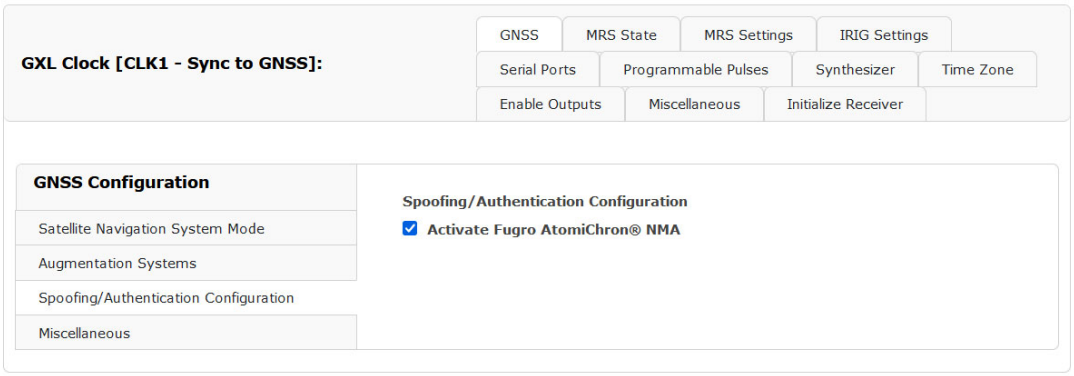


Illustration: Configuring Navigation Message Authentication (spoofing detection)

To enable Navigation Message Authentication (NMA) for spoofing detection, you should enable "**Activate Fugro NMA**" accordingly.

Fugro's AtomiChron® service requires an active subscription. For more information on managing an AtomiChron® subscription, refer to Chapter 10.1.10.2, Enabling the AtomiChron®Service (GXL Clock Module).

For more information on Navigation Message Authentication in general, refer to Chapter 13.8, How Navigation Message Authentication Works.

Information:

Ensure that Galileo and Fugro AtomiChron® reception are enabled accordingly as described in Step 2 above!

Step 6: MRS Configuration

If you only wish to configure GNSS reception, proceed with the MRS configuration process described in Chapter 10.1.10.4, "MRS Settings".

Otherwise, proceed with the configuration of other reference sources.

Final Steps

Once the antenna and power supply have been connected, the reference clock is ready for operation.

After around two minutes of the system being switched on, the oscillator will have warmed up and thus achieved the base precision required to receive satellite signals. If valid almanac and ephemeris data are present in the reference clock's battery-backed memory and the receiver's position has not changed since it was last on, the system's CPU will be able to calculate which satellites should currently be receivable.

In this case, only a single satellite needs to be received to enable the clock to synchronize. Otherwise, the system will switch to **Warm Boot** or **Cold Boot** mode as described below.

Warm Boot

If the location of the receiver has changed by several hundred miles since the last time the system was on, the elevation and Doppler shift of the satellites will not match the calculated values. This will cause the system to switch to "Warm Boot" mode, in which it will systematically search for satellites to receive from.

The receiver can use the valid almanac data to detect the identification numbers of existing satellites. If four satellites can be received, the receiver's new position can be determined and the device will switch to "**Normal Operation**" mode.

Cold Boot

If there is no available almanac data (e.g., because the battery-backed memory has been wiped or corrupted), the GNSS reference clock will launch in "Cold Boot" mode, in which the receiver searches for a satellite and reads the entire almanac.

The almanac is broadcast fully every 12.5 minutes, but the receiver may need to wait for the start of the next transmission. Accordingly, this process can last up to 25 minutes, after which the system will switch to "Warm Boot" mode.

10.1.10.2 Enabling the AtomiChron®Service (GXL Clock Module)

The GXL reference clock supports Fugro's AtomiChron® service to allow the integrity and authenticity of incoming GNSS messages from all of the main GNSS constellations to be verified. The data required to authenticate your GNSS signals is transmitted over a separate L-band satellite frequency transmitted by the Inmarsat constellation that your GXL also receives in addition to the actual GNSS signals.

AtomiChron® is a paid subscriber service and the license for it must therefore be activated and occasionally renewed thereafter. The regularity of license renewal will depend on the length of your service agreement.

Because the IMS LANTIME system in which your GXL is installed is expected to be isolated from the public internet for reasons of practicality or operational security, the signal required to activate or renew an AtomiChron® license will be transmitted over the same L-band satellite signal that it receives the authentication data on. Once a subscription contract is concluded and paid up (or a free subscription entitlement is claimed), the activation signal is transmitted over a specified satellite beam.

To this end, your IMS LANTIME system must have the GXL receiver installed, enabled, and connected to a functioning and operational GNSS Multi-Band Antenna.

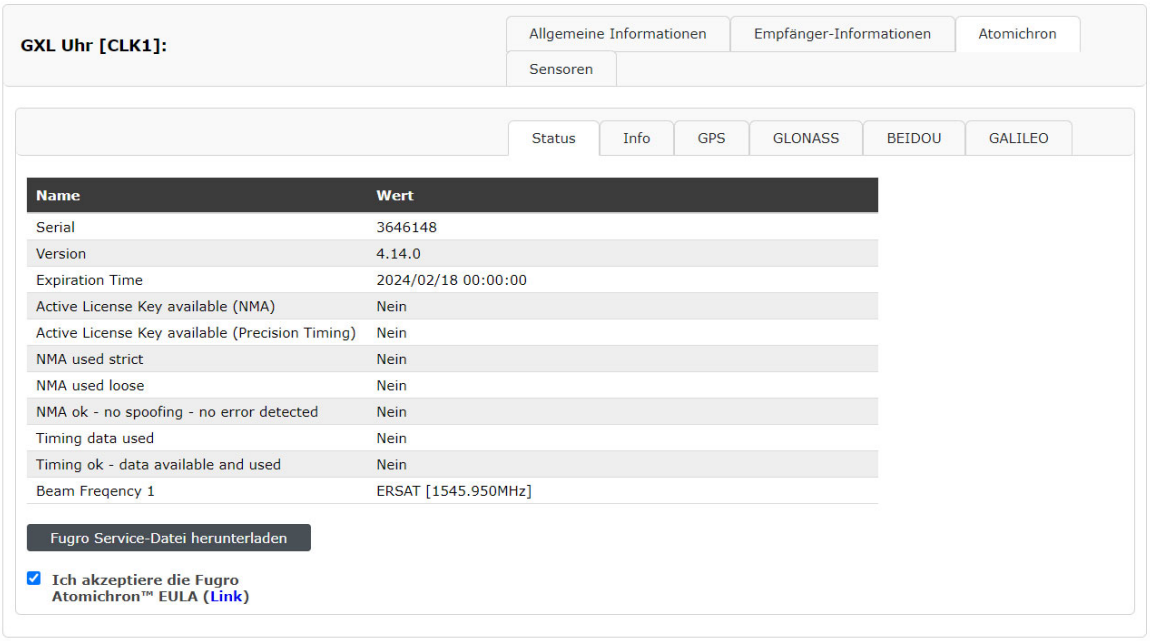


Illustration: Displaying AtomiChron®-related information in the LTOS Web Interface

Certain information is required by Meinberg and Fugro to allow your GXL clock module to receive the appropriate activation data. This information can be conveniently downloaded from your IMS LANTIME system's Web Interface by selecting the "**Clock**" tab, opening the "**Information**" panel, selecting the "**AtomiChron**" tab for the GXL clock module ("**GXL Clock**"), consulting and accepting the Fugro AtomiChron® EULA, and clicking on the button "**Download Fugro Service File**".

This will launch a download of a text file containing all the information needed by Meinberg and Fugro. This file should then be sent as an attachment to Meinberg at *atomichron@meinberg.de* when prompted by Meinberg to do so (i.e., when payment for your subscription has been received or when claiming an entitlement to a free subscription).

Once Meinberg has received and processed this file, the activation data should be transmitted over the frequencies provided in the Fugro Service File within three working days. If you have a specific request regarding the scheduling of the activation data transmission, please also communicate this in the email when sending the Fugro Service File to Meinberg. Please note, however, that Meinberg cannot guarantee that any given schedule request can be honored.

Once you have sent the Fugro Service File to Meinberg, it is essential to leave your IMS LANTIME system operational and connected to a correctly positioned and functioning GNSS Multi-Band Antenna until the activation data is received. You can verify whether the AtomiChron® service has been correctly activated by opening the "**Clock** → **Information** → **GXL Clock** → **AtomiChron** → **State**" tab as described above; if activated, the line "*Active License Key available (NMA)*" will read *Yes*, while the *Expiration Time* line will show the date & time of expiration of your current AtomiChron® license.

Important!

Please note that the activation data is normally only transmitted once and will normally not be transmitted on weekends or Dutch public holidays.

If your GXL clock module still does not show that the activation has occurred within 72 hours of the Fugro Service File being sent (or within 24 hours of a requested activation date), it is possible that the activation signal has been missed.

In this case, please verify that the antenna is correctly installed, connected, and receiving. This can be done in the Web Interface by reviewing the "**Clock** → **Information** → **GXL Clock** → **AtomiChron** → **Info**" tab. The entry "**LBAND SV Information available**" should show *Yes* to indicate that it has locked onto the Inmarsat satellites used for delivery of AtomiChron® data.

Ensure that the antenna is not installed in a location where it might be exposed to interference from other L-band emissions or signal reflections (particularly in built-up areas).

Once you are sure that the clock is capable of receiving the signal reliably, please contact Meinberg's Technical Support team at *techsupport@meinberg.de* in order to schedule another activation signal transmission.

Ensuring the Timely Renewal of Your AtomiChron® License

Atomichron License Expired	Error	Last: Thu Jan 18 11:30:42 2024	☐	☐	☐	☐	☐	☐
Atomichron License Expiration Warning	Warning	Last Event: Sun Jan 21 00:00:28 2024	☐	☐	☐	☐	☐	☐
Atomichron receiver report spoofing detected	Error	Last Event: Thu Jan 18 11:30:42 2024	☐	☐	☐	☐	☐	☐
Atomichron receiver report spoofing stopped	Info		☐	☐	☐	☐	☐	☐

Illustration: Configuration of notifications to ensure that the AtomiChron® license does not expire

An AtomiChron® subscription is not automatically renewed. A renewal must therefore be explicitly purchased from Meinberg.

Please ensure that your AtomiChron® license is renewed in good time to ensure that the service is not interrupted by expiry of the license. While Meinberg will endeavor to contact you to remind you of the upcoming expiry, we cannot guarantee that we will be able to contact the relevant person responsible.

Therefore, Meinberg recommends that you also:

- set some kind of organizational reminder (calendar software or similar) to ensure that you are reminded of the need to renew your AtomiChron® license,
- configure your LTOS notifications to alert you (via email, SNMP, etc.) when your AtomiChron® license is about to expire (in 28 days) and when it has expired.

Further information on configuring notifications can be found in the Notification chapter.

10.1.10.3 MRS Status

Here the states of the reference inputs are shown:

Priority: Arrangement of the time source according to your prioritization.

Source: Type of reference source.

Status: No Connection,
No signal → the reference source is not available.

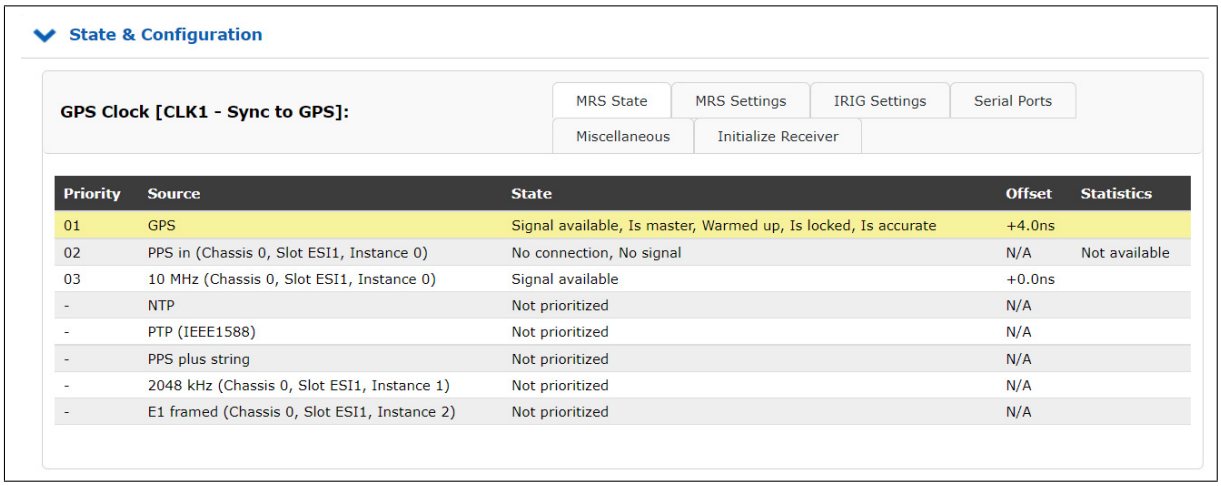
Signal available → the reference source is available.
Is master → the reference source is used to synchronize the system.
Is locked → the system synchronizes itself to the reference source.
Is accurate → Basic accuracy of synchronization reached.

Offset: Time difference of the reference clock to the specified time source.

Statistics: 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	State	Offset	Statistics
01	GPS	Signal available, Is master, Warmed up, Is locked, Is accurate	+4.0ns	
02	PPS in (Chassis 0, Slot ESI1, Instance 0)	No connection, No signal	N/A	Not available
03	10 MHz (Chassis 0, Slot ESI1, Instance 0)	Signal available	+0.0ns	
-	NTP	Not prioritized	N/A	
-	PTP (IEEE1588)	Not prioritized	N/A	
-	PPS plus string	Not prioritized	N/A	
-	2048 kHz (Chassis 0, Slot ESI1, Instance 1)	Not prioritized	N/A	
-	E1 framed (Chassis 0, Slot ESI1, Instance 2)	Not prioritized	N/A	

Figure: An example of available reference signals in the priority order.

The table below shows the possible reference sources - the availability depends on the hardware configuration of the system.

Signal	**provided by**
GPS GNSS	built-in GPS receiver built-in GNS receiver
PPS plus string	external signal generator
NTP	external NTP Server
PTP (IEEE1588) SyncE	HPS / TSU Time Stamp Module HPS Time Stamp Module
E1 framed PPS In Fixed Freq.	IMS ESI - Input module for 2.048 MHz, 2.048 MBit/s, 1PPS and variable frequencies
IRIG PPS in 10 MHz	IMS MRI - IRIG, 1PPS, 10 MHz input module
Video In LTC In Freq. In PPS In	IMS VSI - Video Signal Input Module

10.1.10.4 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.

10.1.10.5 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

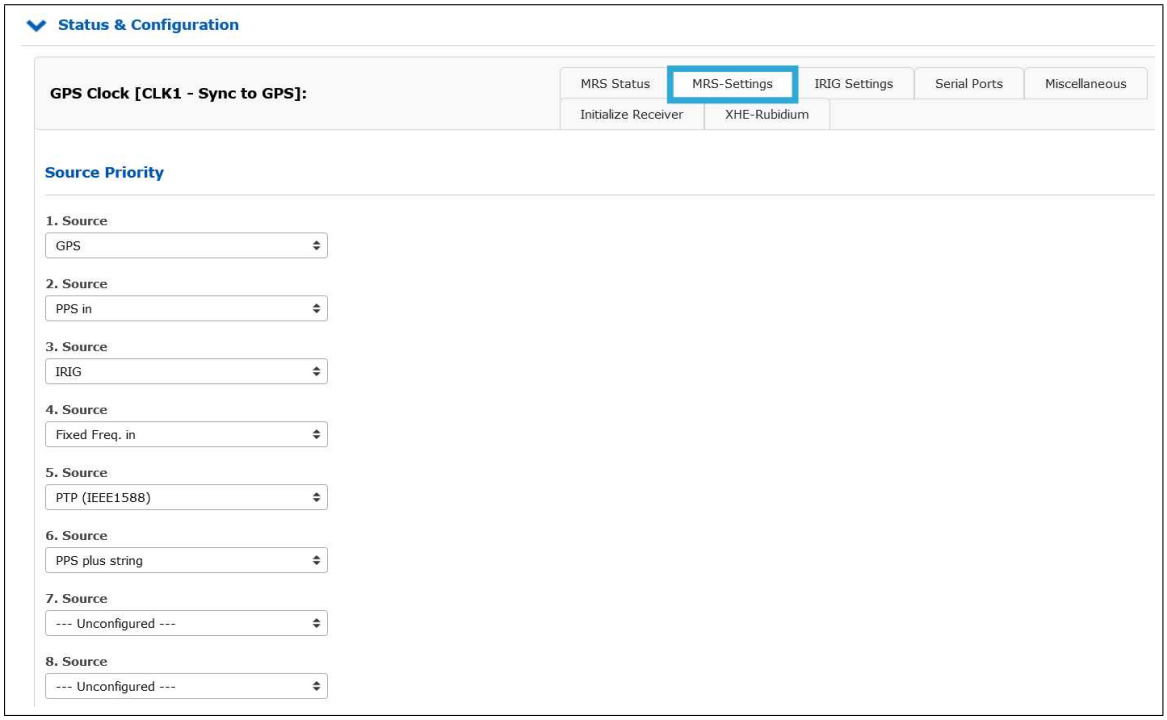


Figure: Configuration example of reference signals in a descending order.

PTP as reference signal

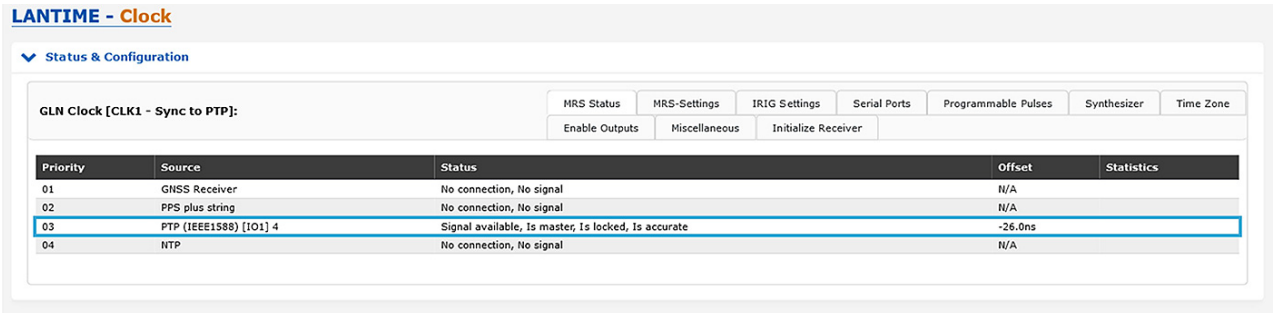


Figure: IMS-HPS100 on IO1 as PTP reference

HPS modules (with FW ≥1.4.1) can operate in all I/O slots as PTP master or slave

An IMS-HPS100 module can be used in slave mode on all slots (MRI, ESI and I/O) of an IMS system. This allows it to act as a high-precision PTP reference input for the system (see figure).

A slave is selected by the BMCA procedure (Best Master Clock Algorithm) if more than one HPS100 module is used in a system and in slave mode, which is then listed in the MRS priority list (see figure). As the master-reference, this slave sends its correction data to the clocks installed in the system (CLK1 and CLK2).

Information:

This function is only possible with the HPS100. The TSU GbE does not support this function.

In case of a redundant receiver configuration and the installation of the HPS100 in an **ESI/MRI slot**, the master/slave mode only works for the assigned clock. If the receiver **CLK1** is to be synchronized via an HPS100, then this must either be in an IO slot or installed in the **MRI1/ESI1 slot**.

10.1.10.6 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.

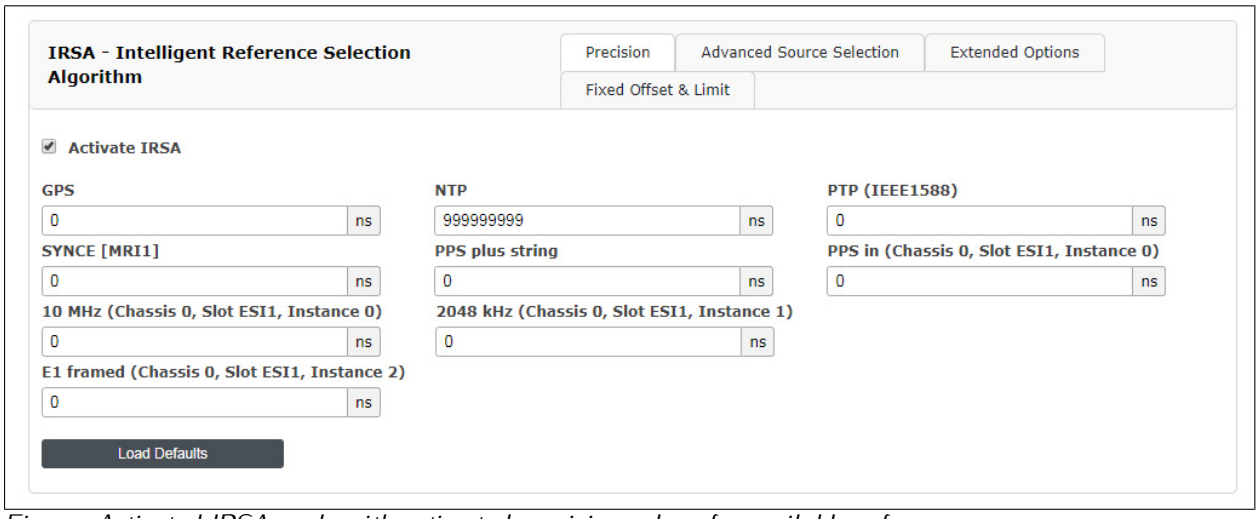


Figure: Activated IRSA mode with estimated precision values for available references.

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

10.1.10.7 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 Rubidum 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:

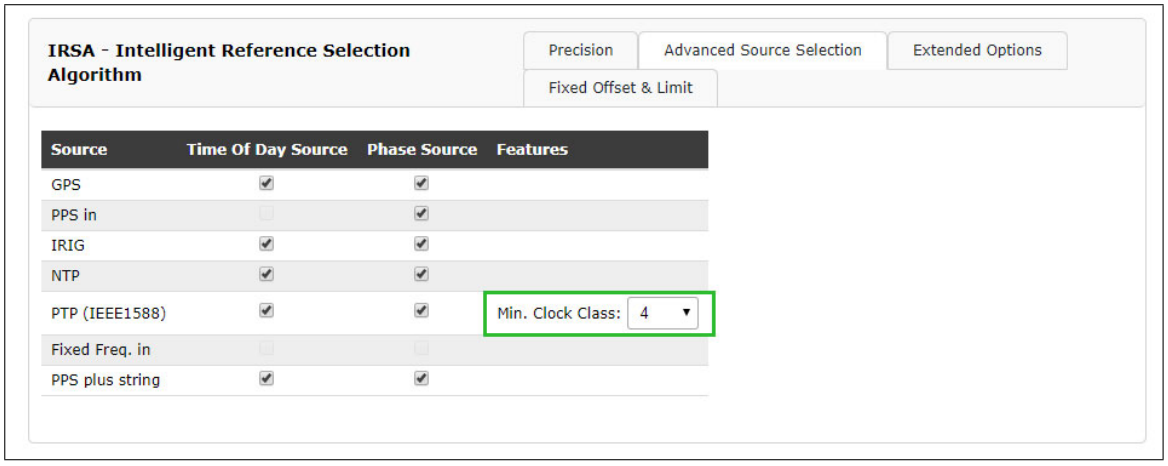


Figure: An example for a mixed combination of ToD and Phase source for given reference signals.

PTP Min. Clock Class

The MRS system should only use a PTP master to synchronize the clock if the desired clock class is given. It should be prevented that the slave remains synchronized to a bad master, although another source is available.

10.1.10.8 Extended Options

The Trusted Source (TRS) feature is a powerful tool to protect the GNSS[1] 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".

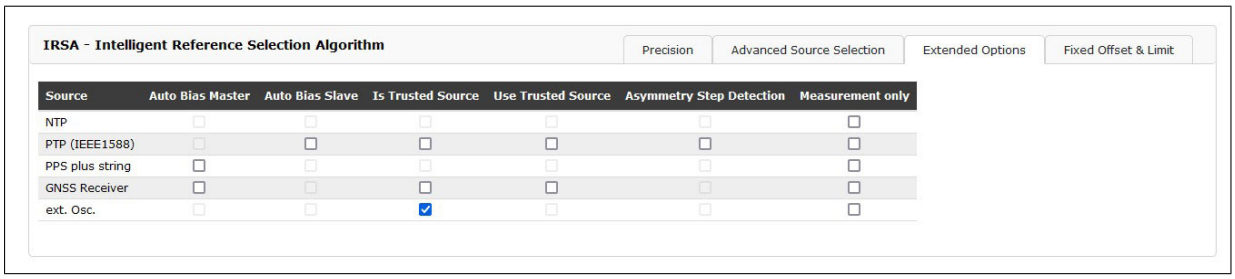


Figure: An example of a Trusted Source mode of operation with an external rubidium.

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.

[1] GPS / GNSS: The Trusted Source (TRS) feature will only work with GPS and GNS 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
```

Measurement Only
If the field is activated, this source is only used for measurements but never as a synchronisation source.

10.1.10.9 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 → Notofication Event → MRS Limit Exceed".

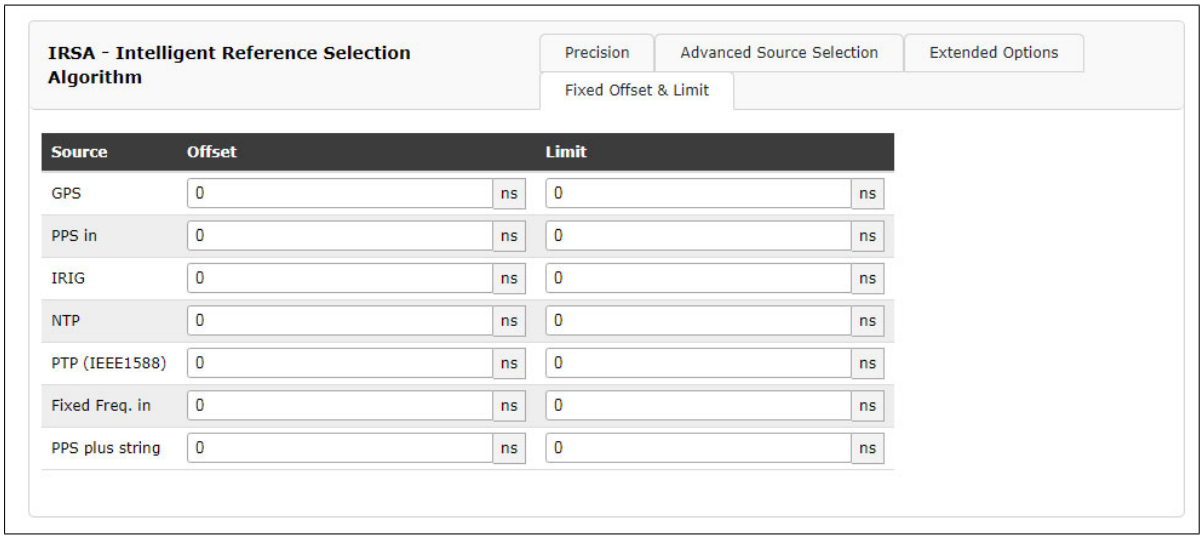
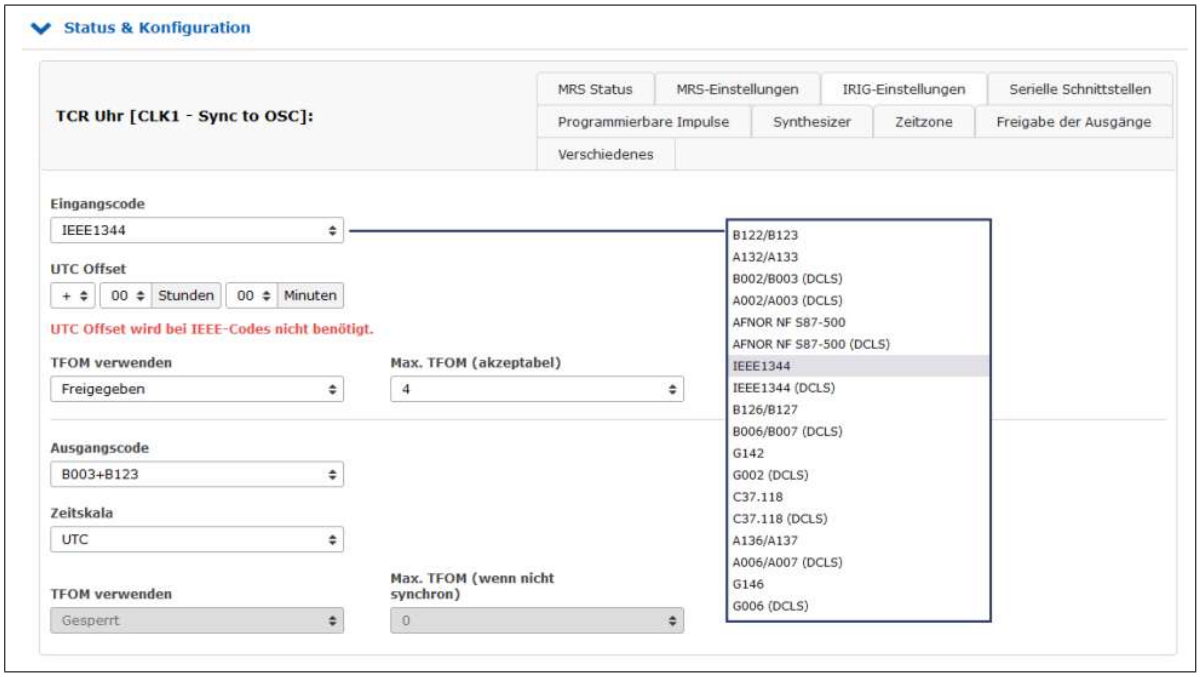


Figure: Configuration dialog for known offsets and limits.

10.1.10.10 IRIG Configuration

This menu allows you to configure the input and/or output time codes (TCs) depending on the modules installed in your system. Compatible modules include the IMS-BPE output modules; these are "passive" modules that pass through the time and synchronization signals generated by the reference clock.



Configuring Signal Output

1. Open the "**Clock**" tab.

2. Open the section "**State & Configuration**" by clicking on it.

3. *If your LANTIME system has a switchover module such as an RSC module:*
   Click on the tab "**IRIG Settings**" under the section "**Switch Card**".

   If your LANTIME system only has one reference clock (i.e. with an SPT module):
   Open the section "**CLK1**" (or "**CLK2**" if the clock module is located there and click on the tab "**IRIG Settings**"

4. Select the tab "**IRIG Settings**".

5. Configure the desired IRIG input or output code. Please refer to the manual of your IMS system for more detailed information.

IRIG

Example: B002/B003

B002 100 pps, PWM DC signal, no carrier, BCD time-of-year

B003 100 pps, PWM DC signal, no carrier, BCD time-of-year, SBS time-of-day with second of the day (0....86400)

AFNOR NF S87-500 AFNOR NF S87-500 A French standardized time code, similar to IRIG time code. Code standardized by NFS-87500, 100 pps, AM sine-wave signal, 1 kHz carrier, BCD time-of-year, full date, SBS time-of-day

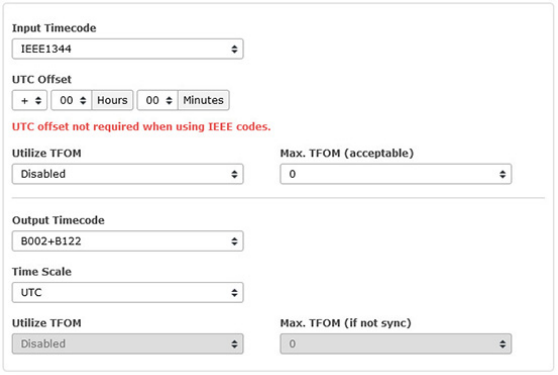
IEEE1344 Code standardized by IEEE1344-1995, 100 pps, AM sine-wave signal, 1 kHz carrier, BCD time-of-year, SBS time-of-day, IEEE1344 extensions for date, time zone, daylight saving time, and leap seconds in Control Functions segment

Input Code:
The appropriate time code must first be set so that the time code signal received from the reference source can be properly decoded.

UTC Offset:
If the incoming time code has a constant offset relative to UTC, this offset must be set here so that the clock can convert the incoming time back into UTC accordingly.

IRIG TFOM

If a TCR module is installed, the TFOM parameters will be enabled and configurable under the "**IRIG Settings**" tab when IEEE1344 or C37.118 is set as the input time code.



The control bits in the format-specific extensions of these time codes include four bits for a 'Time Figure of Merit' value (TFOM) that enables the expected accuracy of the time from the reference system to be conveyed to the receiver system.

If the system is in free-run mode, the TFOM value can be calculated on the basis of the expected oscillator drift and free-run time. If the system is synchronized to the reference source, the TFOM value is set to zero. If the reference system provides no information for the TFOM values, the TFOM is set to 15 (undefined).

Utilize TFOM

Enabled TFOM is applied
Disabled TFOM is ignored

Max. TFOM (acceptable):

If this signal (e.g., C37.118) is used as a reference source, the system can be configured via the Web Interface to have it synchronize with that source only if a defined "Max. TFOM" value is not exceeded. If the TFOM exceeds this defined value, the reference signal will no longer be accepted as a valid reference source and the system will switch to the next source in the priority list or, if none is available, to free-run mode.

TFOM	Estimated Time Error (ETE)	TFOM	Estimated Time Error (ETE)
0*	TQ_LOCKED_TO_UTC	8	ETE < 10 ms
1	ETE < 1 ns	9	ETE < 100 ms
2	ETE < 10 ns	10	ETE < 1 s
3	ETE < 100 ns	11	ETE < 10 s
4	ETE < 1 μs	12	ETE < 100 s
5	ETE < 10 μs	13	ETE < 1000 s
6	ETE < 100 μs	14	ETE < 10000 s
7	ETE < 1 ms	15	ETE undefined

Output timecode:
If the system has a channel for outputting time codes, the parameters for these can be configured in much the same way as for the input time codes.

Information:

In systems with reference clock redundancy, the IRIG output is configured via the "**Switch Card**" menu.

Time Scale:
The selected time code can be output with UTC or in local time. If "*LOCAL TIME*" is selected, the output is based on the configured time zone.

Utilize TFOM:

Enabled TFOM is applied
Disabled TFOM is ignored (TFOM is set to 0)

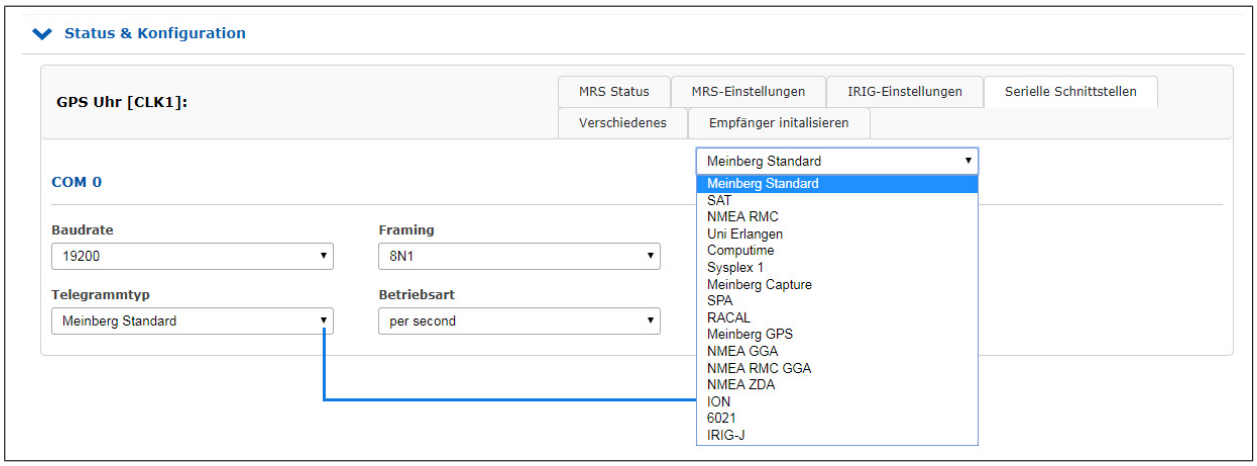
Information:

If the module is in Simulation Mode, the TFOM will be automatically set to zero.

Max. TFOM (if not sync)
If the system also has an IRIG output (e.g., BPE-2000), a "Max. TFOM" can also be configured here to limit the output TFOM. The output signal will continue to be provided, but the TFOM integrated into the IRIG code will not be increased beyond this value.

10.1.10.11 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: Meinberg Standard, SAT, NMEA RMC, Uni Erlangen, Computime, Sysplex 1, Meinberg Capture, SPA, RACAL, Meinberg GPS, NMEA GGA, NMEA RMC GGA, NMEA ZDA, ION, 6021, IRIG-J

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.

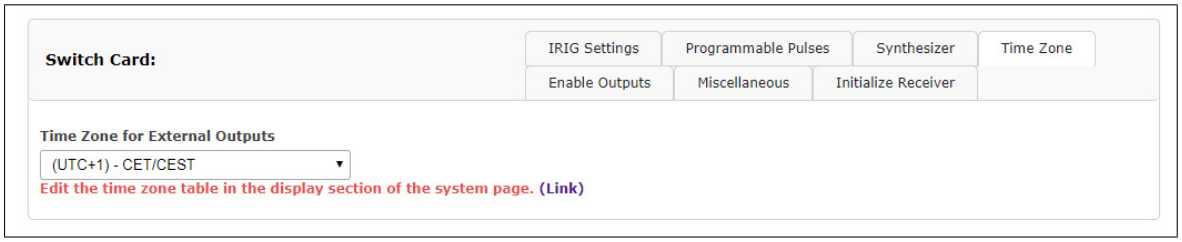
Two operating modes are available for the output of the capture time stamps, "on request ? Only" and "automatically".

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.

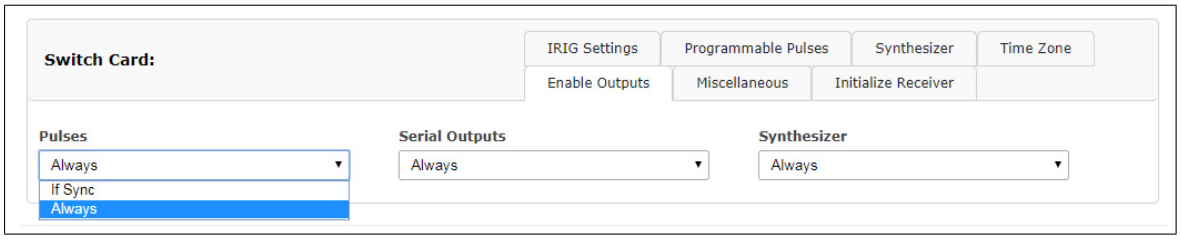
10.1.10.12 Time Zone

In this menu, you can configure the time zones (offsets) for the output signals (IRIG, serial interface, programmable pulses) of the reference clock.



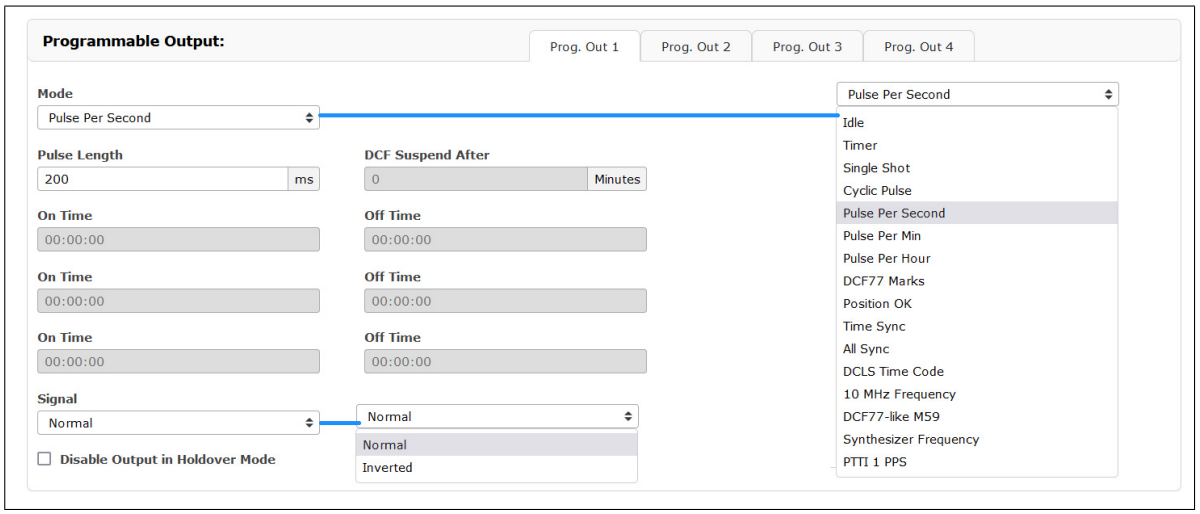
The data of the time zone are used from the time zone table (see chapter 10.1.9.15 System → Display).

10.1.10.13 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.

10.1.10.14 Programmable Pulses



Configuration of Pulse Outputs

1. Open the "Clock" tab to configure the output of your System.

2. Open the "State & Configuration" section by clicking on it.

3. *If your LANTIME system has a switch-over module (e.g., RSC module),*
   click on the "Programmable Pulses" tab in the "Switch Card" section.

   If your LANTIME system has only one reference clock:
   Click on the "Programmable Pulses" tab in the "CLK1" section (or "CLK2" if your clock module is installed there).

4. Four tabs labeled "Prog. Out 1–4" will now be displayed. Select the appropriate tab.

5. Configure the signal output as desired.

Mode: Output signal configuration.
(See also → Chapter 13.5, "Overview of Programmable Signals")

Pulse length (ms): Pulse length configuration.

Cycle: For "Cycle Pulse" mode; allows an interval to be configured in *hh:mm:ss*.

Time: For "Single Shot" mode; allows the time for the pulse to be configured in *hh:mm:ss*.

DCF Suspend After (min): For "DCF77 Marks" mode; allows a switch-off time to be configured for the output port to ensure that DCF markets are not output if the reference clock is not synchronized.

On / Off Time: For "Timer" mode; determines the start and stop times in *hh:mm:ss*.

Signal: Specifies whether the output signal is "active high" or "active low".

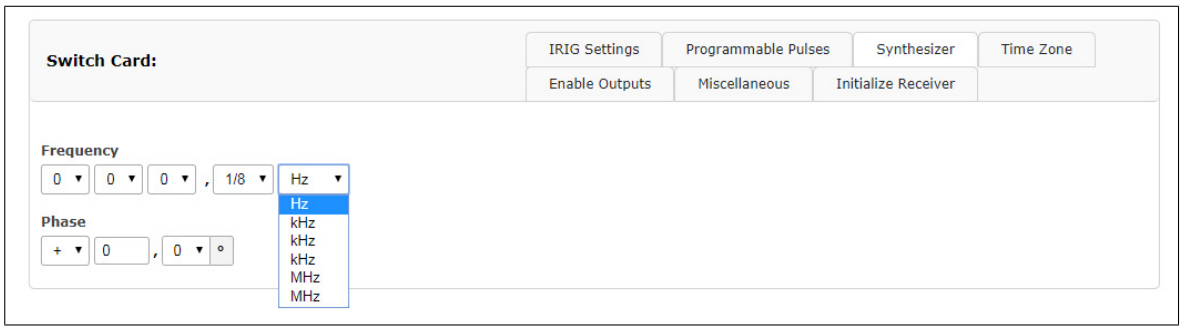
Disable Output in Holdover Mode: If enabled, the output signal will be disabled immediately if the clock loses synchronization.

Information:

The "Enable Outputs" tab must have the "If Sync" option enabled to allow the outputs to be disabled in Holdover Mode.

10.1.10.15 Synthesizer

The output frequency and phase of the integrated synthesizer can be set here.

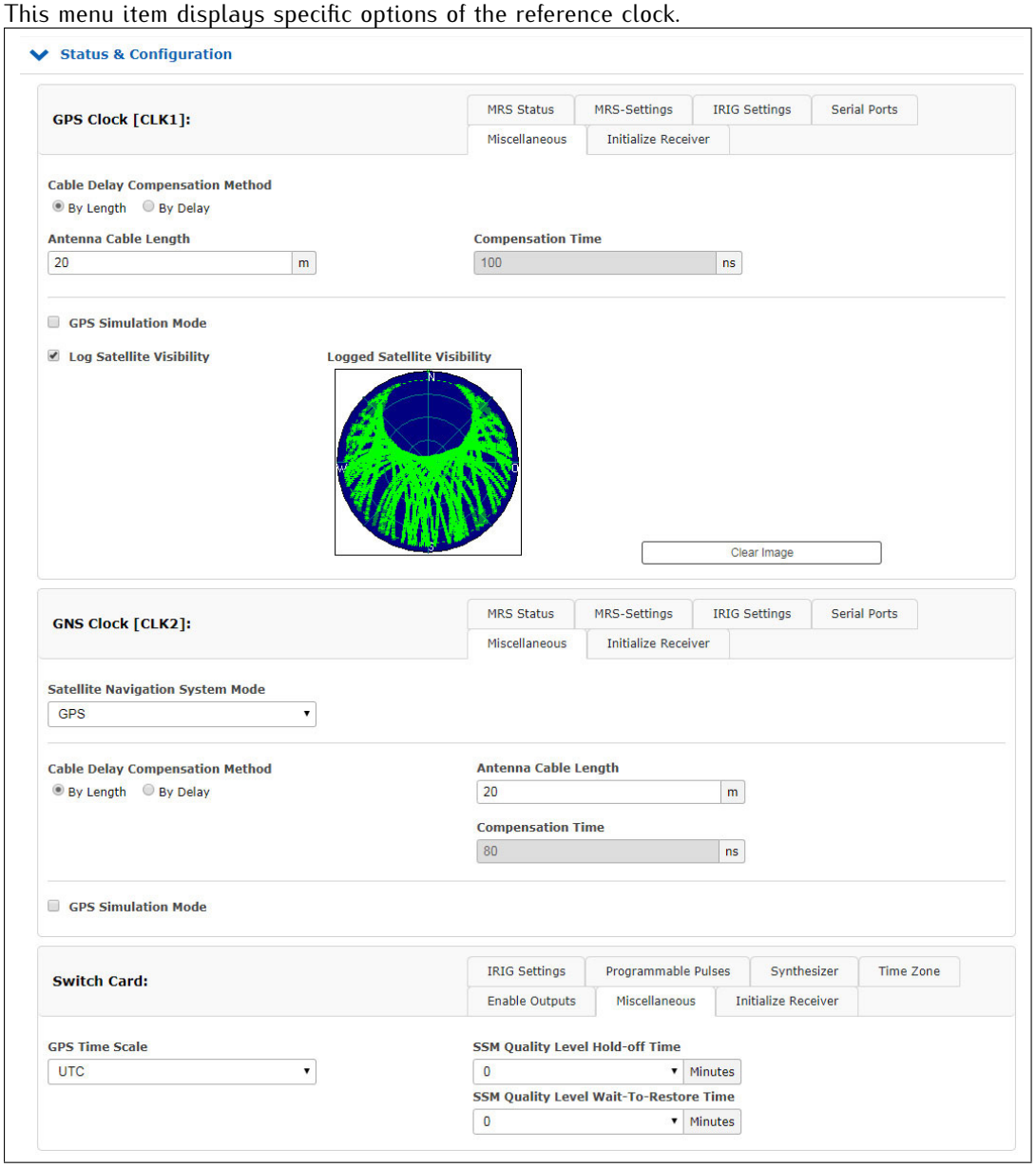


Frequency: Frequencies from 1/3 Hz up to 10 MHz can be set by entering four digits and a frequency range. By entering the frequency 0 Hz, the synthesizer can be switched off.

Phase: With phase you can enter the phase position of the set frequency in the range -180° to +180° 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.

10.1.10.16 Miscellaneous

This menu item displays specific options of the reference clock.



Antenna Cable Length (m):
The signal propagation time of the antenna cable can be compensated by this value. The received time signal is delayed by approx 5ns/m when using RG58U and 4ns/m when using H155 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 500m.

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 is not 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.

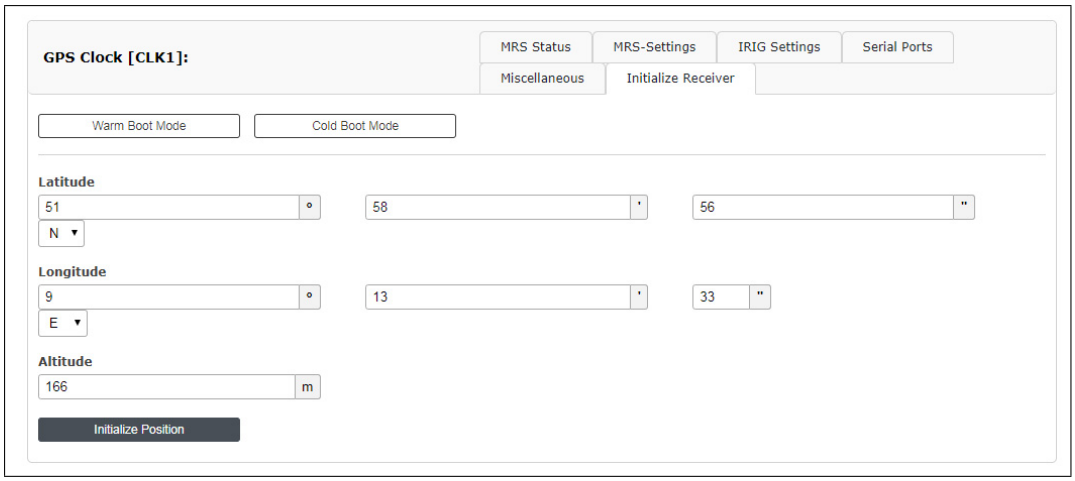
The following combinations can be selected and received simultaneously:

GNS Receiver	GNS-UC Receiver	GNM-Receiver
GPS only	GPS only	GPS
GLONASS only	Galileo only	GLONASS
Galileo only	GPS/Galileo	Galileo
BeiDou only		BeiDou
GPS/GLONASS		(All available systems can
GPS/Galileo		be received simultaneously)
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.

10.1.10.17 Initialize Receiver



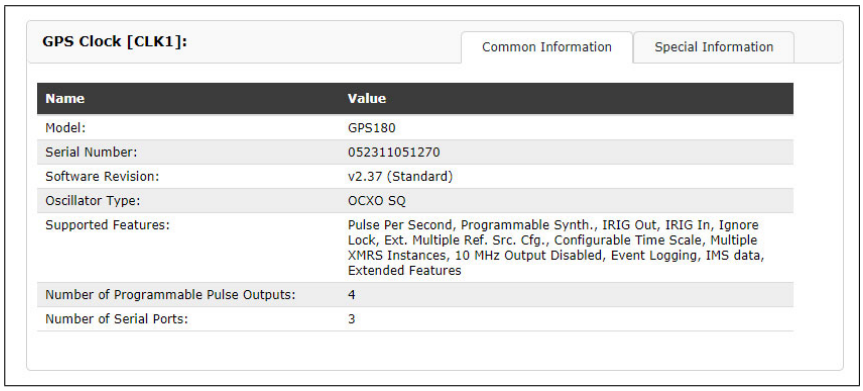
Warm Boot Mode only for GNSS receiver:
This menu allows the user to switch the receiver to WARMBOOT MODE. This may be necessary if the satellite data in the battery-buffered memory is too old, or if the device is operated at a location that is several hundred kilometers away from the last operating location, 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.

10.1.10.18 Receiver Information



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.

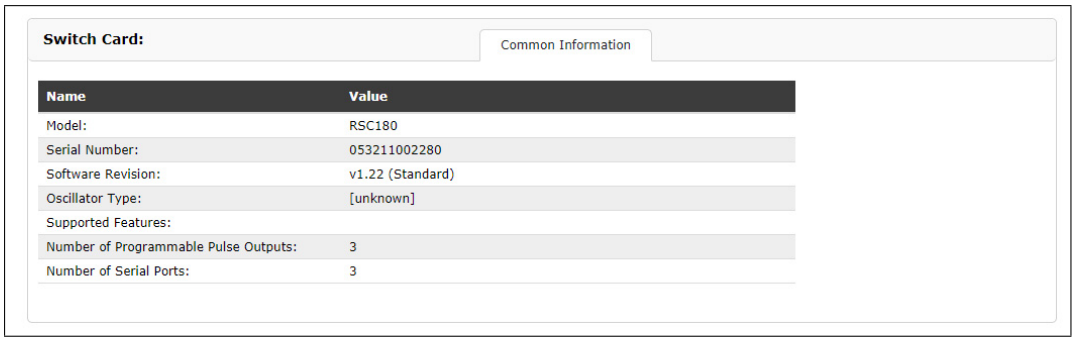
So the number of **good** satellites can never exceed the number of satellites in view, but it can be significantly less if the antenna has been installed in a location with limited view to the sky. In worst case this can lead to limited accuracy, or only temporary synchronization.

10.1.10.19 Switch Card

The RSC (SCU) switch card is an automatic multiplexer for redundant systems with two Meinberg receivers. 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.

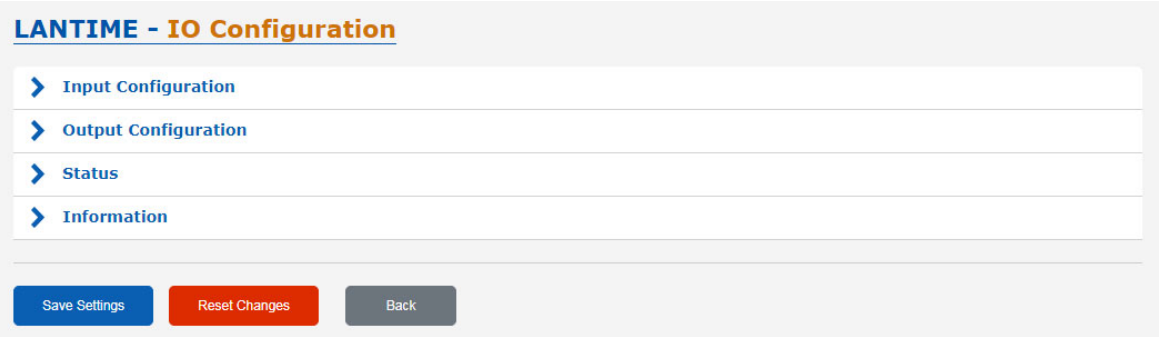
10.1.10.20 Receiver Information Switch Card



This menu item lists all the important information and options of the switch card.

10.1.11 I/O Configuration

This menu is available on IMS systems only. Input and output modules can be configured here.



10.1.11.1 Input Configuration

10.1.11.2 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 10.1.10 - "Web GUI → Clock → MRS Settings".

10.1.11.3 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 SSM/BOC) or clock inputs.

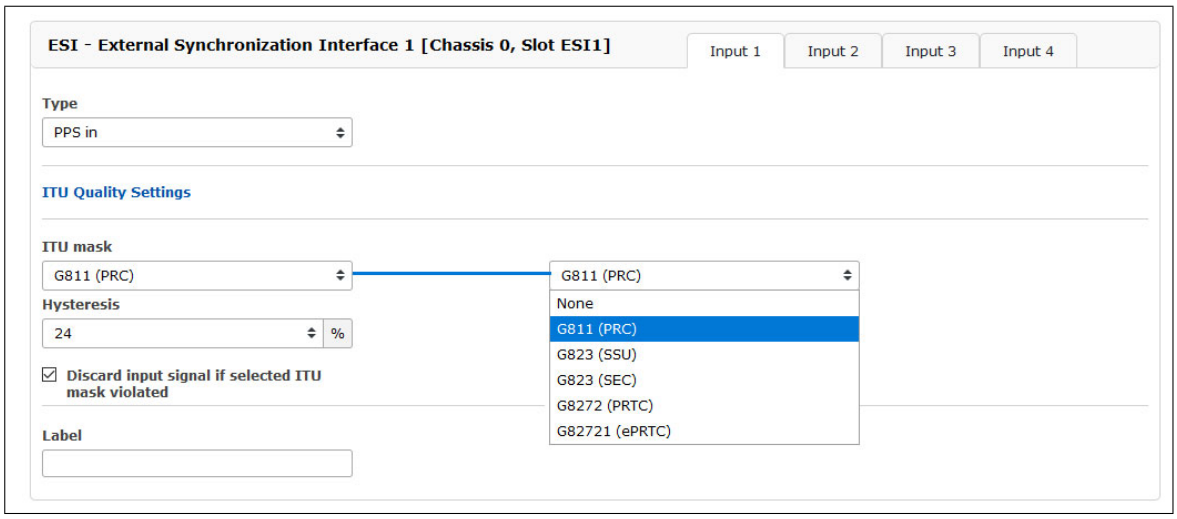
The clock inputs are configurable (1 kHz - 20 MHz). Furthermore a 1PPS input is provided as well.

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 (1 kHz - 20 MHz) unframed, BNC
- var. frequencies (1 kHz - 20 MHz) unframed, RJ45
- BITS E1/T1 framed, RJ45

Hint:
If the specified frequency range is exceeded, an error message is displayed in the web interface and the entered value is not accepted in this case.

Input 1: The input 1 is dedicated to 1PPS pulse synchronization.



Signal Type – PPS in

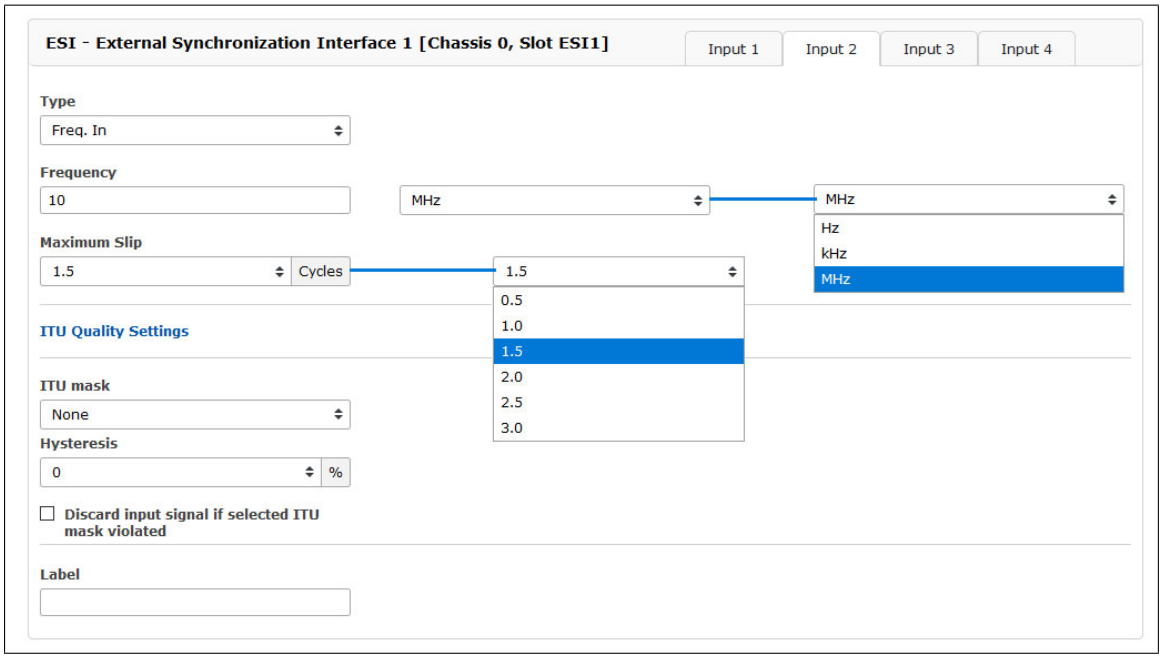
ITU Quality Settings
(settings can be made individually for inputs 1 to 4)

ITU Mask.
Predefined masks can be selected, in which quality requirements regarding jitter and wander of the input signals are defined. If the default values are exceeded, the affected input port is switched off.

Hysteresis.
To avoid that signal inputs are continuously switched off and back on when exceeding the ITU mask, a hysteresis for switching on again can be defined. The signal input port is only reactivated when all the selected mask points are below the defined percentage value's limits.

Discard input signal if selected ITU mask violated.
Only if this box is selected, the input signal is switched off when exceeding an ITU mask.

Input 2: The input 2 accepts as input either 2048/1544 kHz frequency or configurable frequency in range between 1 kHz and 20 MHz, also 1.544kHz if required.



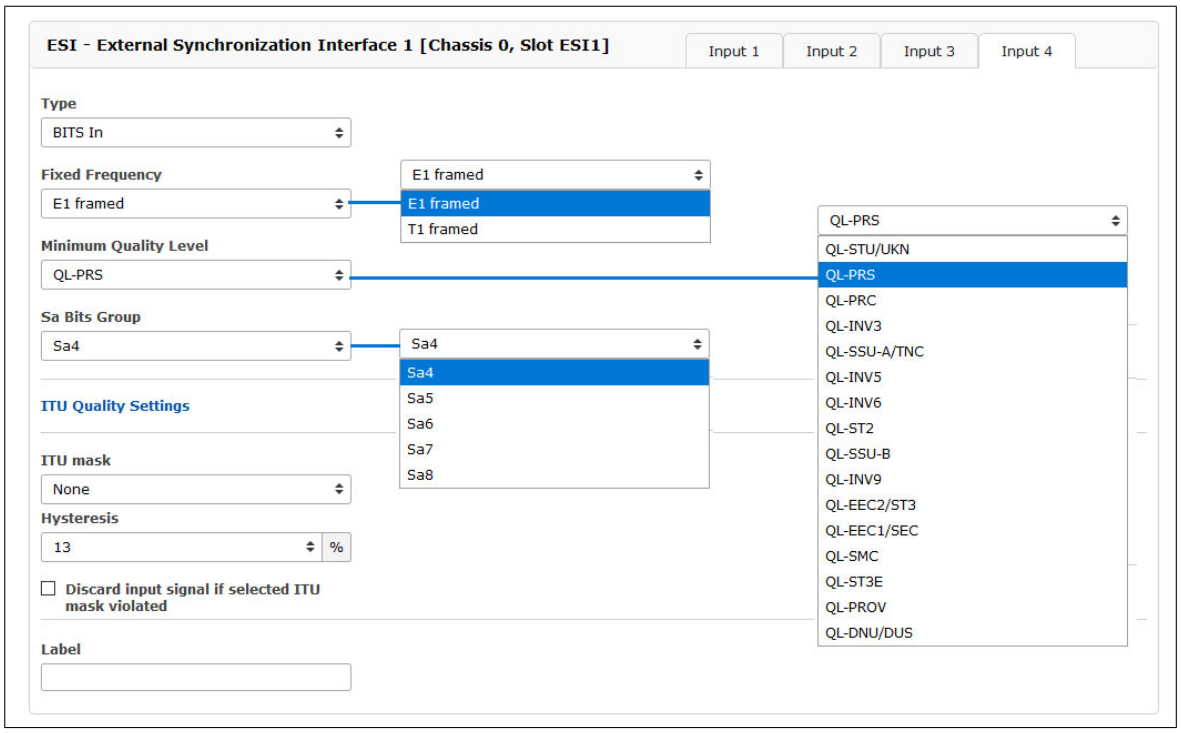
Type: Frequency input

Frequency: 1 kHz - 20 MHz of input signal, 10 MHz is set as default.

Maximum Slip: A discontinuity of an integer number of cycles in the measured carrier phase resulting from a remporary 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.



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

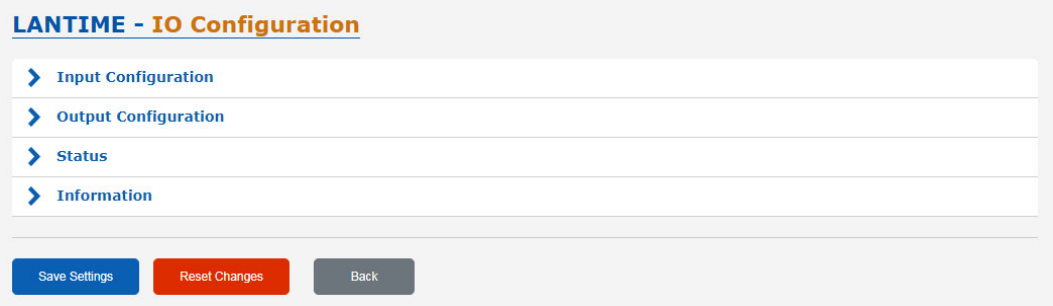
acceptable as input signal. If clock reports a lower quality level than the configured minimum SSM level the system will not use it for synchronization.

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.

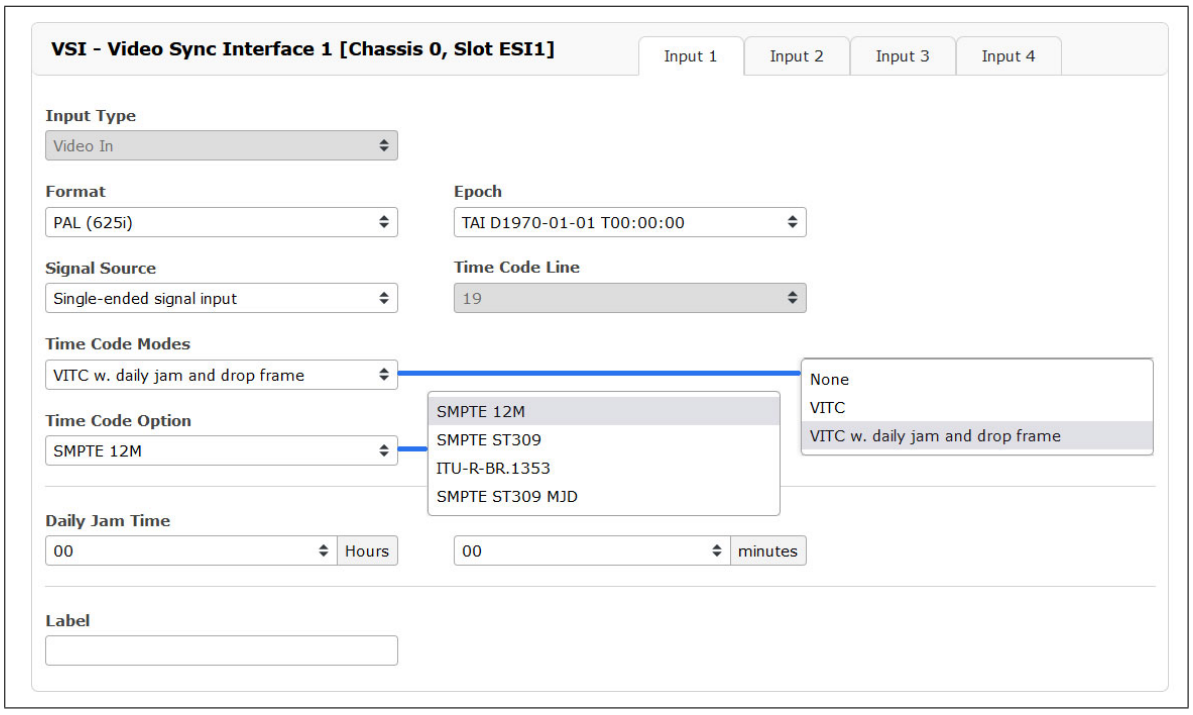
Sa Bits Group
Here you can select between the Sa4 to Sa8 bit group to choose the location for SSM quality bits.

10.1.11.4 VSI Configuration via the Web Interface

VSI - Video Signal Input References
Menü "IO Config → Input Configuration → VSI-Karte"



Video Sync Interface: configurable Inputs



Input 1: Video Sync In

Format: PAL 625i

Epoch: TAI

Signal Source: Single-ended signal input

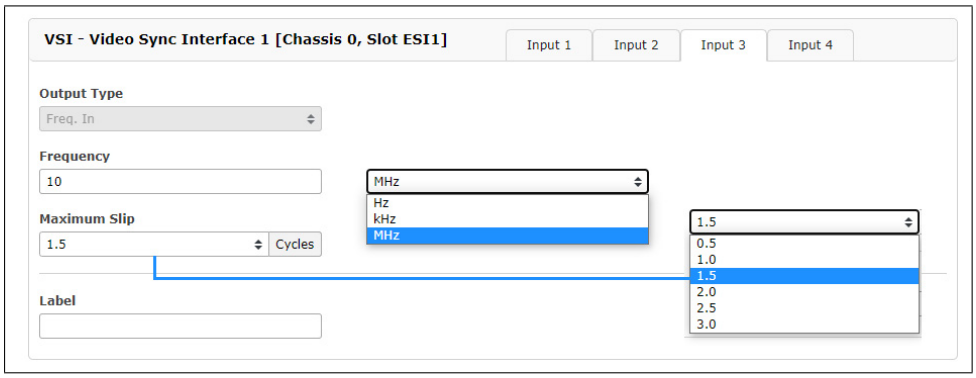
Time Code Modes: VITC

Time Code Line: 6 - 22

Input 2: LTC In

Type: LTC 25 FPS (Frames per Second)

Daily Jam Time: Time of Day (hh:ii)



Input 3: Word Clk In

Port Type: GPIO (General Purpose Input Output)

Direction: Input

Operation Mode: Always enabled

Input 4: PPS In

Pulse length: $\geq 5\mu$s, active high

10.1.11.5 Output Configuration

10.1.11.6 IMS BPE

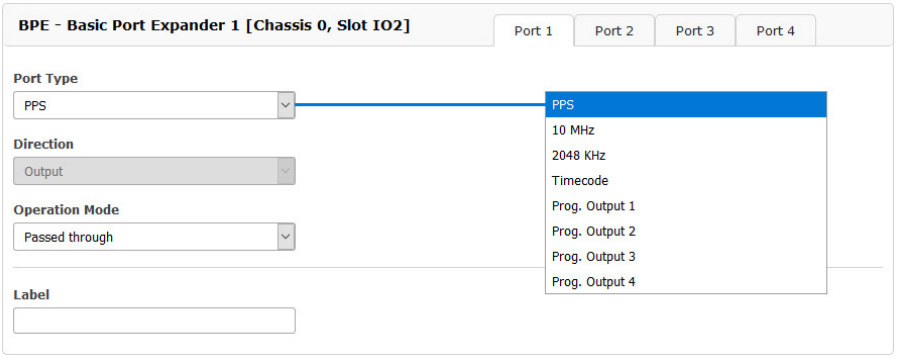
BPE (Basic Port Expansion)
The standard BPE is a passive module and is one of the IMS output modules. When ordering, the customer chooses between different physical connections and signal levels which are generated by the reference clock.

The BPE is pre-configured with the following signals:

- 1PPS, 10 MHz TTL
- 2048 kHz
- Programmable Pulses, provided by clock module (also see ➜ Chapter 13.5, "Overview of Programmable Signals")
- IRIG DCLS+AM (B, AFNOR, IEEE1344 / C37.118)
- ...

There are no other configration settings for a standard BPE card in the I/O Config menu. For further detailed settings on output signals of the BPE card please proceed to the Clock Configuration Chapter 10.1.10.

BPE8000 series: switchable output signals



The BPE8000 series with eight different BNC and ST connector combinations, offers freely configurable output signals via the web interface of an IMS system. An electronically controlled switch (multiplexer) on the module board allows the selection of the signals to be distributed by the receiver module via the backplane.

10.1.11.7 IMS CPE

This module consists of a half-size standard controller card (Back-End) and a connected port expander card (Front-End), allowing a large variety of available and programmable output signals and physical connectors, including various electrical and optical interfaces.

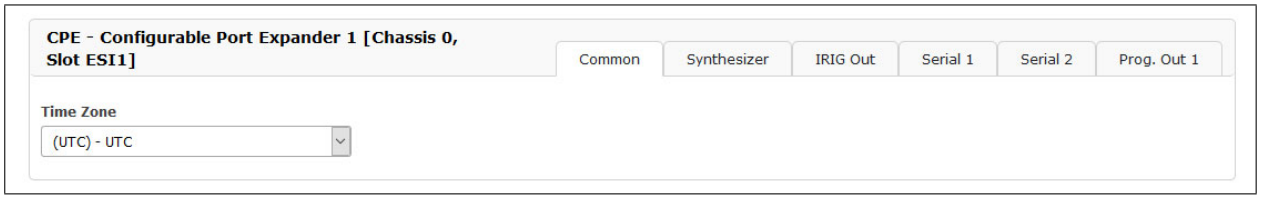
The main menu of the CPE provides access to specific submenus where the available output signals can be configured.

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, etc.
- Cyclic Pulses; DCF77 Mark, Sync Status
- Serial Timestrings (RS232 or RS 422 / 485)

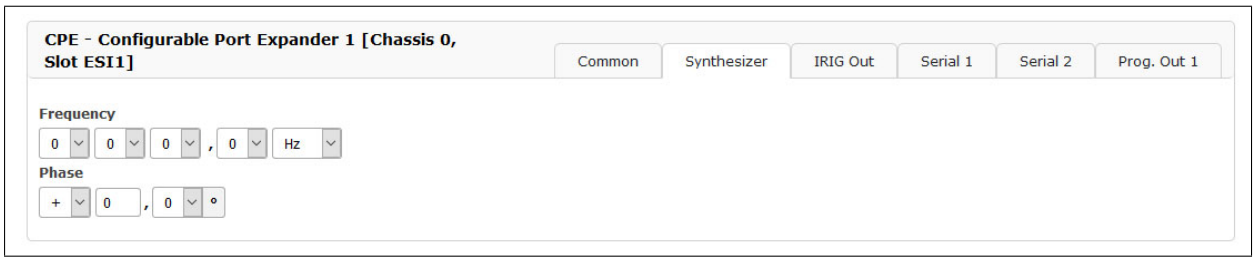
Submenus

Common:



Time Zone Choose local timezone

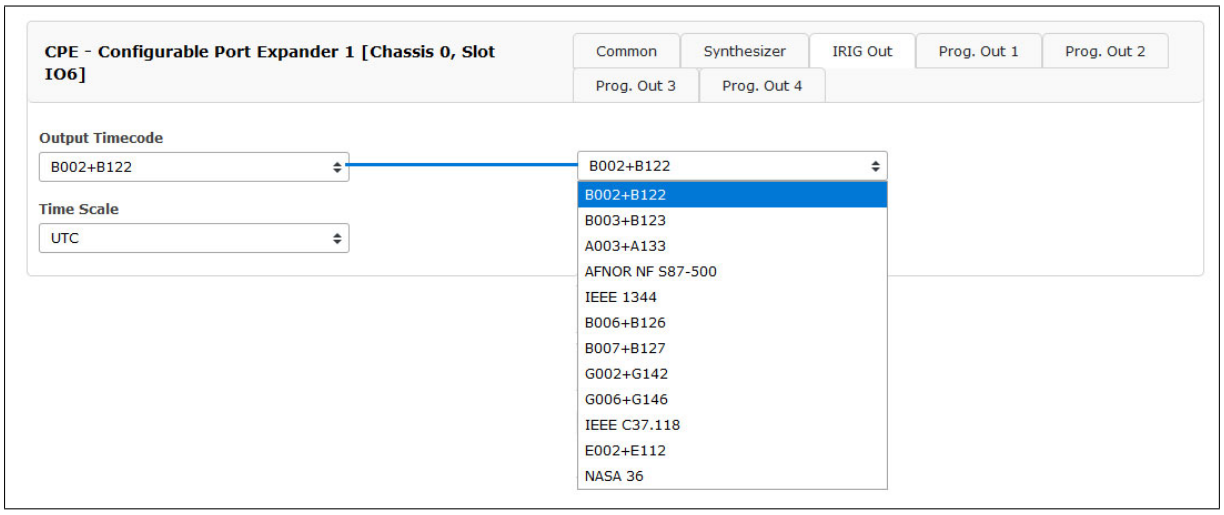
Submenu Synthesizer:



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

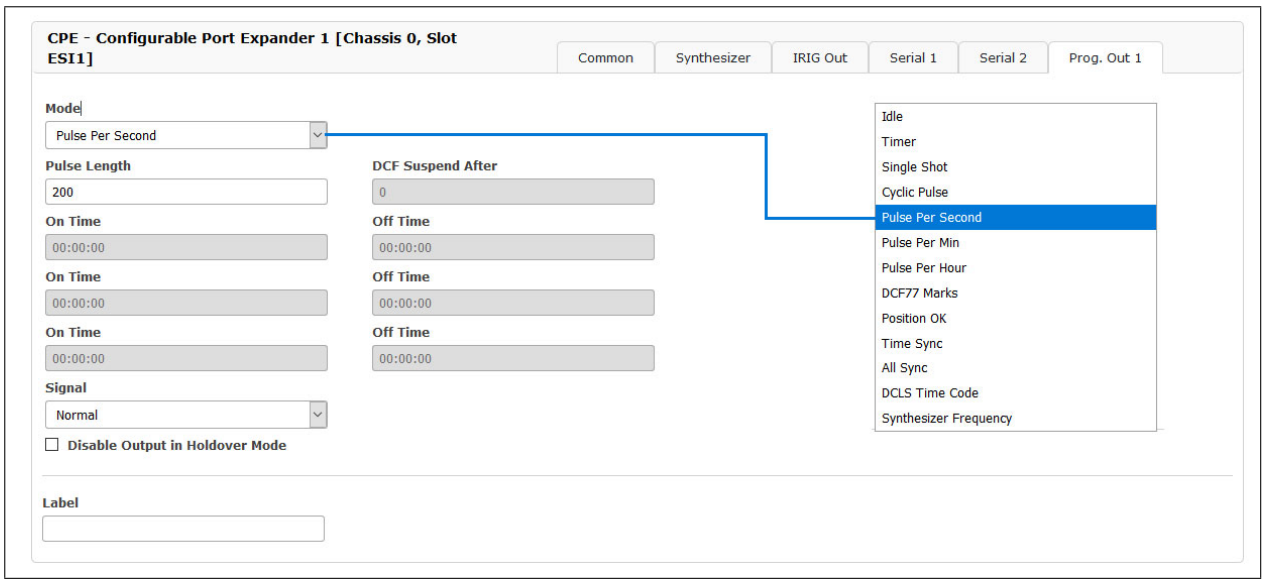


IRIG Output Code Output code that is selected for the CPE.

Time Scale Select the time scale (UTC or local time) which forms the time base for signals with time information (e.g. time code signals).

The individual time code formats are explained in more detail in the → Chapter 13.4, "Time Code Formats".

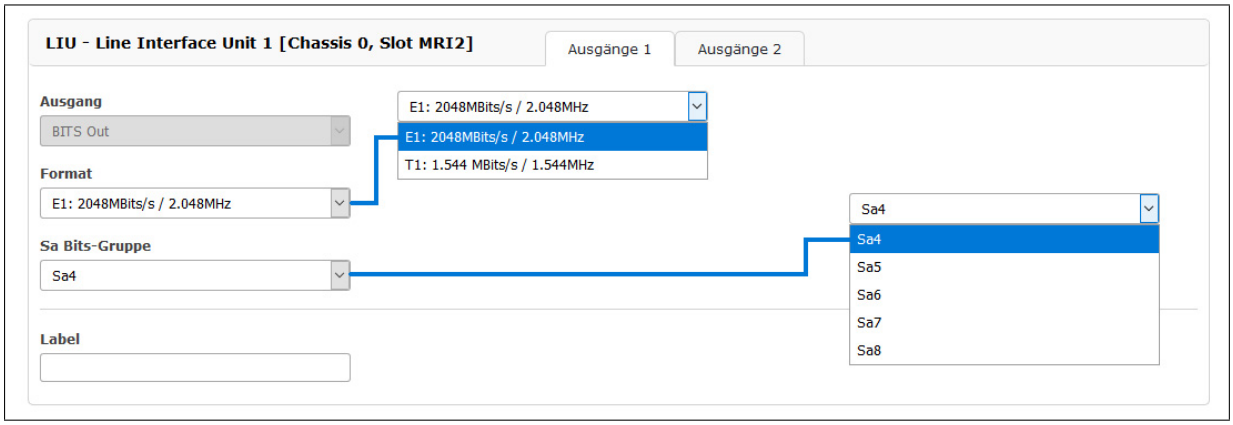
Programmable Outputs



The individual programmable output signales are explained in more detail in the
→ Chapter 13.5, “Overview of Programmable Signals”

10.1.11.8 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.

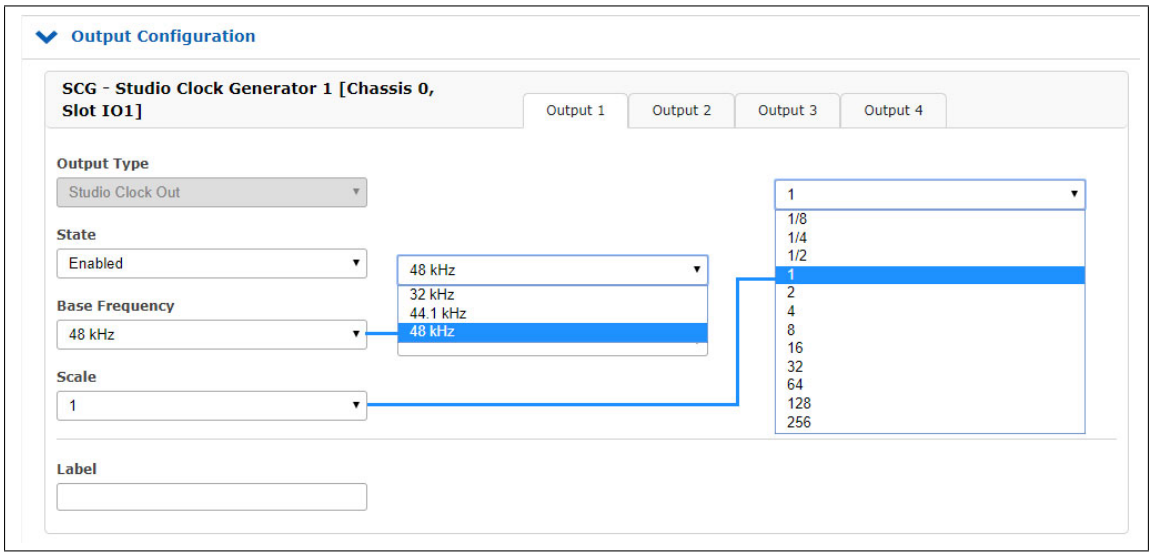
Sa Bits

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.

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.

10.1.11.9 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

Output Type Studio Clock Out (Word Clock) or Digital Audio Out (DARS)

State on or off

Base Frequency 32kHz, 44.1kHz, 48kHz

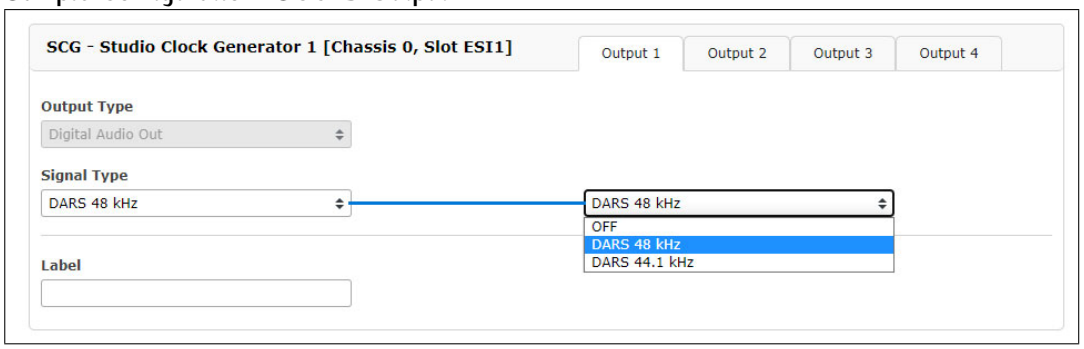
Scale possible scales depends on base frequency
choose a base frequency and a scale to get the right frequency at output x

Example: Output 3 state Enabled base 48kHz, scale 1/8
Output 3 = Base-Frequency * Scale
48kHz * 1/8 = 6kHz on output 3

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.

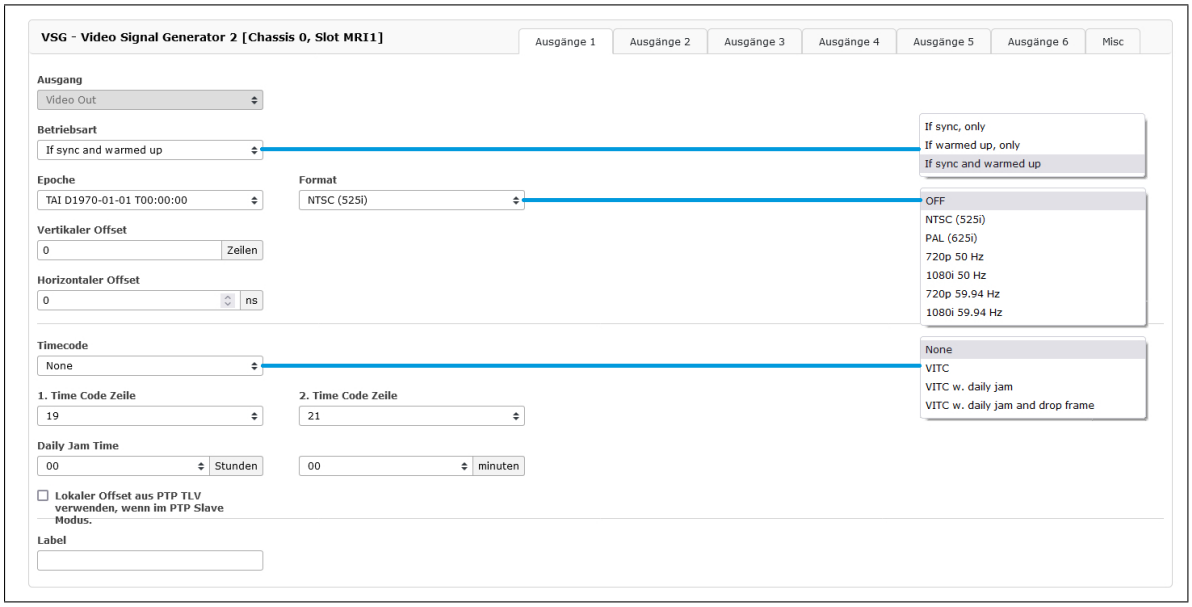
10.1.11.10 IMS - VSG

The VSG modules provide video signal reference signals for studio equipment.

The IMS-VSG181 offers four BNC connectors through which it provides an analog black & burst or tri-level sync signal, a Linear Time Code signal (LTC), a Digital Audio Reference Signal (DARS), and a word clock signal.

The IMS-VSG181H offers two BNC connectors through which it provides an analog black & burst or tri-level sync signal and a Digital Audio Reference Signal, as well as 15-pin D-Sub GPIO connector through which LTC (balanced and unbalanced), DARS (balanced only) and word clock signals (unbalanced only) are output.

Function
The VSG modules are synchronized against an external reference frequency (10 MHz), a pulse-per-second signal (PPS), and a time string from an upstream clock to generate a variety of configurable video output signals. The signal outputs are phase-matched with the PPS signal.



Signal Outputs:

Black Out:	NTSC (525i) *(59.94 Hz, "Black & Burst", ITU-R BT.1700/SMPTE ST 170:2004)* PAL (625i) *(50 Hz, "Black & Burst", ITU-R BT.1700)* 720p 50 Hz *(Tri-Level Sync, SMPTE ST 296)* 1080i 50 Hz *(Tri-Level Sync, SMPTE ST 274)* 720p 59.94 Hz *(Tri-Level Sync, SMPTE ST 296)* 1080i 59.94 Hz *(Tri-Level Sync, SMPTE ST 274)*
DARS:	DARS 48 kHz DARS 44.1 kHz
LTC:	LTC 24 fps / 23.976 Hz LTC 24 fps LTC 25 fps LTC 30 fps LTC 30 fps Drop Frame *(for NTSC content with a frame rate of 29.97 fps)*
Word Clock:	Sample rates - 44.1 kHz or 48 kHz Scale factors - 1/32, 1/16, 1/8, 1/4, 1/2, 1, 2, 4, 8, 16, 32

Information:

By default, all of the supported synchronization signals are only output if the reference clock is synchronized and the internal oscillator is adjusted. This configuration represents the most reliable signal output. However, it can take several hours for the signals to be output after booting. Part of this process can be skipped (with the corresponding risk of temporary timing inaccuracies) by configuring the module to output the signals with a synchronized clock while disregarding the adjusted state of the oscillator, or with an adjusted oscillator regardless of the synchronization state (holdover).

10.1.11.11 IMS - LNO (Low Phase Noise Option)

The IMS-LNO is a 10 MHz generator card, which provides 10 MHz 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 10 MHz 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	**Status Output 1** Green: Ok Red: Error	**St - Status of the LNO180 card** Green: 10 MHz reference ok and PLL has locked Yellow: 10 MHz reference ok but PLL is not locked yet Red: No 10 MHz reference detected
Second LED	**Status Output 2** Green: Ok Red: Error	**In - 10 MHz reference and PLL status** Green: Ok, 10 MHz available at both outputs Red: Error, no signal at one or both outputs
Third LED	**Status Output 3** Green: Ok Red: Error	**A - Output 1-2 status** Green: Ok, 10 MHz available at both outputs Red: Error, no signal at one or both outputs
Fourth LED	**Status Output 4** Green: Ok Red: Error	**B - Output 3-4 status** Green: Ok, 10 MHz available at both outputs Red: Error, no signal at one or both outputs

Output can not be active, before PLL is locked.

10.1.11.12 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 "10.1.3".

For further detailed configuration settings for this card please see chapter 10.1.3, "Web GUI → Network menu".

HPS / TSU - IEEE 1588 Time Stamp Units
A 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.

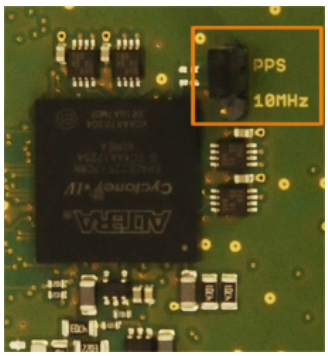
The Synchronous Ethernet function provides a high accurate frequency transport over Ethernet networks. The card can be used either to take a SyncE signal from the network as a source or generate SyncE as a Master.

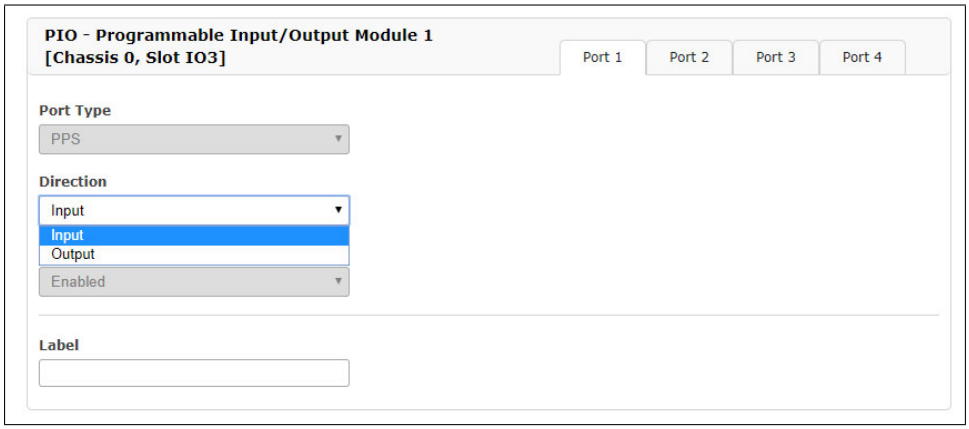
For further information on PTP features and detailed configuration for this card please proceed to Chapter 10.1.7, "Web GUI → PTP menu".

10.1.11.13 IMS Input/Output Cards

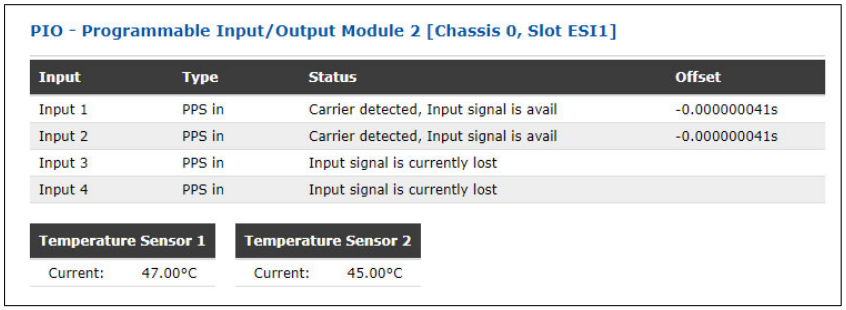
10.1.11.14 PIO - PPS/10MHz Input/Output Module

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.



10.1.12 SyncMon

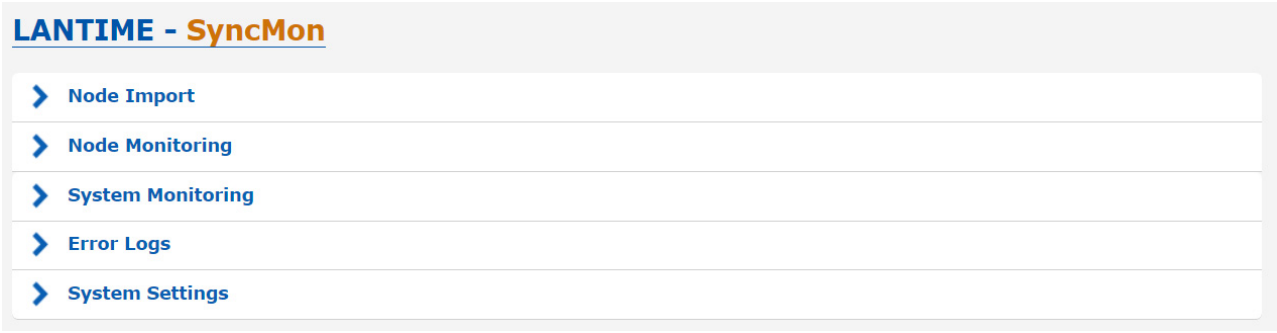


Illustration: SyncMon in the LANTIME Web Interface.

10.1.12.1 SyncMon Introduction

SyncMon (Sync Monitor) is used to measure, monitor, and report the accuracy of network nodes against a UTC-traceable source (such as a GPS clock, a multi-GNSS clock, or a national timing service, for example the NPL). SyncMon can monitor nodes synchronized via the PTP (both IEEE 1588v1 and IEEE 1588v2) or NTP (RFC1305) protocols.

PTP nodes can only be monitored if they support the Meinberg TLV standard or standard PTPv2 management messages. NTP nodes can only be monitored if they are configured to respond to NTP client requests.

Information:

An NTP client that uses the *W32Time* Windows Time Service in its default configuration will not respond to NTP client requests. *W32Time* needs to be configured to operate as both client and server for SyncMon to be able to monitor the node.

It is also possible to monitor any configured MRS, FDM, PIO, or ESI input (such as PPS or frequency inputs) as long as an ESI module (External Synchronization Input) is present. SyncMon is available on all Meinberg IMS and LANTIME systems with LTOS 7.00 or better installed. A license of for at least 1024 clients and an integrated IMS-HPS100 PTP module are required to monitor PTP clocks.

SyncMon can also be operated as an independent node separately from a master clock. As such, it is generally possible to position SyncMon nodes anywhere in a network, although they should be ideally positioned as close to the slaves as possible for the accuracy measurements to be accordingly representative. SyncMon nodes can also measure the performance of a Grandmaster Clock and measure potential network connection asymmetry between a Grandmaster and the SyncMon node.

It is possible to configure up to 1,000 monitoring nodes on a SyncMon interface running on a standard LANTIME or IMS system. Individual monitoring and logging intervals can be defined for each individual node. It is also possible to define an offset limit for each node that will cause an alarm to be triggered (in the form of an SNMP trap, an e-mail sent over SMTP, or some other user-defined channel) whenever this value is exceeded. It is also possible to set a stratum limit for NTP nodes that will likewise trigger an alarm if the defined stratum is exceeded.

SyncMon also provides the ability to download all monitoring data and log files for each node, and these archives can be used in the preparation of reports or other statistical analyses. The data from each monitored node can be sent in various formats via the syslog protocol or stored on a file server to be updated upon changes by an rsync service. The live, up-to-date, online data of each node can be acquired in JSON format using tools such as *curl* or *wget* to be forwarded to other management systems.

A JSON file is provided for each node under */www/htdocs/syncmon/[alias].json*, where [alias] should be substituted with the actual node alias.

10.1.12.2 Starting Out with SyncMon

When SyncMon is started for the first time, monitoring is not yet enabled. To enable monitoring, at least one node must be added. Click on the button "**Add Node**" to add a new monitoring node.

10.1.12.3 Using SyncMon for Status Monitoring and Configuration via Web Interface

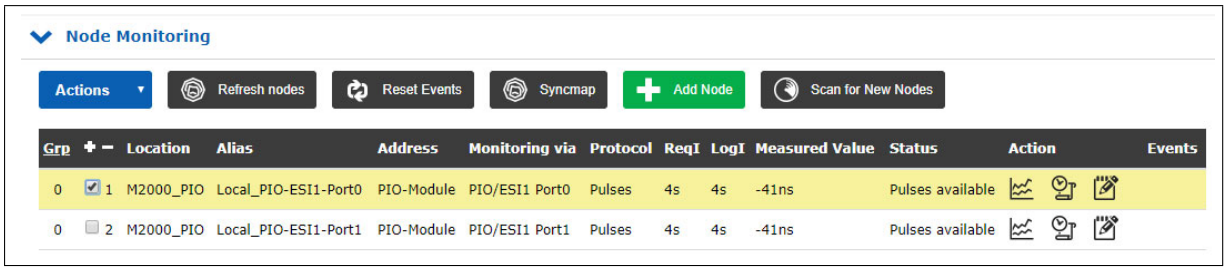
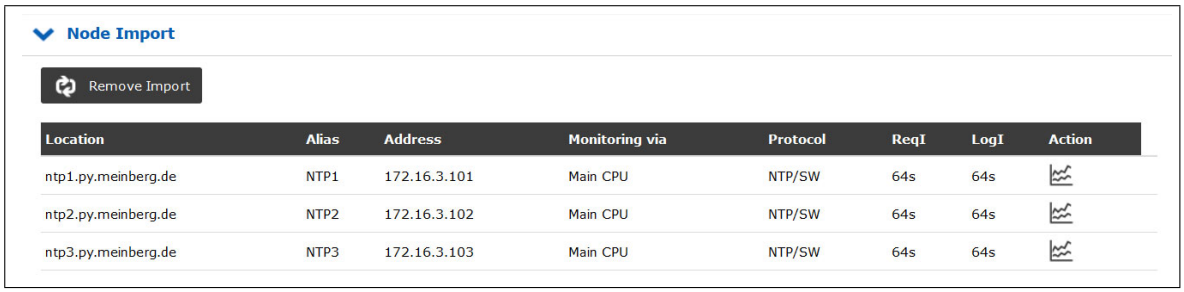


Illustration: SyncMon User Interface on LANTIME systems with LTOS Version 7.00 or later.

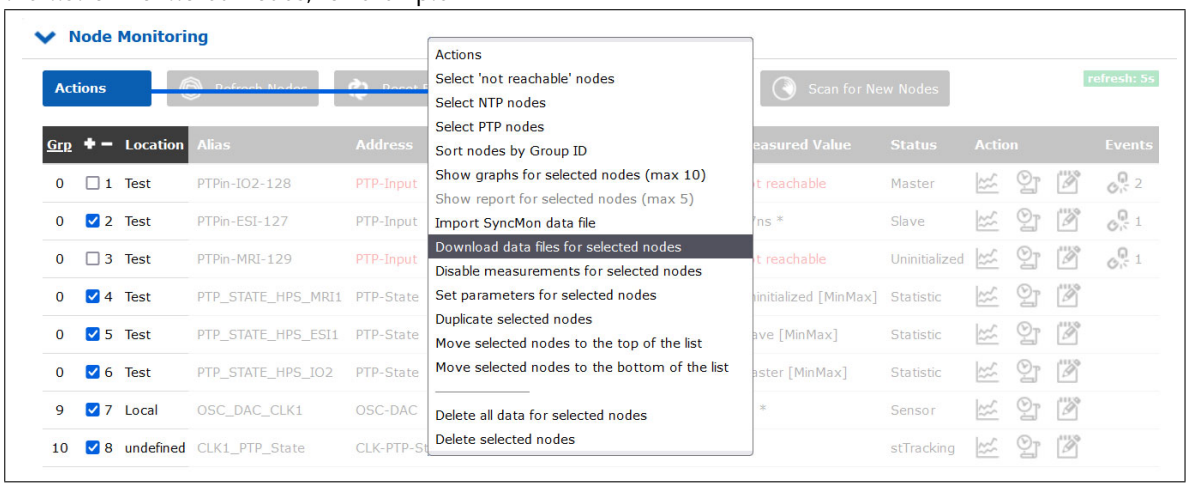
The "Node Monitoring" sections shows the current status and configuration of all monitored nodes. A monitoring node can be either a network device such as an NTP server or PTP device, or a LANTIME-specific input module, for example for pulse or frequency signals. Each line in the table represents a monitored node or a group of nodes. The table can be displayed in Flat or Group mode. In Flat mode, only one node is displayed on each line. To provide a more structured overview, the table can also be switched to Group mode by clicking on the heading "**Grp**" in the first column. This will group all nodes with the same index together and allow each group to be opened individually. Clicking the "**Grp**" heading again will return you to Flat mode.

The status in the Web Interface is refreshed automatically every 10 seconds.

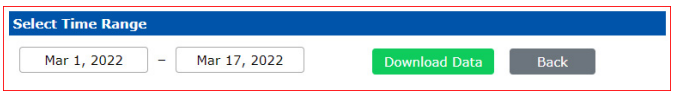
10.1.12.4 Node Import

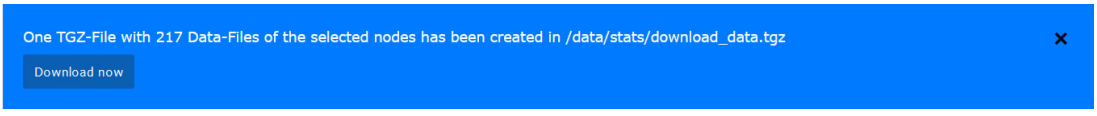


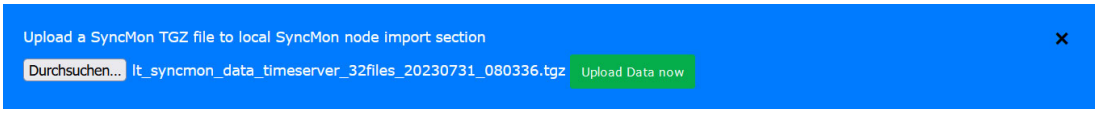
The "Node Import" menu is displayed whenever a node set has been downloaded from a LANTIME using the function "Actions → Download Data Files for Selected Nodes" and then imported to another LANTIME using the function "Actions → Import Sync Mon data files". It is also possible to export and re-import nodes from and to the same LANTIME system. This allows certain nodes to be displayed more clearly in groups in the list of monitored nodes, for example.



To download a file set, first select the nodes and enter the desired monitoring period for the nodes. Once confirmed, a .tgz file will be generated and downloaded by the browser.







This archive can be uploaded back to a LANTIME via "Actions → Import SyncMon data files".

The "Remove Import" button in the "Node Import" menu can be used to easily remove the imported nodes.

10.1.12.5 Node Monitoring

In the "Node Monitoring" section you can add new nodes to measure their accuracy and synchronization performance. Clicking on "+ **Add Node**" will open a configuration dialog that allows you to add a new monitoring node.

"Refresh Nodes" Button:
This button can be used to update the values, even if the automatic request intervals are even less frequent. This will cause a new measurement to be performed and the status of the nodes in the table to be updated. The updated values will be added to the list of measured values for the purpose of calculating an average value. No measurements of PTP instances on any HPS modules will be performed.

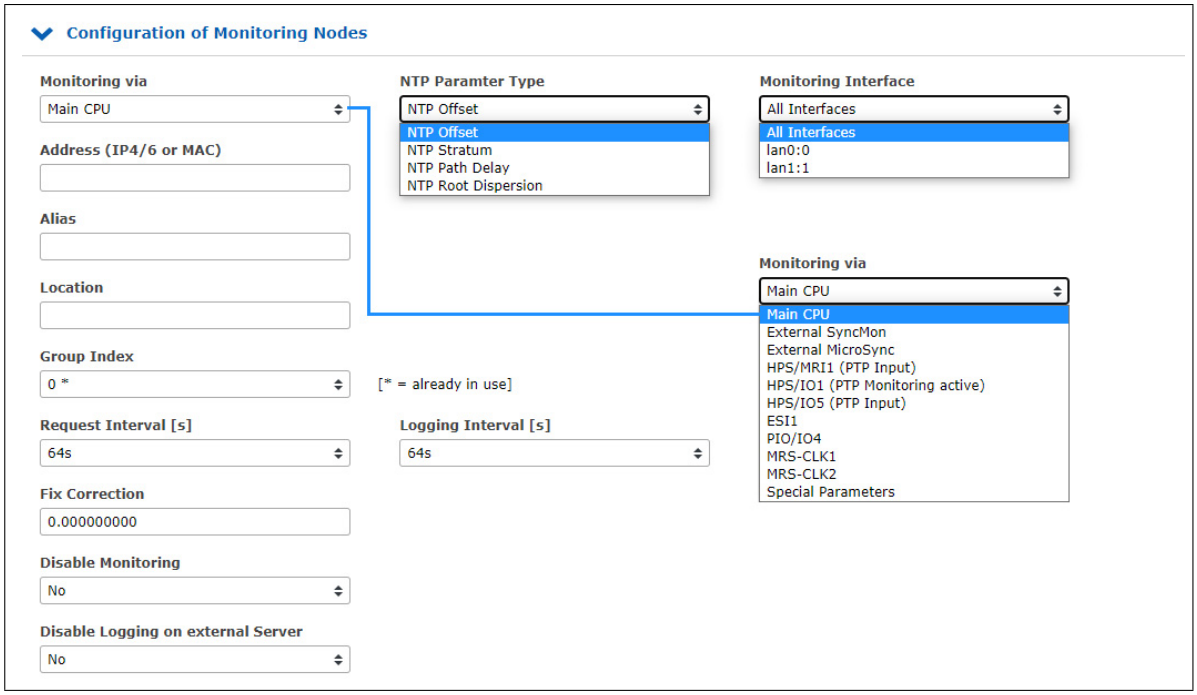
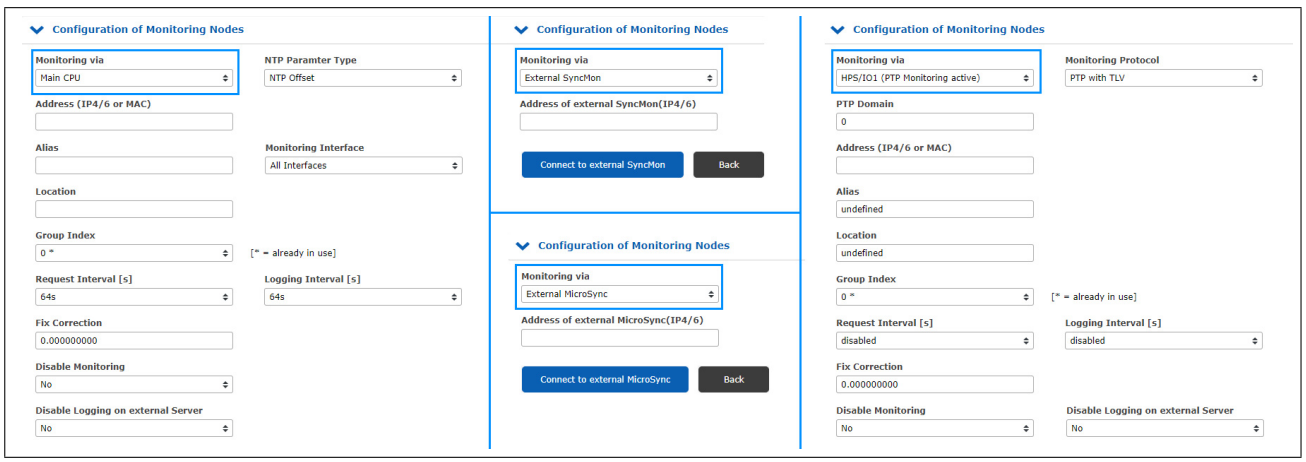


*Illustration: Adding a node using the "***Add Node** *configuration dialog.*

The options provided in the "**Add Node**" are dependent on the option selected in the first drop-down menu "**Monitoring via**" and will activate different input forms with different options:



Monitoring via:
This is where you select the monitoring instance from the drop-down list. This drop-down list will vary depending on your hardware configuration. The following options are possible:

Main CPU: This monitoring instance is always available and is not dependent on the hardware configuration of the LANTIME system. It is only capable of monitoring native NTP nodes responding to NTP client requests.

Information:

An NTP client that uses the *W32Time* Windows Time Service in its default configuration will not respond to NTP client requests. *W32Time* needs to be configured to operate as both client and server for SyncMon to be able to monitor the node.

You can have all assigned interfaces monitored simultaneously or you can select a specific interface from a list, if available.

The drop-down menu "**NTP Parameter Type**" can be used to select whether the "*NTP Offset*", "*NTP Stratum*", "*NTP Path Delay*" or "*NTP Root Dispersion*" should be saved.

If several network interfaces are available, a specific interface or "*All Interfaces*" can be selected via the "Monitoring Interface" drop-down menu.

External SyncMon: This monitoring instance can monitor nodes and sensors of other LANTIME devices with SyncMon activated. When selecting an external SyncMon via its IP address, a list of available nodes from that external SyncMon will be downloaded. The configuration and data will be transferred via HTTP(S) using *curl*.

External Microsync: This can be used to monitor MRS references from external microSync devices. When selecting an external microSync via its IP address, a list of available references will be downloaded from the external microSync. The configuration and data will be transferred via HTTP(S) using *curl*.

HPS: IMS-HPS100 cards can be used to monitor PTP instances or NTP clocks on their own network port.

If an HPS module is configured to operate as a PTP slave (see LANTIME PTP Configuration), the HPS card will operate as a standard PTP slave with all of the options, including profiles and network-specific configurations. However, only one PTP master can be monitored per HPS module at any given time.

If the HPS module is to be configured as a monitoring system (see LANTIME PTP Configuration), it must be licensed to support at least 1024 clients. If this is the case, it will be possible to monitor multiple PTP nodes via the network interface of the HPS card. This monitoring instance can monitor PTP nodes that support the protocols "PTP with TLV" (a proprietary Meinberg sync node format), "PTP with MGMT" (as defined by the IEEE 1588v2 standard), NTP with software timestamping, or "PTPv1 with MGMT" (as defined by the IEEE 1588v1 standard).

Information:

"PTPv1 with MGMT" requires an IMS-HPS100 module equipped with Firmware Version 2.1.0 or better and LTOS Version 7.06.110 or better. Check which firmware version your HPS module has by opening "**System → System Information → Show Device Version**" The version number will be shown at the bottom of the list of installed cards by "ID", e.g., "HPS6 Cyclone5 High Performance Sync Module HPS100 2.0.6 2022-06-30 License (2048/262144)".

If you wish to monitor PTPv1 instances with SyncMon but your HPS100 firmware version is not recent enough, please get in touch with Meinberg's Technical Support team, who will be happy to help you further.

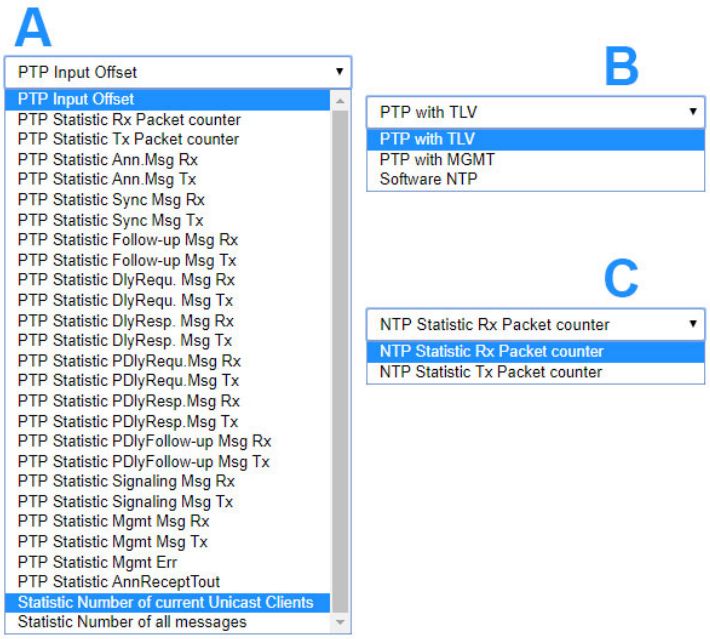
The special protocol "PTP with TLV" acts like a reverse form of PTP—a PTP delay request packet with a special TLV appended is sent to the PTP device, which responds with a sync message and a delay response message. This method allows the PTP device's offset relative to the internal reference to be measured, regardless of whether this PTP system is in Master, Slave, or Passive mode.

Statistic Types:

Various statistics can be acquired on individual nodes monitored via an HPS module in PTPv2, Monitor, or NTP mode. These statistics are requested from the node and are sent to SyncMon as a response to that query.

Information:

It is not possible to record such reported statistics while the HPS module is in PTPv1 mode as the PTPv1 protocol does not support the acquisition of statistics via management messages.



HPS cards in PTP or NTP mode support packet statistics which can be monitored individually:

A: HPS in PTPv2 mode.
B: HPS in monitoring mode.
C: HPS in NTP mode.

ESI: This monitoring instance can monitor PPS and frequency nodes with an External Signal Input (ESI) card. From a drop down list you can select which particular signal you wish to monitor. The available options are: PPS0, Freq In0, Freq In1, BITS In2.

MRS-CLK: This monitoring instance can monitor all activated MRS input signals for each MRS reference clock. You can select which signal you wish to monitor from the drop-down list. The available options are: GNSS/ GPS, NTP, PTP, PPS, IRIG, 10MHz, E1, 2048kHz. The actual options supported are dependent on the hardware installed (see "**Clock**" tab in the Web Interface).

PIO: This monitoring instance can monitor PPS and frequency nodes with a Programmable Input/Output (PIO) card. You can select which signal you wish to monitor from the drop-down list. The The available options are: PPS0, PPS1, PPS2, PPS3, Freq In0, Freq In1, Freq In2, Freq In3. actual options supported will depend on the configuration of the PIO card.

FDM: This monitoring instance can monitor 50/6 0Hz power-line network nodes with a Frequency Deviation Monitor (FDM) card. You can select which signal you wish to monitor from the drop-down list. "**Time Deviation**" and "**Frequency Deviation**" are the options available.

Special Parameters: This monitoring instance can monitor various parameters if they are enabled:

Process Memory:
This can be used to monitor the memory usage of system processes. For this purpose, the name of the process must be specified and the values are displayed in **%**.

After selecting "**Special Parameters** → **Process Memory**" the fields
NTP Parameter Type → **Special Parameter** and
Address (IPv4/IPv6 or MAC) → **Name of Process** will be displayed.

The process name must be entered in the field "**Name of Process**", which could be *ntpd* or *httpd*, for example. You can obtain a list of the running processes (including names) by logging into the LANTIME CLI via SSH and executing *ps ax*.

ID of Selected HPS Card:
This option will only appear if an HPS card is operating as a PTP slave in the system. If multiple HPS cards are operating in PTP slave mode in the system, the best card according to the internal PTP-BMCA (Best Master Clock Algorithm) will be selected as the MRS/PTP reference. This option is used to monitor the ID of the selected card.

ID of selected NTP server:
This option will only appear if external NTP servers have been configured in the system. If multiple external NTP servers are configured, the best external NTP server will be selected by means of a special NTP selection algorithm and use as the MRS/NTP reference. This option is used to monitor the ID of the selected external NTP server.

Address (IP4/6 or MAC):
The IPv4, IPv6, or MAC address of the node you wish to monitor over the network. Hostnames are not allowed.

Alias:
This can be used to specify an alias for a monitoring node so that it can be found more easily in the tabular overview. The alias set by the user also determines the name of the folder on the selected storage medium ("Data Storage Base Path") for each node. The alias must be unique, contain no spaces (spaces are automatically converted to underscores '_'=), and not exceed 63 characters in length. It is possible to monitor a single node (for example based on a common IP address) using different aliases. This can be useful if you wish to monitor the same node from several different monitoring modules (e.g., different IMS-HPS100 cards with different network paths).

Location:
This can be used to specify the physical location of the monitoring node so that you can more easily locate it. The location name must contain no spaces (spaces are automatically converted to underscores '_'=), and not exceed 63 characters in length.

Group Index:
Monitored node can be organized into logical groups by assigning the same index to them. For example, nodes might be assigned a common index if they are of the same type (NTP, PTP, PPS), or are in the same location for ease of organization. Notes with the same group index are automatically sorted in the table. The table can be viewed in Flat or Group mode. In Flat mode, only one node is displayed on each line. To provide a more structured overview, the table can also be switched to Group mode by clicking on the heading "**Grp**" in the first column. This will group all nodes with the same index together and allow each group to be opened individually. Clicking the "**Grp**" heading again will return you to Flat mode.

Request Interval (s):
This specifies the interval in seconds after which a monitoring node will send requests to the slaves/clients. The request interval can be any value between 1 and 3600 seconds. The default interval is 64 seconds. Requests and data logging can be disabled by selecting "*Disabled*".

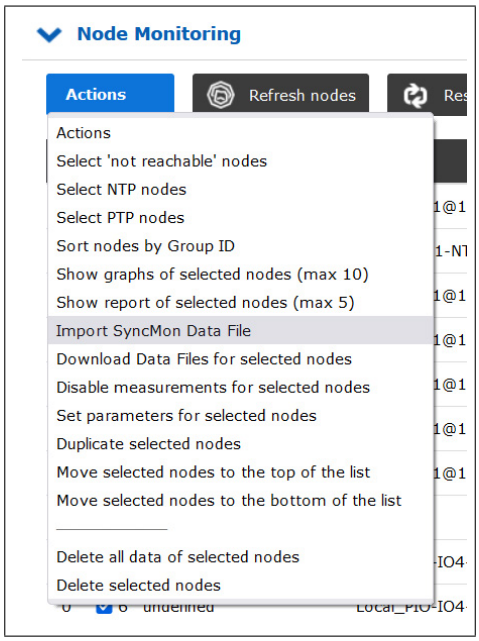
Logging Interval (s):
This specifies the interval in seconds after which the measured offset and stratum are written to a log file. If the logging interval is disabled, no data will be logged in the log file. If the request interval is enabled but the logging interval is disabled, nodes will be monitored and limits and messages will be checks (and corresponding alarms will be triggered), but no data will be saved. If the request interval is less than the logging interval, the minimum and maximum values during the logging interval will be additionally logged alongside the mean value of the offsets measured at each request interval.

Fixed Offset Correction [s]:
If a fixed offset is known (e.g., due to network asymmetry), this value can be entered here as a correction value. The "**Fixed Offset Correction**" is always **added** to the measured value. Any fixed offset correction recorded here will be displayed in the overview with a * in the column "**Measured Value**".

Disable Monitoring:
Monitoring can be disabled for any node. A disabled node will not send any monitoring data to the nodes and not save any data.

Disable Logging on External Server:
Measured values and logged data can be sent to an external server via the syslog or rsync protocol. This can be disabled for each node (see System Settings for External Server Configuration).

10.1.12.6 Actions Button



The "Actions" button can be used to systematically select certain nodes in the SyncMon node list and perform certain operations on them, and to rearrange the list order:

Select 'Not Reachable' Nodes: Selects all nodes that are not reachable.

Select NTP Nodes: Selects all nodes sending or receiving NTP messages.

Select PTP Nodes: Selects only PTP grandmasters or slaves.

Sort Nodes by Group ID: Sorts nodes in ascending order by Group ID.

Show Graphs of Selected Nodes: Displays the graphs for the selected nodes (max. 10).

Show Report of Selected Nodes: Displays the reports for the selected nodes (max. 5).

Import SyncMon Data File: Imports nodes and data from a data file.

Download Data Files for Selected Nodes: Generates a data file for the selected nodes.

Disable Measurements for Selected Nodes: Disables monitoring for the selected nodes.

Set Parameters for Selected Nodes Allows the parameters for several selected nodes to be configured simultaneously.

Duplicate Selected Nodes: Duplicates the selected nodes.

Move Selected Nodes to the Top of the List: Moves the selected nodes to the top of the list.

Move Selected Nodes to the Bottom of the List: Moves the selected nodes to the bottom of the list.

Delete All Data of Selected Nodes: Deletes all of the data (graphs and error logs) related to the selected nodes.

Delete Selected Modes: Deletes all of the selected nodes.

Show a Status Overview for: Current Day:

Displays a status overview of each node shown in the list, including measured and reported offsets and the last error recorded. Also provides access to graphs and error logs for each node.

This option is only displayed if no nodes are selected.

Show Overview for Time Range:

Prompts you to specify a time range for the overview. If *Add SyncMap to Report* is checked, the overview will incorporate a copy of the current SyncMap.

Once the time range is specified, a status overview of each node shown in the list will be displayed, including measured and reported offsets and the last error recorded. Graphs and error logs can also be accessed for each node.

This option is only displayed if no nodes are selected.

10.1.12.7 Exporting and Importing Data in SyncMon

The Export/Import function can be used to export data for selected nodes over a specific period of time. The daily data files are packaged in a downloaded archive (*.tgz*). The export function "Download Data Files for Selected Nodes" is located in the "Actions" menu, provided that at least one node has been selected. You will then be prompted to enter a time period for which the data should be stored. The names of the *.tgz* files follow the format below:

```
lt_syncmon_data_ + hostname + number of files included + date + time
```

Example:

```
lt_syncmon_data_timeserver_6files_20220311_070714.tgz
```

The *.tgz* file includes all data files for the selected nodes over the selected period. Each node is represented by a directory with the alias name. The archive also includes the relevant files for the local clock and node configuration files. The number of included files specified in the download name only relates to the number of data files for the nodes and local clock.

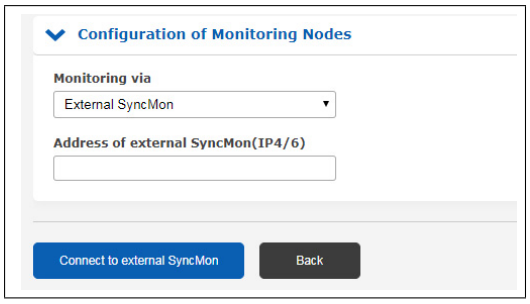
Example of directory structure for an unpacked *.tgz* file:

```
172.27.100.57/
----> ntp_mon_stats.20220314
----> ntp_mon_stats.20220315
----> ntp_mon_stats.20220316
local_reference/
----> ntp_mon_stats.20220314
----> ntp_mon_stats.20220315
----> ntp_mon_stats.20220316
---------> syncmon_selected_nodes.cfg
---------> syncmon_selected_system_monitoring.cfg
```

This *.tgz* file can then be imported to any system with SyncMon—including other LANTIME systems—using the menu item "Import SyncMon Data File". This enables the exported data to be compared directly with other data from SyncMon-equipped systems.

10.1.12.8 External SyncMon

External SyncMon is a special monitoring instance that can monitor nodes and sensors of other LANTIME devices. When selecting an external SyncMon instance via its IP address, a list of available nodes from that external SyncMon instance will be downloaded. The configuration and data will be transferred via HTTP(S) using *curl*.

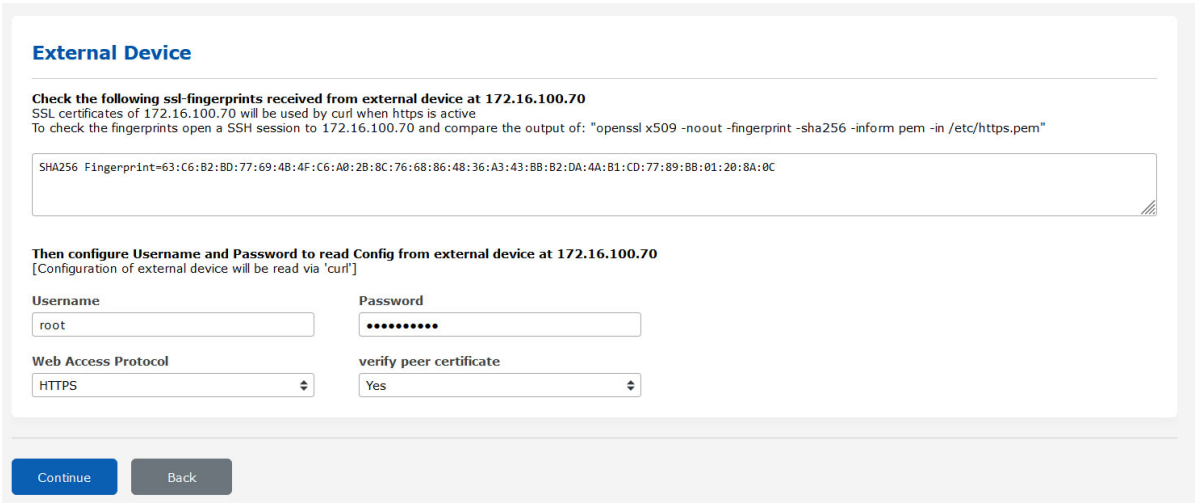


Clicking on "**Connect to External SyncMon**" will initiate an attempt to connect to the external SyncMon instance and display the SSL fingerprint of this server (the 'local' SyncMon instance). The SSL certificates are used by *curl* if HTTPS is enabled.

Compare the SSL fingerprints that the external SyncMon instance has received against the SSL fingerprint of the local LANTIME. To display the fingerprints held by the external SyncMon instance, open an SSH session on the external LANTIME and enter the following command:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem
```

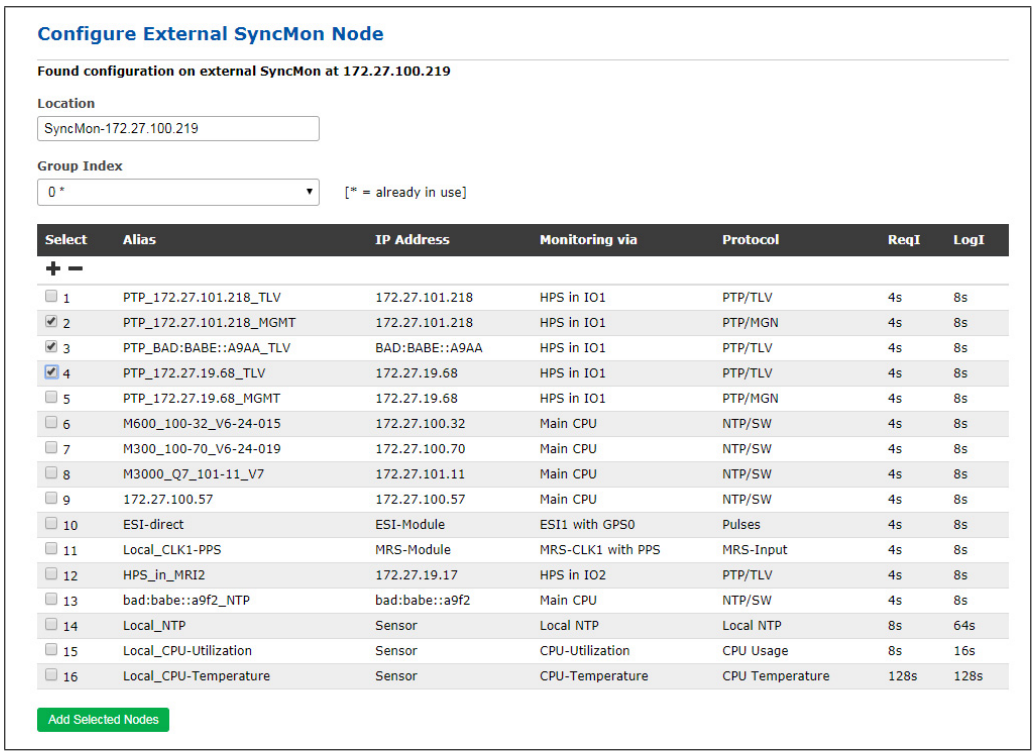
This is to ensure that this is the correct device.



Now enter the username and password to read the configuration from the external SyncMon instance—the current configuration of the external SyncMon instance will be imported using *curl*. If you wish to use a CA certificate package to acquire configuration and measurement data from the external SyncMon, you will need to configure the web access protocol (HTTP or HTTPS accordingly).

Please note that using HTTPS by definition necessitates the encryption and decryption of all data, which can increase the CPU usage for each data request sent to the external SyncMon.

If you wish to use the HTTP protocol, you will need to enable the HTTP network service on the LANTIMEs of both the local and external SyncMon instances. The same applies to the HTTPS protocol.



Configure External SyncMon Node

Found configuration on external SyncMon at 172.27.100.219

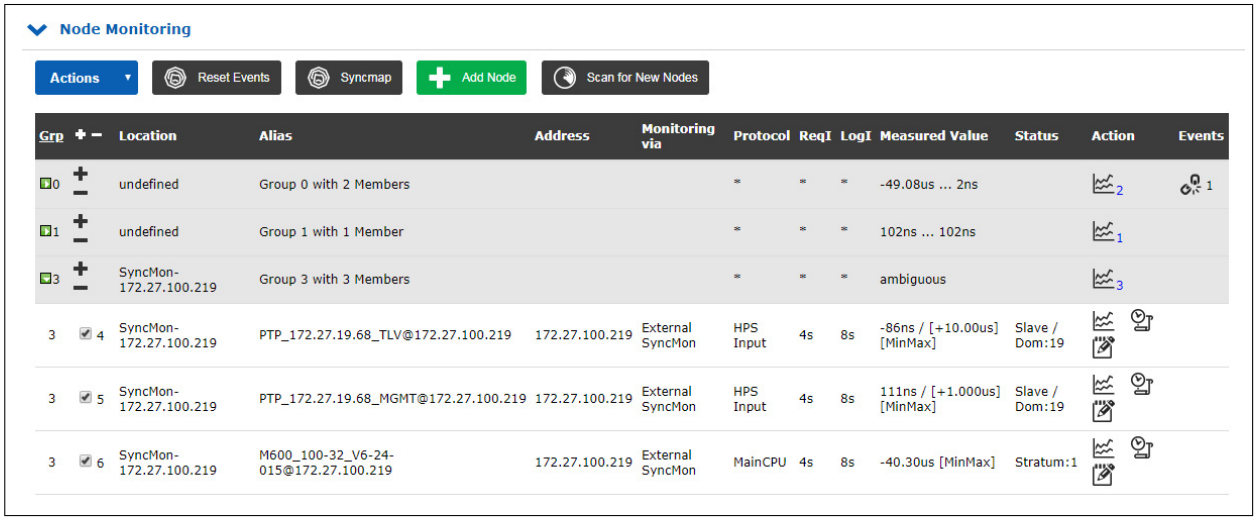
Location: SyncMon-172.27.100.219

Group Index: 0 * [* = already in use]

Select	Alias	IP Address	Monitoring via	Protocol	ReqI	LogI
1	PTP_172.27.101.218_TLV	172.27.101.218	HPS in IO1	PTP/TLV	4s	8s
2	PTP_172.27.101.218_MGMT	172.27.101.218	HPS in IO1	PTP/MGN	4s	8s
3	PTP_BAD:BABE::A9AA_TLV	BAD:BABE::A9AA	HPS in IO1	PTP/TLV	4s	8s
4	PTP_172.27.19.68_TLV	172.27.19.68	HPS in IO1	PTP/TLV	4s	8s
5	PTP_172.27.19.68_MGMT	172.27.19.68	HPS in IO1	PTP/MGN	4s	8s
6	M600_100-32_V6-24-015	172.27.100.32	Main CPU	NTP/SW	4s	8s
7	M300_100-70_V6-24-019	172.27.100.70	Main CPU	NTP/SW	4s	8s
8	M3000_Q7_101-11_V7	172.27.101.11	Main CPU	NTP/SW	4s	8s
9	172.27.100.57	172.27.100.57	Main CPU	NTP/SW	4s	8s
10	ESI-direct	ESI-Module	ESI1 with GPS0	Pulses	4s	8s
11	Local_CLK1-PPS	MRS-Module	MRS-CLK1 with PPS	MRS-Input	4s	8s
12	HPS_in_MRI2	172.27.19.17	HPS in IO2	PTP/TLV	4s	8s
13	bad:babe::a9f2_NTP	bad:babe::a9f2	Main CPU	NTP/SW	4s	8s
14	Local_NTP	Sensor	Local NTP	Local NTP	8s	64s
15	Local_CPU-Utilization	Sensor	CPU-Utilization	CPU Usage	8s	16s
16	Local_CPU-Temperature	Sensor	CPU-Temperature	CPU Temperature	128s	128s

Add Selected Nodes

To import the up-to-date configuration from the external SyncMon instance, you will need to select the nodes of that LANTIME that you wish to monitor. Only nodes that are not disabled and have external logging allows will be listed as options. The parameters for request and logging intervals will be imported from the external configuration. The location and group index can be configured for all selected nodes. The default location will be "SyncMon-" plus the IP address. The alias for the external SyncMon nodes is the original alias plus "@ip_address". It is recommended to assign all nodes of an external SyncMon instance to an unassigned group ID.

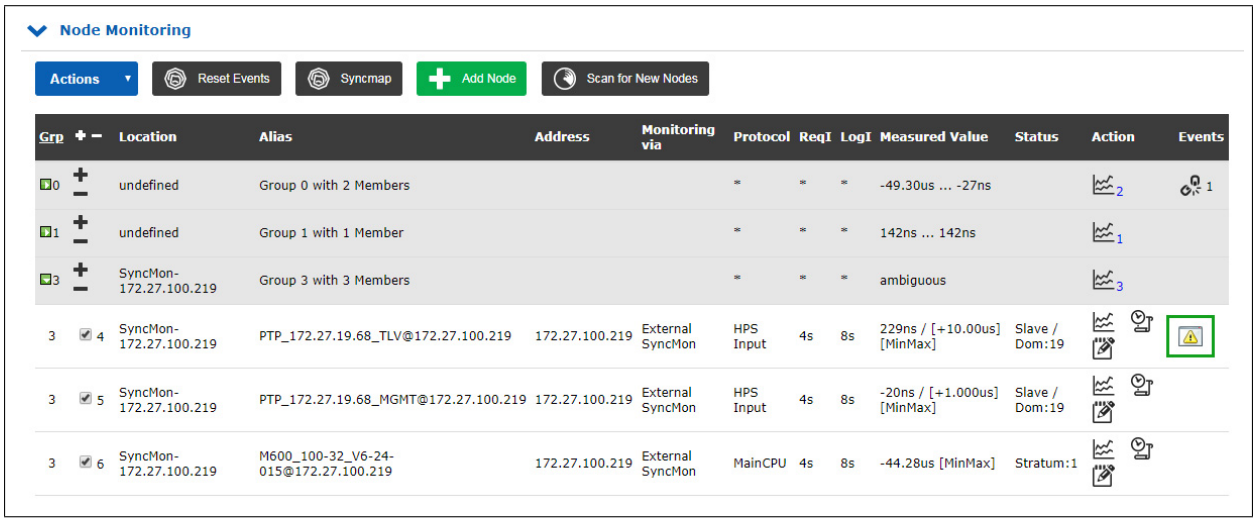


Node Monitoring

Actions | Reset Events | Syncmap | Add Node | Scan for New Nodes

Grp		Location	Alias	Address	Monitoring via	Protocol	ReqI	LogI	Measured Value	Status	Action	Events
0		undefined	Group 0 with 2 Members			*	*	*	-49.08us ... 2ns		2	1
1		undefined	Group 1 with 1 Member			*	*	*	102ns ... 102ns		1	
3		SyncMon-172.27.100.219	Group 3 with 3 Members			*	*	*	ambiguous		3	
3	4	SyncMon-172.27.100.219	PTP_172.27.19.68_TLV@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	-86ns / [+10.00us] [MinMax]	Slave / Dom:19		
3	5	SyncMon-172.27.100.219	PTP_172.27.19.68_MGMT@172.27.100.219	172.27.100.219	External SyncMon	HPS Input	4s	8s	111ns / [+1.000us] [MinMax]	Slave / Dom:19		
3	6	SyncMon-172.27.100.219	M600_100-32_V6-24-015@172.27.100.219	172.27.100.219	External SyncMon	MainCPU	4s	8s	-40.30us [MinMax]	Stratum:1		

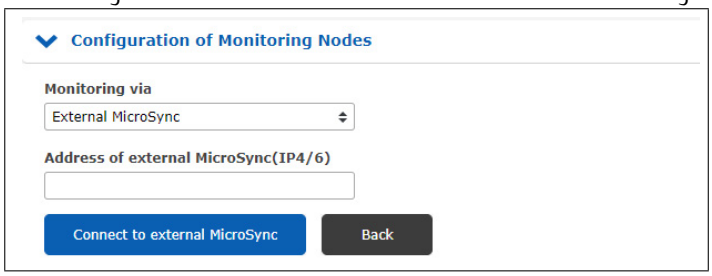
If changes have been made to the node of the external SyncMon configuration to be monitored, the column "**Events**" in the main table will show a warning sign for that node, in which case you will need to modify the parameters for that node manually.



10.1.12.9 External MicroSync

External MicroSync is a special monitoring instance that can monitor MRS references of external microSync devices. When selecting an external microSync via its IP address, a list of available references from that external microSync instance will be downloaded.

The configuration and data are transferred via HTTPS using *curl*.



Clicking on "**Connect to External MicroSync**" will initiate an attempt to connect to the external microSync and display the SSL fingerprint of this server (the 'local' SyncMon instance). The SSL certificates are used by *curl* if HTTPS is enabled.

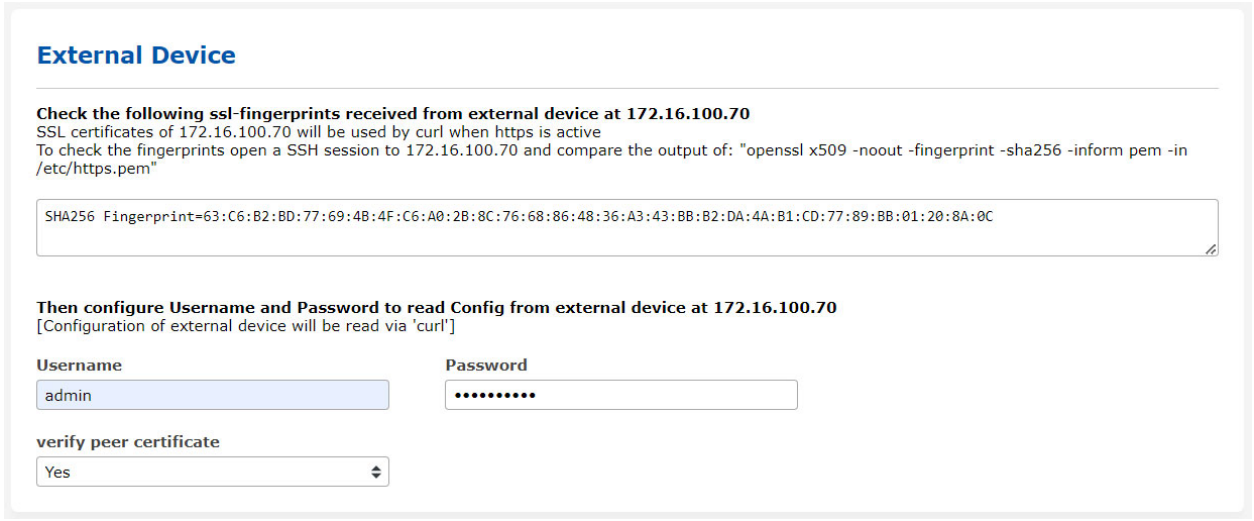
Compare the SSL fingerprints that the external microSync has received against the SSL fingerprint of the local LANTIME. To display the fingerprints held by the external microSync, open an SSH session on the microSync and enter the following command:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem
```

This is to ensure that this is the correct device.

Now enter the username and password to read the configuration from the external microSync—the current configuration of the external microSync will be imported using *curl*.

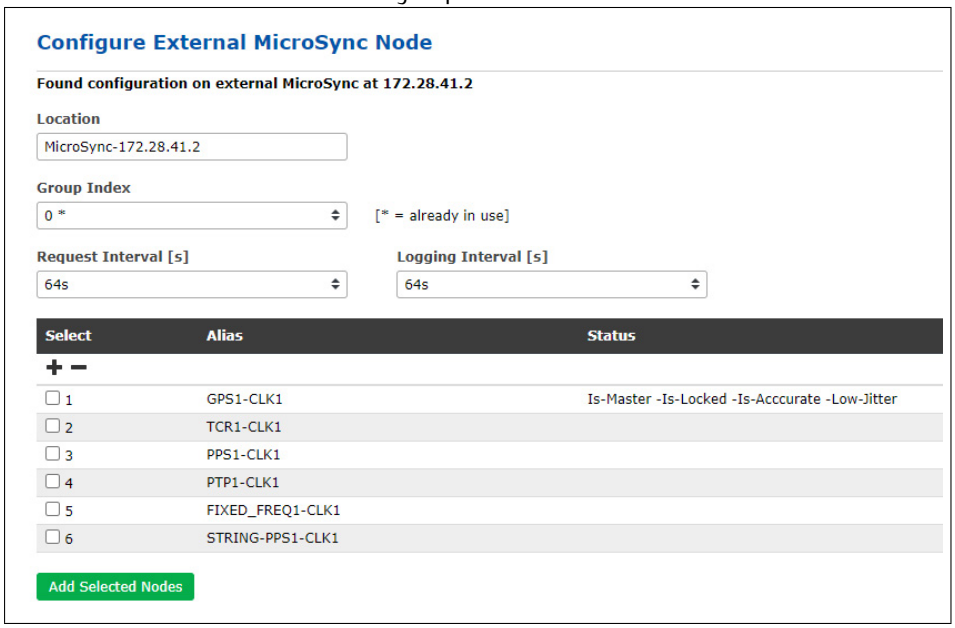
Please note that the use of HTTPS by definition necessitates the encryption and decryption of all data, which can increase the CPU usage for each data request sent to the external microSync.



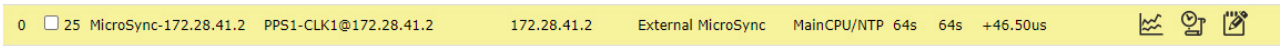
To import the up-to-date configuration from the external microSync, you will need to select the MRS references that you wish to monitor from the local LANTIME. The parameters for request and logging intervals will all be set to the same value.

The location and group index can be configured for all selected MRS references. The default location will be "MicroSync-*" plus the IP address. The alias for the external microSync MRS reference is the original alias plus "@ip_address". It is recommended to assign all MRS references of an external microSync to an unassigned group ID.

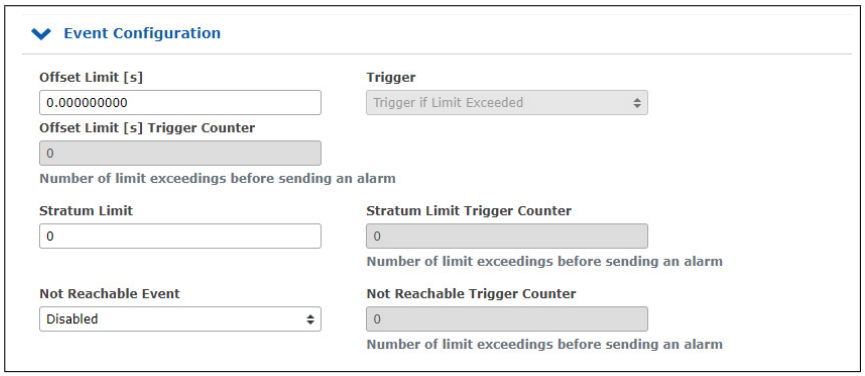
The alias names for the external MicroSync MRS references are the original alias name plus *@IP address*. It is recommended to use an unused group ID for all MRS references of an external MicroSync.



If changes have been made to the node of the external microSync configuration to be monitored, the column "**Events**" in the main table will show a warning sign for that node, in which case you will need to modify the parameters for that node manually.



10.1.12.10 Event Configuration

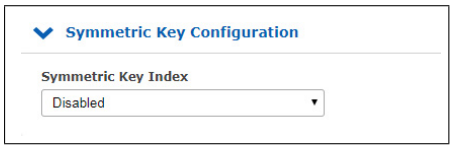


Offset Limit (s):
Offset limit value in seconds. The measured offset between a node and the reference is compared against the configured limit value. If the calculated difference is greater than the configured offset limit, the LANTIME will generate a SyncMon alarm (which can be sent as an e-mail notification, SNMP trap, or message to an external syslog server). The drop-down menu "Trigger" provides two options—"Trigger if Limit Exceeded" and "Trigger if Below Limit"—to specify if the alarm is triggered when the value exceeds or falls below the defined limit. The option "Offset Limit[s] Trigger Counter" triggers the event once when the number of consecutive offset limit triggers exceeds the defined value.

Stratum Limit:
Limit value for an NTP stratum. If the stratum of a monitored client is greater than the configured stratum limit, the LANTIME will generate a SyncMon alarm (sent as an e-mail notification, SNMP trap, or message to an external syslog server). The option "Stratum Limit Trigger Counter" triggers the event once when the number of consecutive stratum limit triggers exceeds the defined value.

Not Reachable Event:
If a configured node is not reachable for monitoring, the LANTIME will generate a SyncMon alarm (sent as an e-mail notification, SNMP trap, or message to an external syslog server). This option allows this function to be enabled or disabled accordingly. The option "Not Reachable Limit Trigger Counter" triggers the event once when the number of consecutive "not reachable" triggers exceeds the defined value.

10.1.12.11 Symmetric Key Configuration

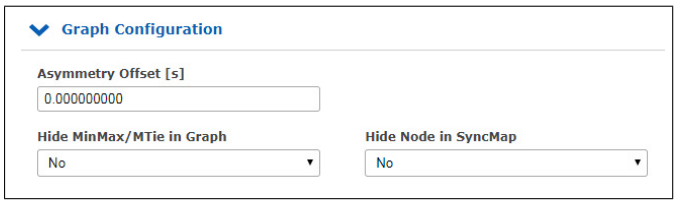


Symmetric Key Index:
If you wish to use symmetric key authentication with SyncMon, select one of the key indices from the list of existing keys. If the keys are not yet defined, proceed with the NTP key setup procedure under "**NTP → NTP Symmetric Keys**" to generate a new keyfile, which must be copied to and activated on the node to be monitored.

For further information on Symmetric Key Generation, please refer to the LTOS7 configuration section "**NTP → NTP Symmetric Keys**".

10.1.12.12 Graph Configuration

Graph Offset Correction:
If an asymmetry constant is known for the nodes being measured, the graph output can be adjusted accordingly. Note that this does not affect the logged values—the graph offset value is simply a fixed adjustment for the graph output.



Hide MinMax/MTie in Graph:
If the request interval is lower than the logging interval, additional Min and Max values will be logged in the logfiles. These Min-Max values are plotted as a filled curve in gray behind the logged offset curve. This feature can be disabled.

Hide This Node in SyncMap:
Hides the node in the SyncMap.

Once have finished configuring the new node, save the updated configuration by clicking on the "**Save Member**" button.

When you are finished with configuration of a new monitored node, save the current configuration by clicking the "Save Member" button. Clicking on the "**Remove Member**" button will conversely remove the currently selected node from the list of all monitored nodes. All sampled data for that node will be lost if you do not back up the data beforehand.

The "**Remove Existing Data**" erases all data for that node only.

10.1.12.13 Scan for New Nodes

Scan for new Nodes automatically searches for NTP and PTP nodes within your network. HPS cards can only search for PTP nodes if the license covers at least 1024 clients.

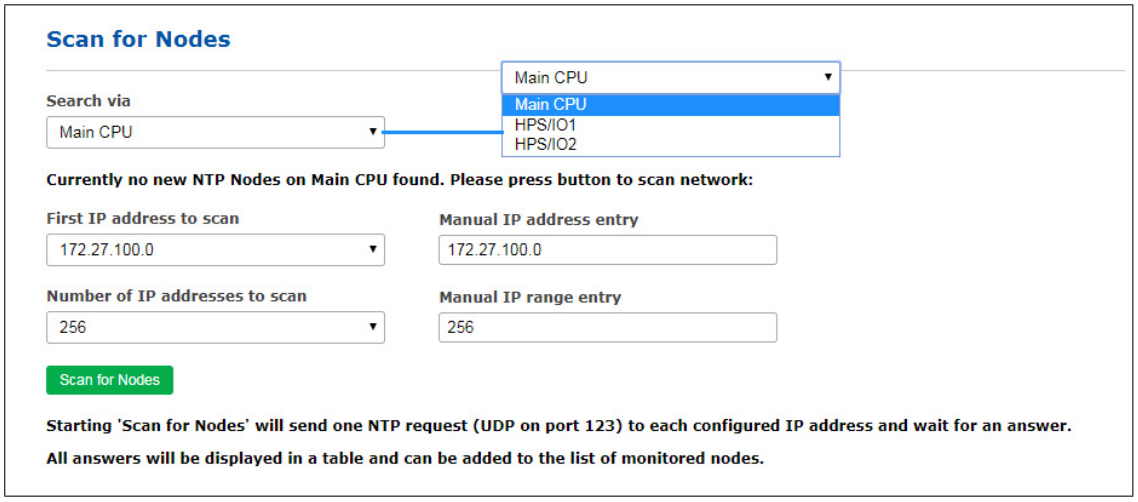


*Illustration: The "***Scan for New Nodes***" dialog. This temporary table only lists the newly found nodes that are not already being monitored. Mark the nodes that you wish to add to the "***Node Monitoring***" table.*

Search via:
Begin by selecting an instance from the drop-down list that you wish to use to search for new nodes. The options will be either "*Main CPU*" or, provided that your system has one or more HPS modules installed, an "*HPS*" entry for each card. The "*Main CPU*" option can only be used to scan for NTP nodes. Scans for PTP nodes are only supported by HPS modules with a license for at least 1024 clients.

Searching via "Main CPU"

First IP Address to Scan:
This defines the first IP address that the automatic NTP scan will start with. The drop-down list shows all subnet ranges for each of the network interfaces. It is possible to override this starting address with a different address not provided in the drop-down menu using the field "**IP Scan Address - Manual Override**".

Number of IP Addresses to Scan:
This defines the number of IP addresses to be scanned. A separate NTP request packet is sent to each IP address within the IP address range. If an NTP client responds to such a request and that IP address is not yet configured, this node will appear in this table. A different number of IP addresses to scan can be entered in "**IP Scan Range - Manual Override**" if necessary.

Scan for Nodes:
Starting "**Scan for Nodes**" via the Main CPU will send a single NTP request (UDP on port 123) to each configured IP address (IP address range) and wait for a response.

All responding nodes are displayed in a table, from where they can be added to the list of monitored nodes by selecting them under "**Select**" and accepting them by clicking on "**Add Selected Nodes**". The parameters *Location*, *Group Index*, *Request Interval*, *Logging Interval*, *Offset Limit*, and *Stratum Limit* can be defined in the next step before they are added to the monitored nodes table.

Searching via a HPS Card

If a HPS card in monitoring mode is selected (requires a license of at least 1024 clients license and monitoring to be activated), then "PTP Domain" will need to be set up to detect PTPv2 nodes.

PTPv1 nodes must be part of one of the subdomains *_DFLT, _ALT1, _ALT2,* or *_ALT3* to be found by SyncMon.

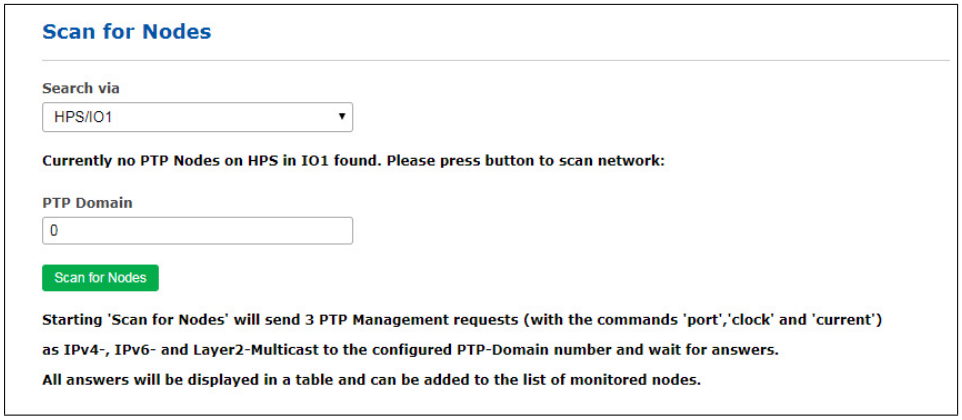


*Illustration: To be able to scan the network for PTP nodes, a HPS card with monitoring activated must first be selected in the "***Search via***" drop-down list.*

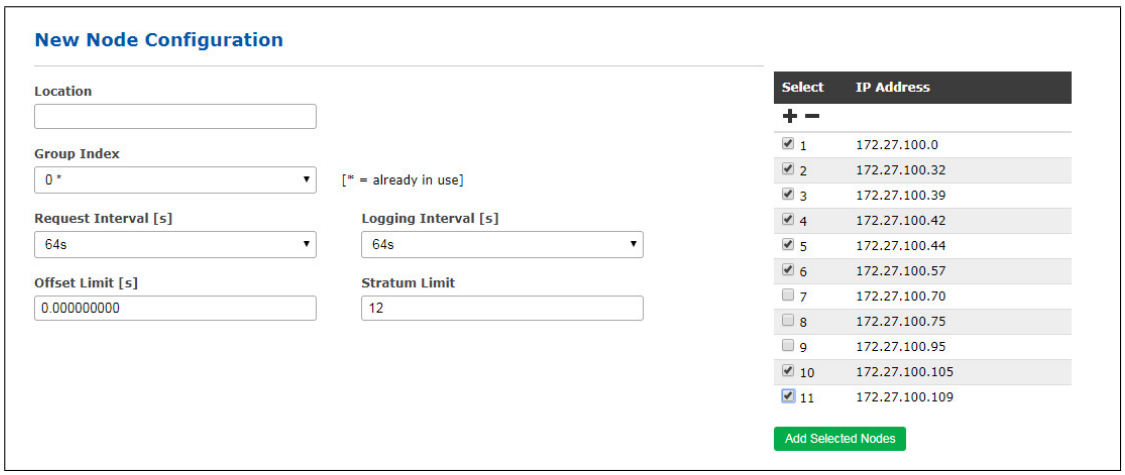
PTP Domain:
The network connected to the HPS card will be scanned for devices in the domain or subdomain defined by the user here. The following device addressing methods are supported by the scan:

- UDP/IPv4/Ethernet,
- UDP/IPv6/Ethernet,
- Ethernet (IEEE 802.3, layer 2).

When the scan is first started, a PTP Management message is sent in broadcast mode to acquire the "port state" of each PTP node—this is done with IPv4, IPv6, and with Layer 2.

All PTP nodes responding to this request will ask for the "current status" and "clock status" with management messages as described below. The result is displayed as a list of all available PTP nodes. Each new PTP node is added to the overall list of available nodes.

The table only shows new nodes that have not yet been configured. The values PTP-UUID, PTP version, IP address, vendor name, node type, domain number (PTPv2) or subdomain (PTPv1), the status (current PTP state such as slave, master, listening), offset, and delay (values most recently measured by the PTP are automatically shown in the list of nodes. The checkboxes can be used to select which new nodes should be imported into the list of monitored nodes. The parameters *Location*, *Group Index*, *Request Interval*, *Logging Interval*, *Offset Limit*, and *Stratum Limit* can be defined in the next step.



The monitoring engine will begin to transmit PTP or NTP request at the defined intervals to each note in the list and measure the time received in the responses against its own time (which may be based on UTC or a GNSS reference, for example). The most up-to-date offset and status information can be viewed in the status overview table in the "Node Monitoring" section.

10.1.12.14 Node Monitoring

The monitored nodes status table in the "**Node Monitoring**" section shows three buttons under the "**Action**" heading next to the status information: **Graph**, **Error Logs**, and **Edit**.

Selecting the **Graph** button will bring up a graph for the selected node. This page provides a variety of options for customizing the graph's appearance.

"Graph" Button

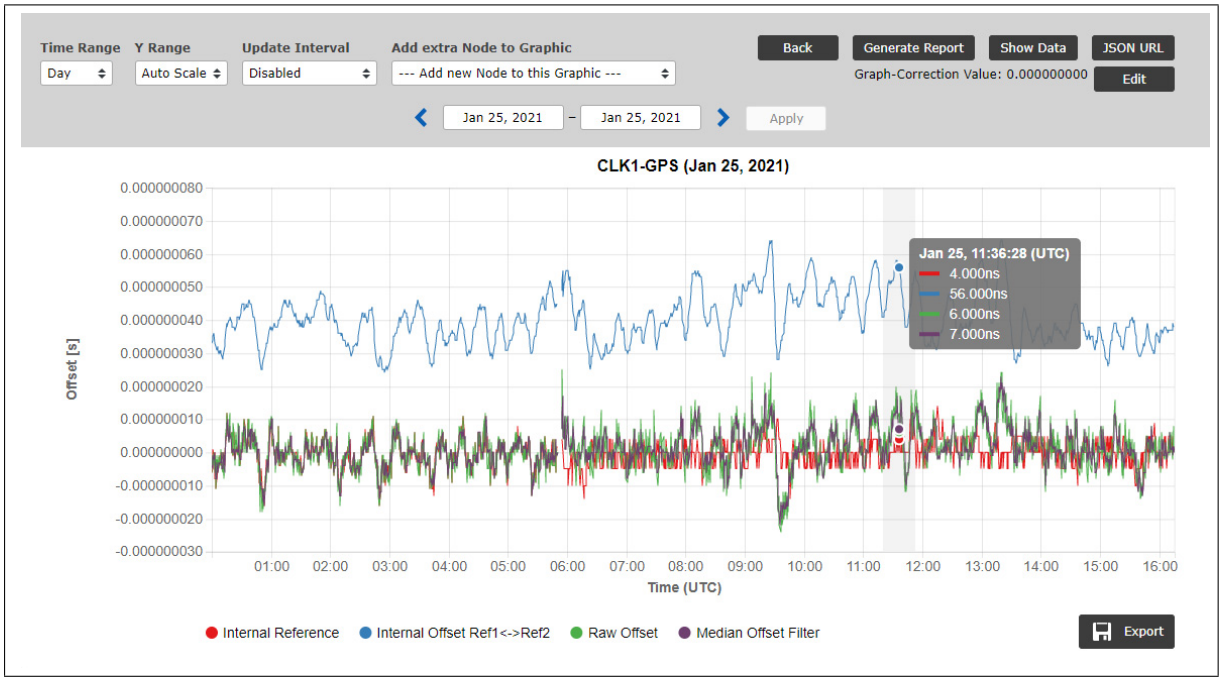
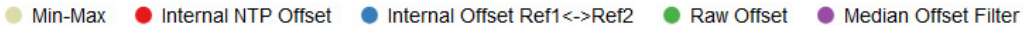


Illustration: Graphical representation of offset values for each node with selectable time scales (day, week, month, custom scale). The graph can be set to any desired timescale for that SyncMon node in the Web Interface using the timescale controls.

Offset data is collected for each monitored node (NTP, PTP or otherwise) and can be presented as a graph for any arbitrary time period in the Web Interface for the SyncMon node in question.

The collected data is written continuously to the sync node record under "**Data Storage Base Path**" at the start of each new day at 0:00 UTC. This data is then available for further statistical analysis whenever it is needed.

A legend is provided at the bottom of the graph that shows which color represents which data. In this case, the red line represents the internal NTP offset, which is the reference for the monitored NTP node. The green line is the offset between the reference time of the sync node and the measured time of a monitored system.



If the cursor is positioned over an element in the legend, only that element will be displayed in the graph; all other elements will be faded. Clicking on that same element in the legend will cause the graph element to remain hidden until it is re-enabled by clicking on it again.

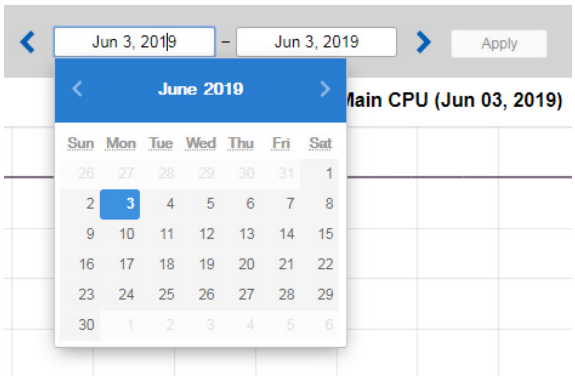
For PTP and PPS signals, the sync node reference is the internal reference time of the receiver, e.g., GNSS (GPS, GLONASS, Galileo, BeiDou), an external UTC time service, an IRIG time code, a long-wave time reference (for example, DCF77, MSF). The sync node reference is shown as a red line; if a second reference is available, the blue line will show the offset between the two reference clocks.

With a GNSS reference clock operating normally, the y-axis of the reference clock line will generally show offset values measurable in a few nanoseconds (typically up to 5 ns), with a resolution of 1 ns.

When monitoring NTP nodes, the sync node is synchronized with the internal NTP service, which in turn is synchronized against an internal clock (which draws upon a source such as a GNSS signal, IRIG time code, or long-wave signal). In this case the red line in the graph represents the internal NTP system time.

Time Range:
This provides various different timescale options: one day, one week, one month, or a custom scale. When a custom scale is specified using the corresponding fields, click on "**Apply**" to update the graph based on the specified timescale.

Regardless of which timescale is selected, the arrow buttons can be used to adjust the time range to review past data. The timescale always remains constant, i.e., if you have selected a custom two-week scale, clicking the back arrow button will jump back to the previous two weeks.



Y Range:
This provides a variety of options: Auto-scale, or fixed Y-scales progressing with each option a multiple of ten of the last: 100 ns, 1 μs, 10 μs, 100 μs, 1 ms, 10 ms, and 100 ms.

Update Interval:
This is used to determine how frequently the current graph is automatically updated, in a range from once per second to once per hour. Alternatively, automatic graph updates can be disabled entirely.

For NTP nodes, the graph shows the internal NTP offset (red line), the raw offset (blue line), and the median offset filter value (green line).

For PTPv2 nodes, the following values may be represented in the graph:

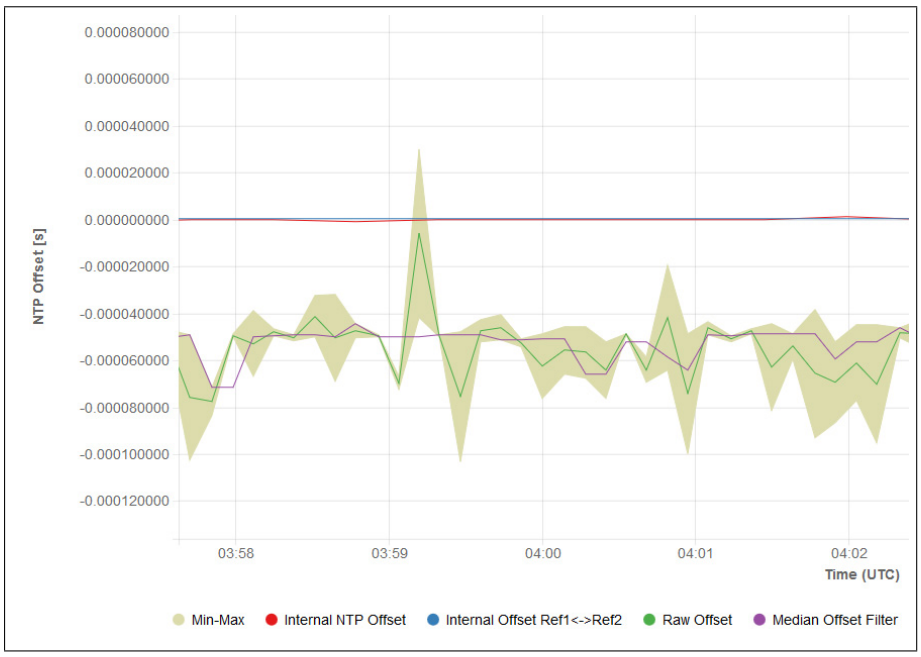
Reported Values: Data obtained from a PTP node via standard PTPv2 management messages.

Measured Values: Offset of a PTPv2 slave measured against the internal reference. The measurements are available only for PTP nodes which support monitoring the PTP protocol using TLVs. The monitored node can be in Slave, Master or Passive mode. The measured values curve based on the values obtained by reverse PTP can be overlaid with the reported values, and if Min-Max value measurement is supported by the monitored node, with the filled MTie curve .

Für PTPv1-Knoten (LTOS 7.06.007 or later only), the graph wil show the internal PTP offset (red line) and the measured offset (blue line).

For PPS nodes monitored via an ESI or PIO input card at the sync node, the graph shows the internal reference offset (red line), the raw offset (blue line), and the median offset filter value (green line).

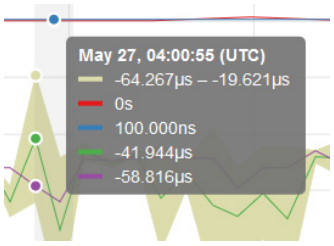
If the request interval is lower than the logging interval, additional Min and Max values will be logged in the logfiles. These Min-Max values are plotted as a filled curve in gray behind the logged offset curve and the mean values are shown as a red line in the filled min/max curve.



Zooming the X/Y Scale:
To zoom the Y scale of the graph in and out, position the mouse cursor on the Y-axis and use the mouse wheel to zoom in and out. Clicking on the Y-axis once will reset the scale to the selected Y scale. Holding down the mouse button and moving the mouse up and down will shift the Y-axis scale up and down accordingly.

To zoom the X scale (timeline) of the graph in and out, position the mouse cursor on the graph itself (not on the X-axis) and use the mouse wheel to zoom in and out. Holding down the mouse button and moving the mouse left and right will shift the graph timeline left and right accordingly.

Hovering with the mouse cursor over any part of the graph will show a summary of all visible values at that point in the graph.



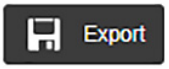
"Show Data" Button:
The "**Show Data**" button will switch from the graph view to a tabular view of the values currently displayed. The first line shows a description of each column. You may use the "**Show Graph**" button to return to the graph view. The data encompasses only the values visible in the graph at the time; therefore, if the graph is zoomed in, only the data range visible at the time will be represented in the table.

# Day	Sec	Julian_day_time	Meas_offset	Report_offs	Path_delay	Port_state	Min	Max		
58638	00002	2019-06-04T00:00:02+00:00	-0.000000002	0.000000173	0.000009348	9 M	-0.000000876	0.000000578	R -0.000000036	0.000000031
58638	00010	2019-06-04T00:00:10+00:00	0.000000078	0.000000055	0.000009064	9 M	-0.000000876	0.000000578	R -0.000000028	0.000000185
58638	00018	2019-06-04T00:00:18+00:00	-0.000000087	-0.000000001	0.000009067	9 M	-0.000000876	0.000000578	R -0.000000359	0.000000185
58638	00026	2019-06-04T00:00:26+00:00	0.000000234	0.000000152	0.000009123	9 M	-0.000000876	0.000000578	R -0.000000159	0.000000628
58638	00034	2019-06-04T00:00:34+00:00	0.000000497	0.000000104	0.000009059	9 M	-0.000000876	0.000000578	R 0.000000366	0.000000628
58638	00042	2019-06-04T00:00:42+00:00	0.000000084	-0.000000147	0.000009064	9 M	-0.000000876	0.000000578	R 0.000000045	0.000000124
58638	00050	2019-06-04T00:00:50+00:00	0.000000334	-0.000000237	0.000009015	9 M	-0.000000876	0.000000578	R 0.000000124	0.000000544
58638	00058	2019-06-04T00:00:58+00:00	0.000000136	-0.000000306	0.000009015	9 M	-0.000000276	0.000000352	R -0.000000077	0.000000349
58638	00066	2019-06-04T00:01:06+00:00	0.000000247	-0.000000230	0.000008820	9 M	-0.000000276	0.000000352	R 0.000000145	0.000000349
58638	00074	2019-06-04T00:01:14+00:00	0.000000117	0.000000124	0.000008703	9 M	-0.000000276	0.000000352	R 0.000000117	0.000000117
58638	00083	2019-06-04T00:01:23+00:00	0.000000073	-0.000000322	0.000008846	9 M	-0.000000276	0.000000352	R -0.000000216	0.000000362
58638	00232	2019-06-04T00:03:52+00:00	0.000000107	0.000000019	0.000008869	9 M	-0.000000486	0.000000387	R -0.000000063	0.000000277

"JSON URL" Button:
The "JSON URL" button is used to display the HTTP(S) URL from which the most recently measured value of the selected node can be acquired. This can be used to read the latest values via HTTP(S) from an external program using a suitable tool such as *wget* or *curl*. The JSON file is formatted as follows:

```
{
   "SyncMon_Data": {
       "LastLogValues" :  {
       "NodeName"              : "172.27.100.57",
       "OffsetLimit"           :  0.000000000,
       "RawOffset"             : -0.000050076,
       "MedianOffset"          : -0.000048733,
       "PathDelay"             : -0.000002693,
       "Status"                : 1,
       "LastErrorCode"         : 0,
       "LastConfigChange"      : 0,
       "LogTime"               : 1559025024
  }
 }
}
```

"Export" Button:
The "**Export**" is used to generate a PNG image of the current graph. This image can be printed and saved accordingly.



"Generate Report" Button
The "**Generate Report**" button can be used to prepare a report on the latest data for the relevant node. You can also select a timeframe so that the report will only relate to data from that period. The report will contain current status data, the monitor configuration, statistical trends over the selected period, a graph, and optionally also a complete SyncMap for the monitored node, for which the checkbox "**Add SyncMap to Report**" must be checked.

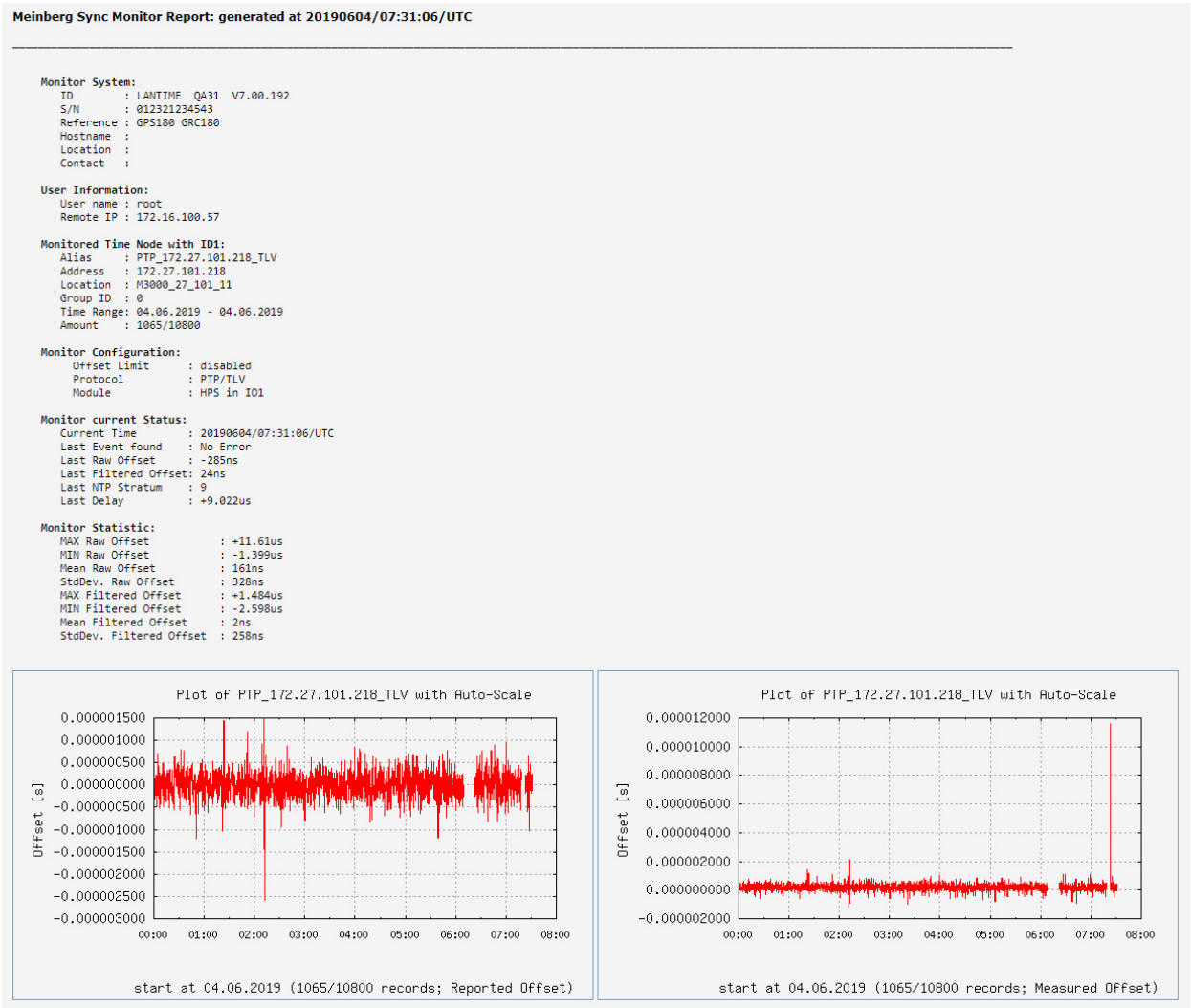


Illustration: Report output for a selected node. The report includes status data on the selected nodes, the monitor configuration, key statistical trends, and graphs.

"Back" Button:
From the Graph View, the "**Back**" button will return you to the main Table View, showing all of the configured nodes.

"Error Logs" Button

In the "Node Monitoring" section, clicking on the button "**Error Logs**" will open the "**Error Logs**" section and filter it to only display the error log messages for the selected node. The messages displayed are generated as of the last boot. When the flash memory is full, the oldest messages will be overwritten.

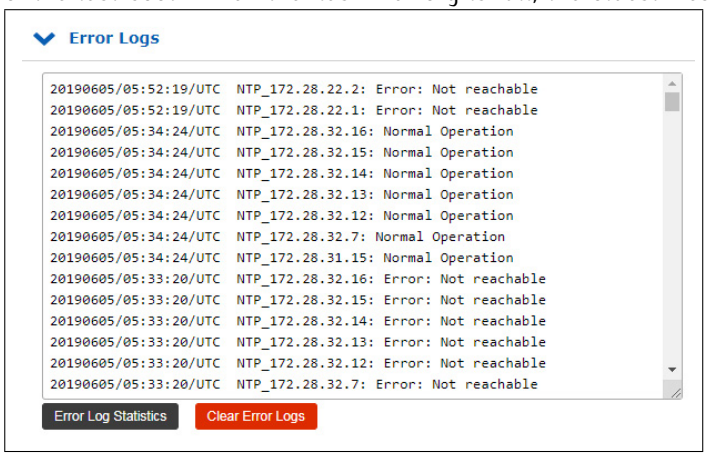
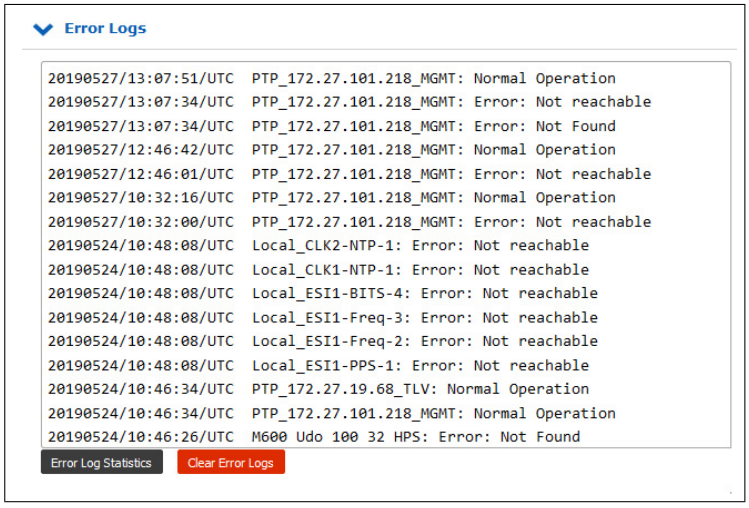
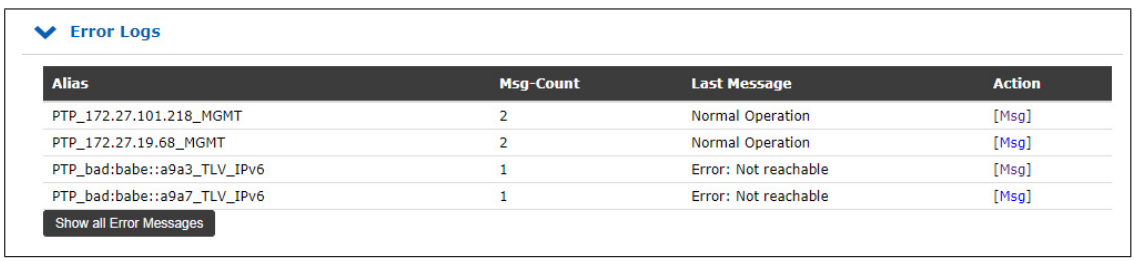


Illustration: Error log messages for a selected monitored node.

The button "**Show Global Error Logs**" beneath the error log can be used to 'reset' the error log display to its default state, i.e., a list of all error log messages for all monitored nodes. This button will only appear if messages in the "Error Logs" section have been filtered out.



"**Error Log Statistics**" shows a statistical summary of the logs for all monitored nodes. "**Clear Error Logs**" erases all log entries.

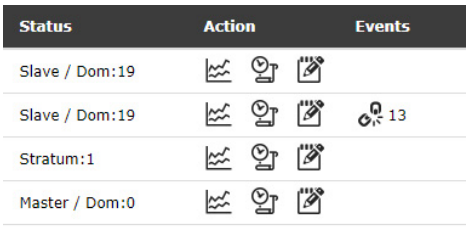


"Edit" Button

The "**Edit**" button can be used to review and adjust all parameters relating to the presentation of the graph. The "**Graph Offset Correction**" in the node settings can be used to adjust the graph with a fixed offset (e.g., to compensate for a known asymmetry in a network or propagation time over a given length of cable). Note that, unlike the "Fixed Offset Correction", this does not affect the logged values—the graph offset value is simply a fixed adjustment for the graph output.

10.1.12.15 Events

The global "Node Monitoring" table shows alerts under the "**Events**" heading as defined for the monitored nodes and are updated every 10 seconds:



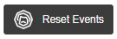
Offset Limit Exceeded

This alarm is triggered whenever the offset limit defined in the node configuration is exceeded (once or several times successively). The number of times that the limit can be exceeded consecutively before an alarm is triggered is determined by the corresponding "Trigger Counter" setting in the node settings.

Not Reachable

This alarm is triggered whenever the node is deemed to be unreachable. The alarm can be triggered upon the first connection failure or following multiple unsuccessful connection attempts and is determined by the corresponding "Trigger Counter" setting in the node settings.

These events are also displayed on the SyncMap.



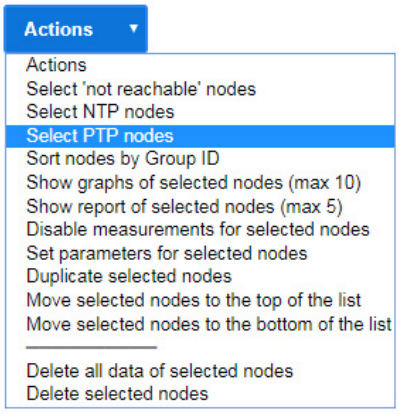
Whenever an "offset limit exceeded" or "not reachable" alert is displayed, the number of occurrences of that event is shown alongside the alert icon in the "**Events**" column. The event counter can be reset using the "**Reset Events**" button located above the Node Monitoring table.

10.1.12.16 Actions Menu

In LTOS 7.00 or later, certain actions can be applied to multiple selected nodes in the table concurrently and nodes can be selected based on certain conditions.

Selecting Nodes

Select the nodes that you wish to manage by either clicking on the checkbox on the left of each node entry or, if you wish to select all nodes together, by clicking on the "+" symbol in the table header. To deselect the selected nodes, either click on the corresponding checkboxes again or select the "-" symbol in the table header to deselect all nodes simultaneously.



Select 'Not Reachable' Nodes:
Selects all nodes whose displayed offset status is "Not Reachable".

Select NTP Nodes:
Selects all monitored NTP nodes.

Select PTP Nodes:
Selects all monitored PTP nodes, both via MGMT and TLV messages.

The option "**Sort Nodes by Group ID**" sorts the entire list based on each node's group ID.

Overviews for All Nodes

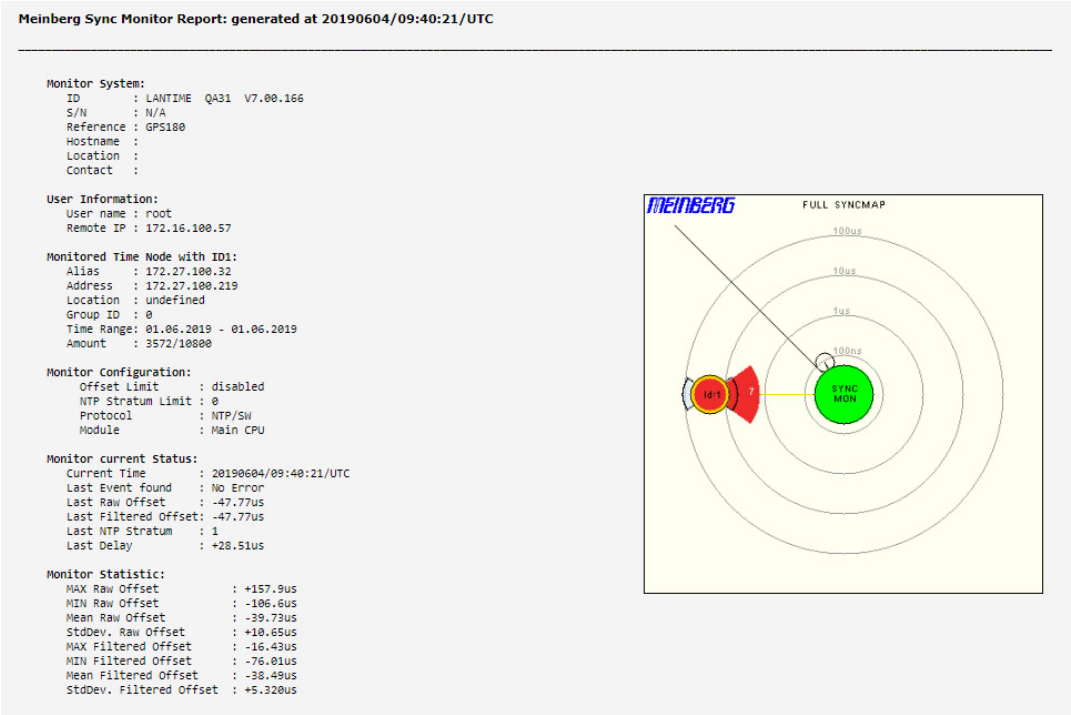
The options "**Show Overview for Current Day**" and "**Show Overview for Time Range**" will only be visible while no nodes have been selected. These options provide a statistical overview of the recorded values properties for all nodes in the table, and also display graphs for the current day or selected time range respectively.

Actions for Selected Nodes

Show Graphs of Selected Nodes (Max. 10):
If you select up to ten nodes in the table, you can have the graphs displayed for these overlaid on top of each other. The default presentation applies to the current day, but you may select a different time period for the graphs.

Show Report of Selected Nodes (Max. 5):
If you select up to five nodes in the table, this option will prepare a report based on the current data for the selected nodes. You will be prompted to enter a time range to form the basis for the report. The report contains the up-to-date status data, the SyncMon configuration, the captured statistical values over the selected period, and a graph illustrating the offset trend.

The report also provides a simplified SyncMap showing only the nodes selected in the table. Each individual node is highlighted in the image and the rest are shown in the background, enabling a comparison of the performance of each node relative to other nodes specified in the report.



Meinberg Sync Monitor Report: generated at 20190604/09:40:21/UTC

Monitor System:
ID : LANTIME QA31 V7.00.166
S/N : N/A
Reference : GPS180
Hostname :
Location :
Contact :

User Information:
User name : root
Remote IP : 172.16.100.57

Monitored Time Node with ID1:
Alias : 172.27.100.32
Address : 172.27.100.219
Location : undefined
Group ID : 0
Time Range: 01.06.2019 - 01.06.2019
Amount : 3572/10800

Monitor Configuration:
Offset Limit : disabled
NTP Stratum Limit : 0
Protocol : NTP/SW
Module : Main CPU

Monitor current Status:
Current Time : 20190604/09:40:21/UTC
Last Event found : No Error
Last Raw Offset : -47.77us
Last Filtered Offset: -47.77us
Last NTP Stratum : 1
Last Delay : +28.51us

Monitor Statistic:
MAX Raw Offset : +157.9us
MIN Raw Offset : -106.6us
Mean Raw Offset : -39.73us
StdDev. Raw Offset : +10.65us
MAX Filtered Offset : -16.43us
MIN Filtered Offset : -76.01us
Mean Filtered Offset : -38.49us
StdDev. Filtered Offset : +5.320us

Illustration: Report generated for selected nodes in the table. The report contains status information on the selected nodes, the SyncMon configuration, key monitoring statistics, and graphs.

Disable Measurements for Selected Nodes:
Nodes for which measurements are disabled will be displayed as such as in the status. Measurements will no longer be requested or logged for these nodes. Disabling a node sets the the Request Interval to "*Disabled*"; therefore, to restart the measurements, open the configuration page of the node and set the "Request Interval" back to the desired value.

Set Parameters for Selected Nodes:
It is possible to edit specific monitoring parameters for multiple selected nodes simultaneously. Selecting this function will bring up a configuration dialog page in which you can adjust each of the parameters. Once you confirm the changes using the button "**Save Selected Nodes**", the configuration will be applied to all of the nodes that you had previously selected for this action. Only the parameters that you have selected an option for will be adjusted; leaving a field empty means that no changes will be made to the corresponding parameters of those nodes.

Duplicate Selected Nodes:
The selected nodes are copied and added beneath the original nodes. Their parameters can then be modified accordingly.

Move Selected Nodes to the Top of the List:
The selected nodes are moved to the top of the list.

Move Selected Nodes to the Bottom of the List:
The selected nodes are moved to the end of the list.

Delete All Data of Selected Nodes:
The logged measurements for the selected nodes are permanently deleted from the configured storage medium.

Delete Selected Nodes:
The selected nodes are removed from the node monitoring table. The measurements taken up to this point for those nodes will be preserved; if you wish to delete that data as well, you should select "**Delete All Data of Selected Nodes**" *first*. Deleted nodes can of course be re-added later via a search or manual entry.

10.1.12.17 SyncMap

SyncMap is a graphical polar diagram representation of monitored nodes in a network. SyncMap is designed to provide an at-a-glance perspective of the synchronization state of all monitored devices in a complex network structure.

Monitored devices are referred to as nodes. Nodes must support any of the following signal types: NTP (RFC1305), PTP (IEEE 1588v1 or IEEE 1588v2), PPS (in conjunction with an IMS-ESI card). Please note that PTPv1 nodes will only be displayed on LTOS 7.06.007 or later.

It enables the absolute offset values of the monitored nodes to be visualized within pre-defined offset limits. Data can be displayed in accordance with the current node status over a selectable time period (e.g., one day). It is also possible to generate an animation showing the changes to the monitored nodes over the past 60 minutes, with SyncMaps generated once every minute.

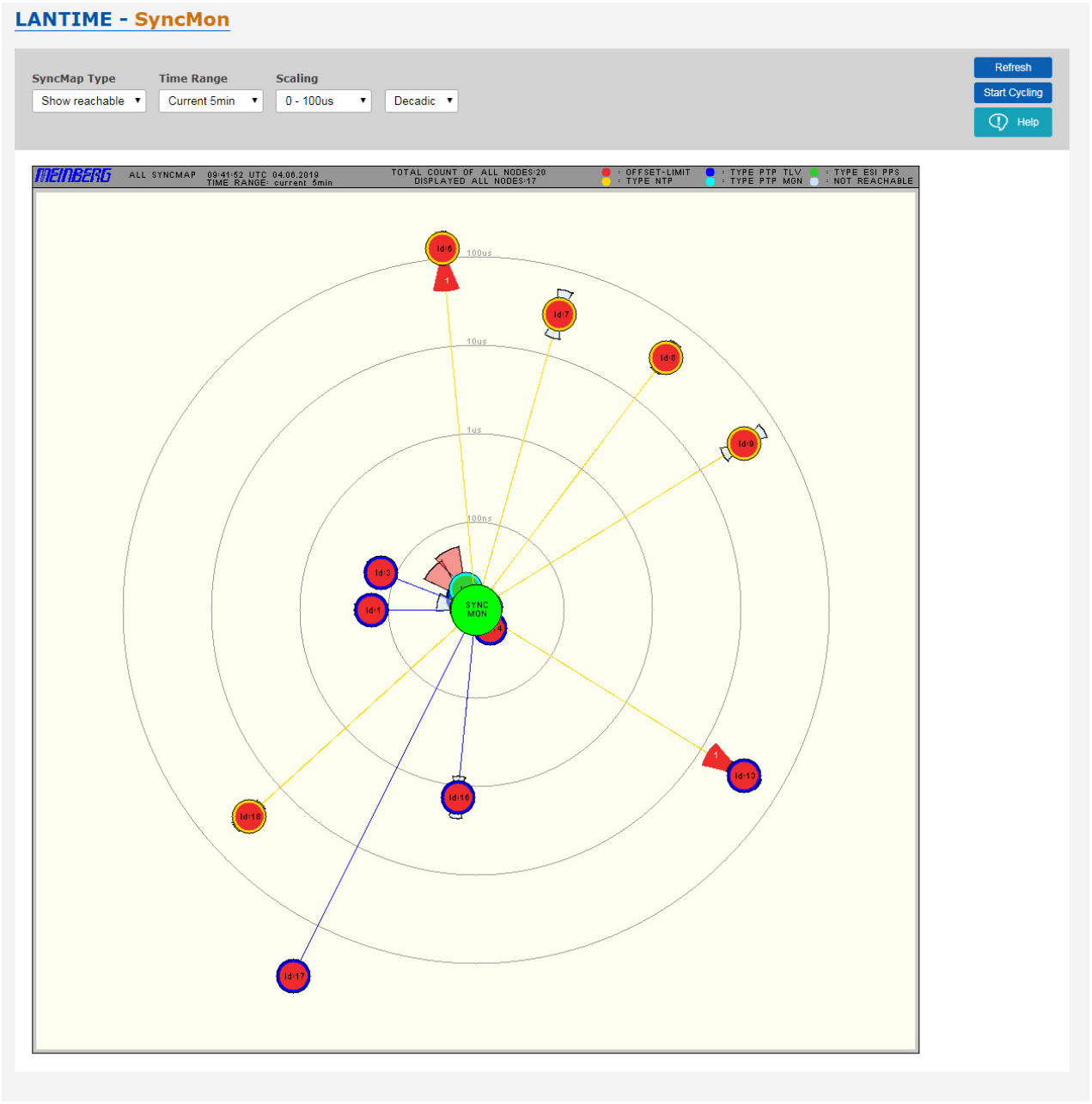


Illustration: The SyncMap as a graphical representation of the monitored nodes in a network, visualized as a polar diagram. It can display nodes which support NTP, PTP (IEEE 1588v1, IEEE 1588v2) or PPS signals.

Each monitored node is represented as a circle containing different statistical information.

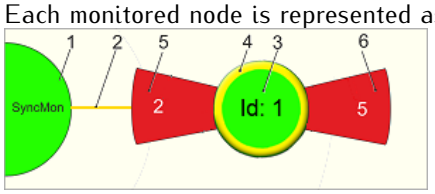


Illustration: A representation of a node in SyncMap.

The reference time monitor "SyncMon" with its reference clock is shown in the middle [1]. This represents a time reference with a disciplined oscillator (which may be synchronized by GPS, GLN, DCF77, Galileo, BeiDou, or some other external reference). The SyncMon node in the center [1] will be green as long as the reference clock is synchronized.

There are four concentric circles around the SyncMon node that represent the scale of the polar diagram. All 'satellite nodes' [3] are connected to the central SyncMon node by a node [2]. The distance between the satellite node and SyncMon represents the absolute average time offset between the time monitor SyncMon and each individual satellite node. The mean value is calculated over the selected time period. Each satellite node is shown as a circle with two fill colors: the inside fill color [3] represents the status, while the outside ring [4] represents the type.

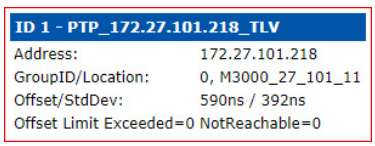
Status:	Green	= Offset has not exceeded limit
	Red	= Offset has exceeded limit or maximum scale has been exceeded
Type:	Yellow	= NTP
	Dark blue	= PTP with TLV (PTPv2 only)
	Light blue	= PTP with Management Messages (PTPv1 or PTPv2)
	Green	= ESI PPS
	Gray	= Not available

The satellite nodes also represent certain statistical values. The standard deviation, which represents the temporal jitter of the measurements relative to the mean value, is represented by two 'wings' ([5] and [6]). The wing facing SyncMon [5] represents the number of "not reachable" events, while the wing facing **away** from SyncMon [6] shows the number of times that the offset limit has been exceeded.

If a wing is red, this means that the standard deviation exceeds half of the configured scale. For example: If the average deviation is in a range of 1 μs - 10 μs and the largest maximum found is > 5 μs, the wing will be shown in red. If not, it will be blue.

If an offset limit is exceeded or a node is "not reachable", the wing will turn dark red and will show a value in white that represents the number of corresponding events.

Hovering over a node with the mouse without clicking will bring up an information box in SyncMap, showing some statistical values:



Left-clicking on a specific node in SyncMap will open the following context menu:

"**Show Graphic**" will open the corresponding graph for that node.

"**Reset Event Counter**" resets the "not reachable" and "offset limit exceeded" counters and changes the SyncMap accordingly.

"**Edit Node Parameters**" opens the configuration page for that node (see Using SyncMon for Status Monitoring and Configuration via Web Interface for further information).

"**Close This Menu**" closes the context menu.

Example of a Complete SyncMap
The image below shows a SyncMap for a network with 250 monitored NTP nodes running on a SyncFire server. This is based on an actual measurement of our test networks used for burn-in testing in LANTIME production. The nodes in red are DCF77 receivers for which no signal propagation value has been entered to account for the distance between the transmitter and receiver.

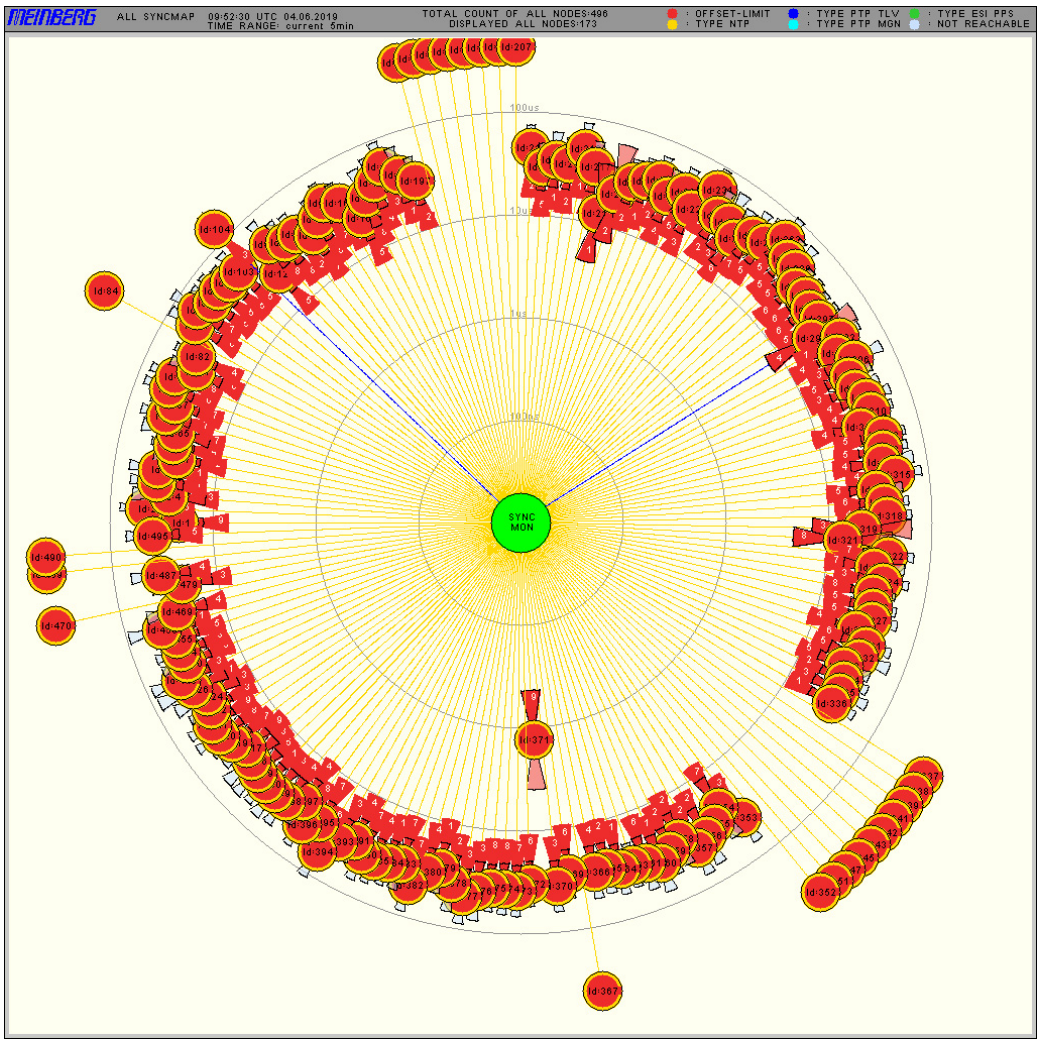


Illustration: An example of a SyncMap with 250 nodes.

SyncMap Type:

- Show Reachable: Nodes that are currently reachable are shown in the SyncMap.
- Show All Nodes: All nodes configured in the monitoring list are shown in the SyncMap, including unreachable ones.
- Show NTP only: Only monitored NTP nodes are shown in the SyncMap. NTP nodes are shown with a yellow outer ring in the SyncMap.
- Show PTP only: Only monitored PTP nodes are shown in the SyncMap. PTP nodes monitored via TLV are shown with a dark blue outer ring in the SyncMap, while PTP nodes monitored via management messages are represented by a light blue outer ring.

Time Range: The SyncMap can be generated from monitoring data sampled over the past 30 minutes, 5 minutes, 24 hours, or within a manually selected time range. Statistical values are also calculated based on the data from the selected time period.

Scaling: There are various options for scaling, ranging from 0–100 ns to 0–10 ms, rising in power-of-10 intervals. The scale of the SyncMap itself can be set to a linear (equidistant intervals between circles) or decadic logarithmic scale (increasing at power-of-ten intervals between circles). For PTP nodes, a 0–10 μs scale is advisable, while for NTP, scales of 0–1 ms or 0–10 ms would be recommended.

Refresh: Immediately refreshes the SyncMap based on the statistics currently available for each single node. A new SyncMap with the selected time range is generated—this function has same effect as reloading the page with the latest measurements.

Start Cycling: Activates the SyncMap animation mode. This generates a new SyncMap once a minute based on the latest measurements. The last 60 SyncMaps will then be displayed as an animation. New sequences begin with an empty SyncMap. The time range for the statistics is set by default to 5 minutes.

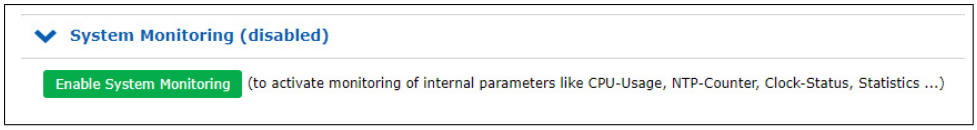
The number of SyncMap images stored in RAM in this automatic refresh mode is limited to 1000 on LANTIME systems with 2 GB RAMN (e.g., IMS-CPU-G15G2 module) or on SyncFire systems.

Help: Displays the online help page for the SyncMap function.

10.1.12.18 System Monitoring

System Monitoring is used to monitor internal signals of the LANTIME system that are not associated with the monitored network—these include data such as CPU utilization as well as parameters related to the local NTP server, ESI inputs, MRS references, and the reference clock. The number and type of internal signals will depend on the hardware components present in the LANTIME system.

System Monitoring is an optional function and is disabled by default. It can be enabled via the menu "**SyncMon → System Settings → SyncMon Configuration**" using the drop-down menu "**Enable System Monitoring**" or more directly via the panel "**System Monitoring**".



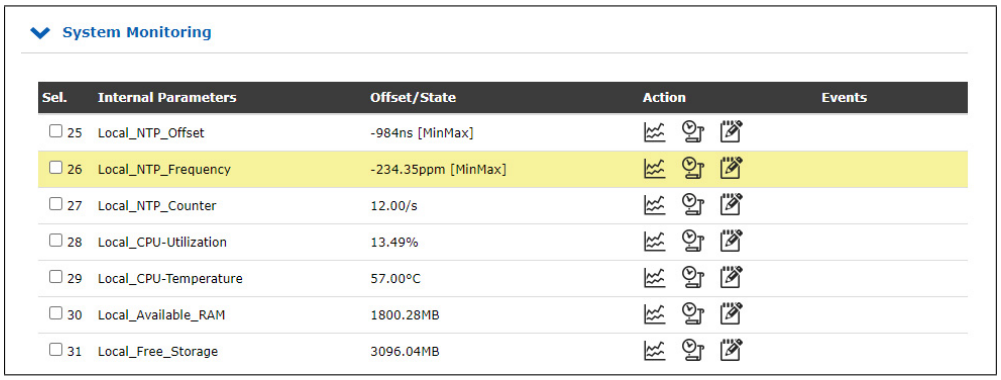
To disable System Monitoring again, simply select "*No*" via the same drop-down menu "**SyncMon → System Settings → SyncMon Configuration → Enable System Monitoring**".

While System Monitoring is enabled, all signals are measured and logged automatically in the same way as with network node monitoring.

The number of MRS references (CLK1-GPS-0, CLK1-NTP-1, CLK1-PTP-2, etc.) depends on the activated source priorities for each reference clock—this can be configured via "**MRS Settings**" in the "**Clock**" menu of the Web Interface for each reference clock used.

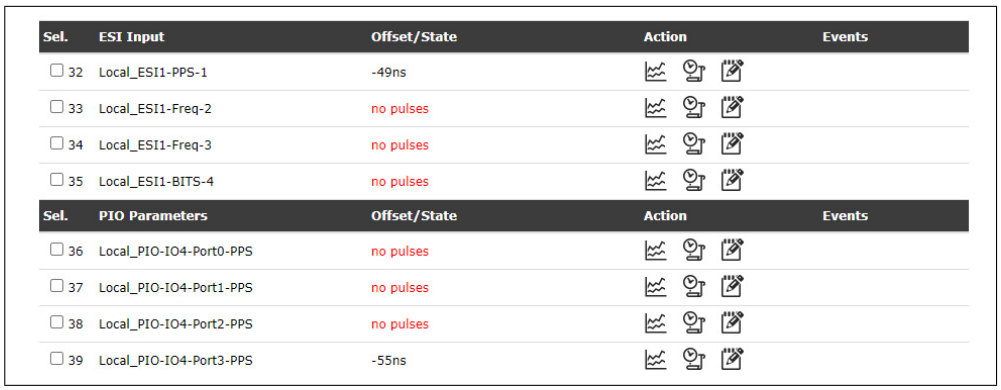
Each node in the "**System Monitoring**" panel can be selected and displayed in a graph alongside the monitored network nodes.

List of Possible Sensors in SyncMon:



Internal Parameters:

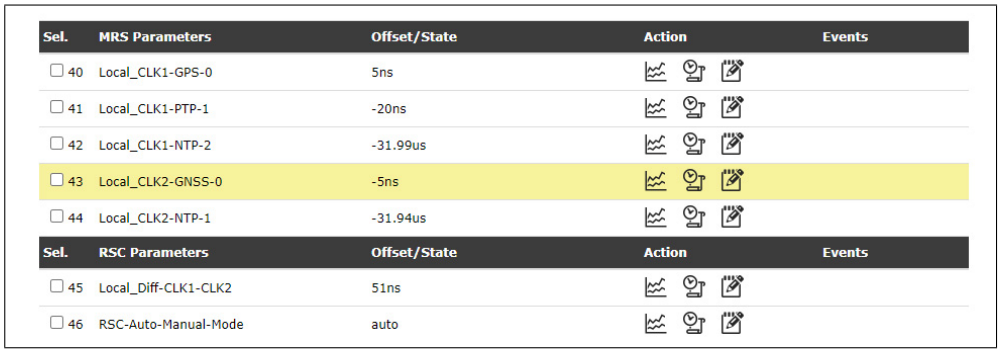
Local NTP Offset
Local NTP Frequency
NTP Counter
Local CPU Utilization
Local CPU Temperature
Free RAM Memory of System
Available Flash Storage of System



Sel.	ESI Input	Offset/State	Action	Events
32	Local_ESI1-PPS-1	-49ns		
33	Local_ESI1-Freq-2	no pulses		
34	Local_ESI1-Freq-3	no pulses		
35	Local_ESI1-BITS-4	no pulses		
Sel.	**PIO Parameters**	**Offset/State**	**Action**	**Events**
36	Local_PIO-IO4-Port0-PPS	no pulses		
37	Local_PIO-IO4-Port1-PPS	no pulses		
38	Local_PIO-IO4-Port2-PPS	no pulses		
39	Local_PIO-IO4-Port3-PPS	-55ns		

ESI Input:
ESI PPS In
ESI Freq In
ESI BITS In

PIO Parameters:
PIO PPS In

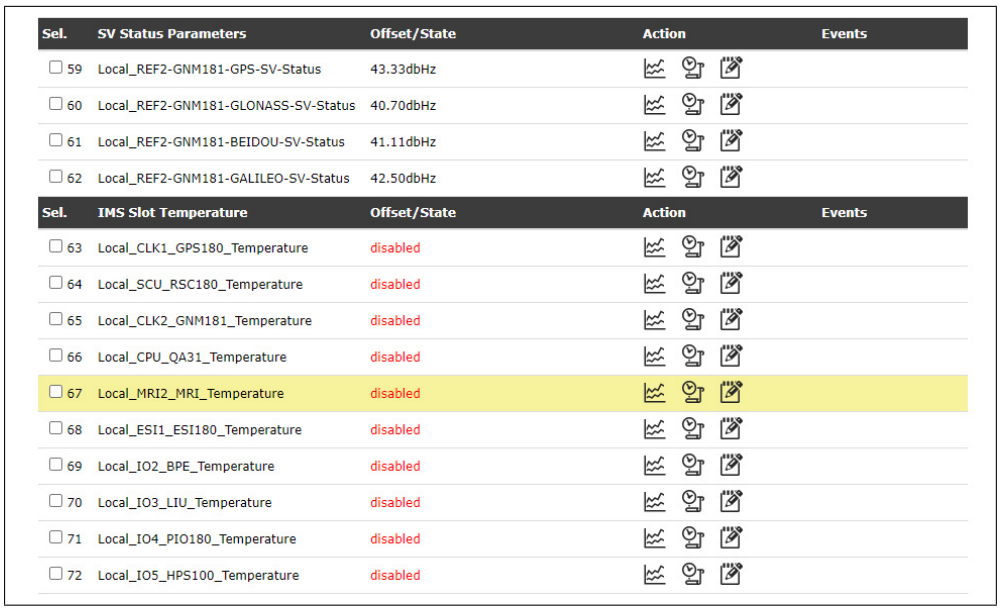


Sel.	MRS Parameters	Offset/State	Action	Events
40	Local_CLK1-GPS-0	5ns		
41	Local_CLK1-PTP-1	-20ns		
42	Local_CLK1-NTP-2	-31.99us		
43	Local_CLK2-GNSS-0	-5ns		
44	Local_CLK2-NTP-1	-31.94us		
Sel.	**RSC Parameters**	**Offset/State**	**Action**	**Events**
45	Local_Diff-CLK1-CLK2	51ns		
46	RSC-Auto-Manual-Mode	auto		

MRS Reference Inputs:
Standard GPS
10 MHz input frequency
PPS input signal
Combined 10 MHz plus PPS
IRIG input
Network Time Protocol (NTP)
Precision Time Protocol (PTP/IEEE1588)
Fixed frequency
PPS plus time string
Variable input signal via GPIO
DCF77 (pseudo-random noise)
Long-wave receiver. e.g., DCF77 AM, WWVB, MSF, JJY
GNSS receiver

RSC Parameters:
Local difference between both clocks
RSC auto/manual mode

For Each Reference Clock:
- Refclock-State
- MRS-SubState
- Refclock-Usage
- Refclock-DCF-Field
- Refclock-DCF-Correlation
- Refclock-Sat-in-view
- Refclock-good-Sat
- Position change



Sel.	SV Status Parameters	Offset/State	Action	Events
59	Local_REF2-GNM181-GPS-SV-Status	43.33dbHz		
60	Local_REF2-GNM181-GLONASS-SV-Status	40.70dbHz		
61	Local_REF2-GNM181-BEIDOU-SV-Status	41.11dbHz		
62	Local_REF2-GNM181-GALILEO-SV-Status	42.50dbHz		

Sel.	IMS Slot Temperature	Offset/State	Action	Events
63	Local_CLK1_GPS180_Temperature	disabled		
64	Local_SCU_RSC180_Temperature	disabled		
65	Local_CLK2_GNM181_Temperature	disabled		
66	Local_CPU_QA31_Temperature	disabled		
67	Local_MRI2_MRI_Temperature	disabled		
68	Local_ESI1_ESI180_Temperature	disabled		
69	Local_IO2_BPE_Temperature	disabled		
70	Local_IO3_LIU_Temperature	disabled		
71	Local_IO4_PIO180_Temperature	disabled		
72	Local_IO5_HPS100_Temperature	disabled		

SV Status Parameters:
- GPS SV Status
- GLONASS SV Status
- BEIDOU SV Status
- GALILEO SV Status

IMS Slot Temperature: CLK, SCU, CPU, MRI, ESI, IO

10.1.12.19 Local NTP Counter

A LANTIME system automatically counts all network packets arriving at UDP port 123 of every available network interface. The current value is displayed in the "**System Monitoring**" table under "**Local_NTP_Counter**" and the evolution of this value over time can be shown in a graph by clicking on the graph icon. The red line in this graph shows the number of NTP packets received over a specified time period.

10.1.12.20 Error Logs

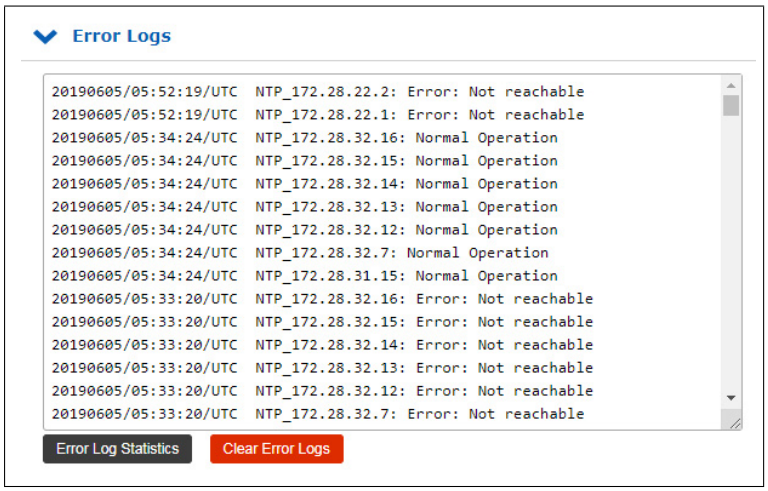


Illustration: Log messages for all monitored nodes.

The general error log allows you to track all error events related to all monitored nodes.

Error Log Statistics: This performs an analysis of the messages in the error log and generates a statistical report. This allows you to identify which nodes most commonly generate error messages.

Clear Error Logs: This button can be used to erase all messages in the error log to date.

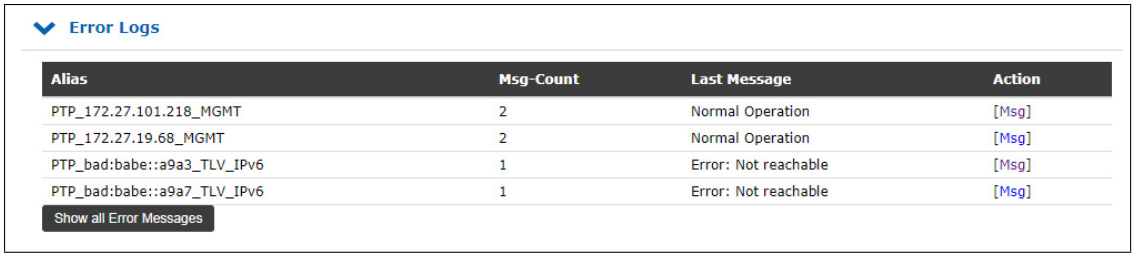


Figure: Error Log Statistics.

10.1.12.21 System Settings

The menu "**System Settings**" shows the storage space currently available on the selected storage medium (internal or external) as well as the number of days that the system expects to be able to store, depending on the number of monitored nodes and the logging interval. It also contains a number of system-related functions and options.

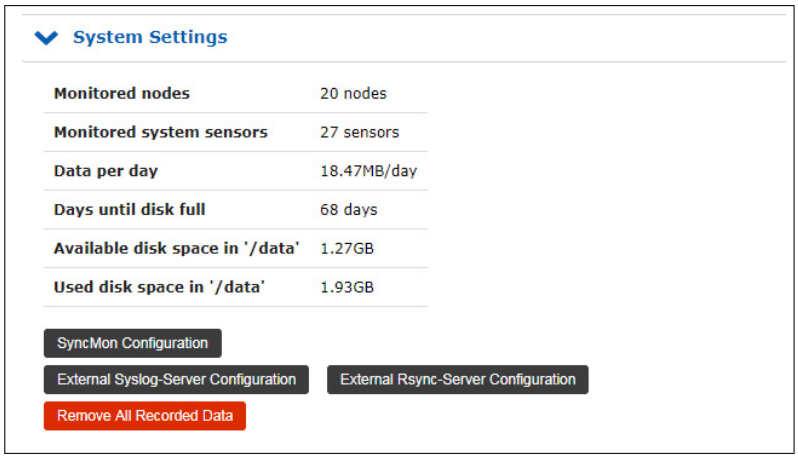


Illustration: Status of the storage medium, available storage space, and archiving options for log files.

Monitored Nodes shows how many external nodes are currently being monitored.

Monitored System Sensors shows how many internal system nodes are currently being monitored.

Data per Day shows how much data is expected to be generated with the current SyncMon monitoring configuration. The corresponding value "**Days Until Disk Full**" is derived from this to enable you to identify the timeframe over which data can be stored on the selected storage medium.

"**Available Disk Space**" shows how much free space is left on the selected storage medium, while "**Used Disk Space**" shows how much space on the selected storage medium has already been used.

The load on the system CPU will vary depending on the number of nodes (up to 1,000 nodes are possible) and the corresponding request and logging intervals.

Important!

It is important to consider system capacity utilization when configuring SyncMon. With large numbers of nodes and high-frequency request and logging intervals, the amount of data generated will be particularly high. The performance of the NTP server may suffer accordingly.

Examples of System Use:

- A single monitoring node with a logging interval of 64s will generate around 110 KB of data per day. A single monitoring node with a logging interval of 1s will store data 64 times as often, generating 64 times as much data accordingly, i.e., around 7 MB.
- 10 monitoring nodes with a logging interval of 1s will store 70 MB per day. If the selected storage medium has 400 MB of free space, this will allow five days of data to be stored on it.
- 100 monitoring nodes with a logging interval of 1s will store 700 MB per day. If the selected storage medium has 400 MB of free space, the space will be exhausted before the end of the first day; as a result, the recording will cease at that point. The log rotation for SyncMon takes effect at 00:00 UTC, resulting in the erasure of files that are older than two days. This scenario results in a CPU utilization increase of around 10 %.
- 100 monitoring nodes with a request interval of 1s and a logging interval of 64s will store around 12 MB per day. This allows 40 days of data to be stored on the selected storage medium. This scenario results in a CPU utilization increase of around 7 %.
- 900 monitoring nodes with a request interval of 1s and a logging interval of 64s will store around 100 MB per day. This allows 4 days of data to be stored on the selected storage medium. However, this scenario results in a CPU utilization increase of around 45 %, which can impair the performance of the NTP server.

10.1.12.22 SyncMon Configuration

The button "**SyncMon Configuration**" displays a number of system configuration parameters that can be modified:

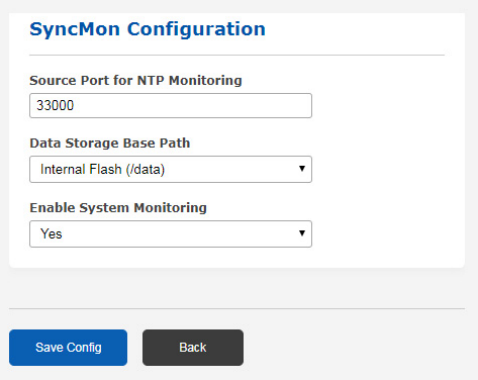


Illustration: System configuration parameters for SyncMon, enabling adjustment of options such as the current path under which data is saved.

Source Port for NTP Monitoring: This parameter determines which port outgoing NTP packets are sent. This is 33000 by default.

Data Storage Base Path: The default path for the internal Compact Flash card is */data*. The option */mnt/usb-storage* will also be provided if an external USB storage medium is connected.

Enable System Monitoring: This enables monitoring of a number of internal system parameters. This allows internal values such as CPU utilization, parameters relating to the local NTP service, ESI inputs, MRS references, and the reference clock to be monitored, depending on the hardware integrated into the system. System Monitoring is disabled by default.

The measurement data of the monitored nodes is stored in separate directories on the selected storage medium. Data is stored separately for each day and each monitored node.

Note: If the selected storage medium is full, the oldest data will be overwritten.

```
/data
    |    /stats
    |         |    /syncmon
    |         |         |      /alias-name1
    |         |         |              |      /ntp_mon_stats.20190501
    |         |         |              |      /ntp_mon_stats.20190502
    |         |         |              |      /ntp_mon_stats.20190503
    |         |         |              |      ...
    |         |         |      /alias-name2
    |         |         |              |      /ntp_mon_stats.20190501
    |         |         |              |      /ntp_mon_stats.20190502
    |         |         |              |      /ntp_mon_stats.20190503
    |         |         |              |      ...
```

Illustration: Example showing the default file structure of the daily records on the storage medium.

Format of the file:

1. MJD: Modified Julian date. This is the continuous number of days since the start of the Julian Period (starting on 1858 Nov 17 - 0:00 Uhr).
2. Time since midnight ins seconds
3. Timestamp (ISO MJD and time since midnight)
4. Raw measured clock offset (if the request interval is lower than the logging interval, the mean value of the measured offsets during the request interval will be recorded).
5. For NTP: Clock offset median (median of the last five offsets measured on request)
   For PTP: Reported offset
6. Path delay in seconds
7. NTP stratum or PTP status
8. 'R' (optional designator for Min/Max values of raw data; if the request interval is lower than the logging interval, the Min/Max values for the raw data will automatically be recorded in the subsequent two lines).
9. See 8. (optional)
10. See 8. (optional)
11. 'M' (optional designator for Min/Max values of MTie values [Maximum Time Interval Error] from PTP nodes supporting this option; if a PTP node supports MTie functionality with enhanced TLVs, the Min/Max values will be stored in the subsequent two lines).
12. See 11. (optional)
13. See 11. (optional)

Extract of monitoring data stored in the daily data files:

Example of NTP daily data files:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay Stratum
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 1
```

Example of NTP daily data files where the request interval is lower than the logging interval:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay St Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.00000129 -0.000000053 0.000007667 1 R -0.01 0.01
```

Example of PTP daily data files:

```
# Day Sec Modified_Julian_day_time Raw_offset Report_offs Path_delay Portstate
58043 21705 2017-10-17T06:01:45+00:00 -0.000000129 -0.000000053 0.000007667 9
```

Example of PTP daily data files with support for MTie functionality:

```
# Day Sec Modified_Julian_day_time Raw_offset Median_offs Path_delay St Min Max
58043 21705 2017-10-17T06:01:45+00:00 -0.00000129 -0.000000053 0.000007667 9 M -0.01 0.01
```

10.1.12.23 External syslog Server Configuration

For the purpose of backing up monitoring data for later analysis, you can have data sent to up three external database servers via the syslog protocol.

The button "**External syslog Server Configuration**" allows you to configure these three external servers to which measurement data is sent at each log interval via the syslog protocol. The corresponding service on the external server must operate as a standard syslog server. Each node measurement performance upon each logging interval is transmitted to each of these servers, unless logging on external servers has been disabled for specific nodes (**Disable Logging on External Server** in node configuration).

This form allows you to configure the destination servers for the data:

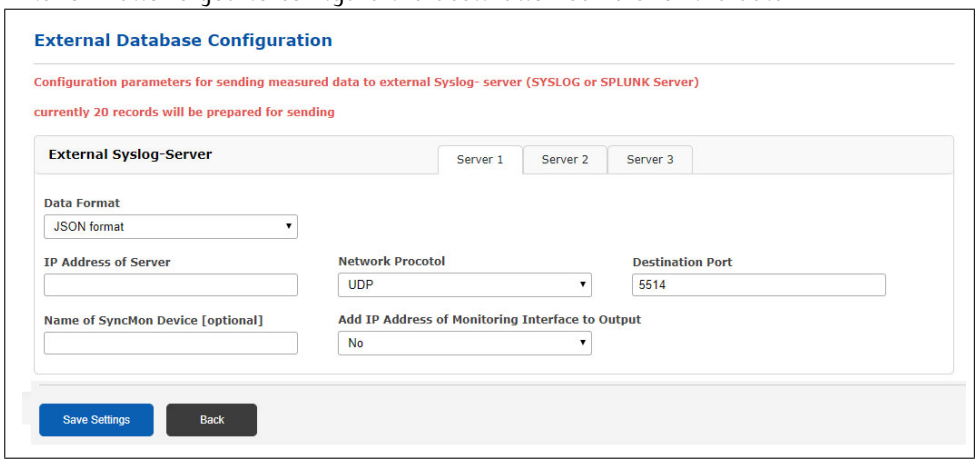


Illustration: Configuration options for external database servers where monitoring data can be stored.

The following parameters can be configured for each of these external servers:

Data Format: This is used to define the output format of the data: MBG Data Format (the standard Meinberg format), SPLUNK-Friendly (key value pairs) or JSON format.

IP Address of Server: This is where the IP address of the syslog server is entered.

Network Protocol: This is where the network protocol handling communication with the syslog server is specified.

Destination Port: This is the port of the syslog server; syslog instances generally expect data via port 514 by default.

Name of SyncMon Device: You can optionally assign a name to the SyncMon device here. This name will be sent along with the measurement data to the syslog server, which facilitates organization of the data from this SyncMon instance on the syslog server.

Add IP Address of Monitoring Interface to Output: If "*Yes*" is selected here, the IP address of the network interface receiving the measurement data will also be included in the output.

Here is an example of the "Meinberg Standard" SyncMon format, which can be sent via the syslog protocol.

```
SyncMon 172.27.100.32 M3000_100_57_NTP_LAN0 58154 34813 2018-02-05T09:40:13+00:00
0.000000494 0.000041453 0.000073266 1 R -0.000011100 0.000041453
```

Please refer to the chapter "Appendix → SyncMon Formats" for further information on SyncMon formats.

10.1.12.24 External rsync Server Configuration

The button "**External rsync Server Configuration**" is used to configure up to three external servers to which measurement data can be copied once an hour or once a day at 00:00 UTC. The corresponding service on the external server must operate as a standard rsync server.

The following form can be used to configure the destination server where you wish to store the data:

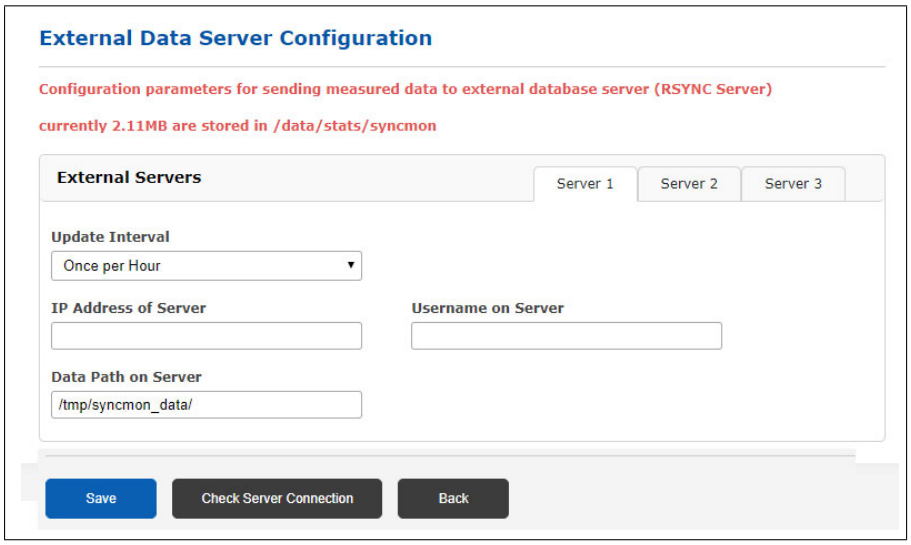


Illustration: Configuring an external rsync server

To have data automatically transmitted once an hour or once a day over *rsync*, you will need to set up an ssh key for the external rsync server:

1. Log into the LANTIME server via an SSH terminal.
2. Check whether identity keys are already available in */root/.ssh/id_rsa.pub*.
3. If not, generate an identity key by entering: *ssh-keygen -t rsa*.
4. Save this identity key permanently by entering: *saveconfig @*.
5. Copy the identity key from the LANTIME to the external rsync server by entering: *ssh-copy-id ip-address-of-RSYNC-server*.

10.1.12.25 Remove All Recorded Data

The button "**Remove All Recorded Data**" is used to erase all measurement data for all nodes irrevocably. When this button is pressed, you will be prompted to confirm that you really wish to perform this action.

10.1.12.26 Accessing SyncMon Status File via CLI

The current status of the monitored nodes as displayed in the Web Interface is stored in an ASCII file */var/log/syncmon_node_status*, which is updated after every full scan of the configured nodes and can be accessed via the CLI.

```
#   Net Sync Monitoring Status with total 15 Nodes (updated  at  ...)

#   Node-Address    NTP:Offset     -filtered        Delay         NTP-Stratum   Auth  MTIE    CntErr     CntErr   Err    Message
#                   PTP:OffsNode   -measured                     PTP-Status                  Offset     Reach
#   ------------------------------------------------------------------------------------------------------------------------------
172.16.100.65:      -0.000113960    0.000055254   0.001663415   2             0     0       3          0        0      Normal Operation
172.16.3.11:        -0.005109100   -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 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:Auth. 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: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
```

Illustration: The status information table, which can be accessed via CLI.

10.1.12.27 Configuration of SyncMon via CLI

The configuration of all monitored nodes is stored in a central text file */etc/mbg/syncmon.cfg*. Each line represents the configuration of a single monitoring node.

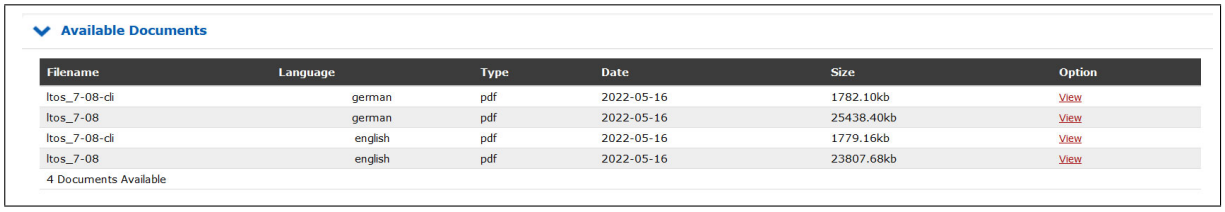
```
# Time Monitoring Node
Configuration
#
@ SourcePort: 33000
@ BaseLogPath: /data
@ BaseCurrDayPath: /data
# Supported Time Protocols: 0:NTP  1:MBG-PTP
# Support ESI Module: Protocol value define the input port
#
#   IP4-Address        CPU-Module   Interface     Protocol   Offset-Limit[s]   Stratum  Req-Intv  Log-Intv   Group  Alias                                Location
NtpKey   NtpKey       NtpKey
#   IPv6 or MAC        (MainCPU=-1)    Name         Index                     Domain                        Index
Index     Type        Secret
#
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
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	:	IPv4/6 or MAC address of the monitoring node
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 type (M=MD5 see NTP documentation)
ksecr	:	NTP key secret (see NTP documentation)

This file can be edited directly within the CLI environment (using *vi*, *nano*) or replaced with an externally prepared file. SyncMon checks this configuration file for changes automatically after every full scan of the configured nodes.

10.1.13 Documentation and Support

This page provides easy access to some documents stored on your LANTIME, in particular the manuals. The list shows the filename, language, file type, date, and size of the documents/notes.



LT_CLI Help

For our LANTIME and SyncFire time server systems a comprehensive documentation for the Command Line Interface and for the RestApi interface is available. In addition, you can download a ZIP archive with an offline version of these HTML help files to your local system and also view the help "offline".

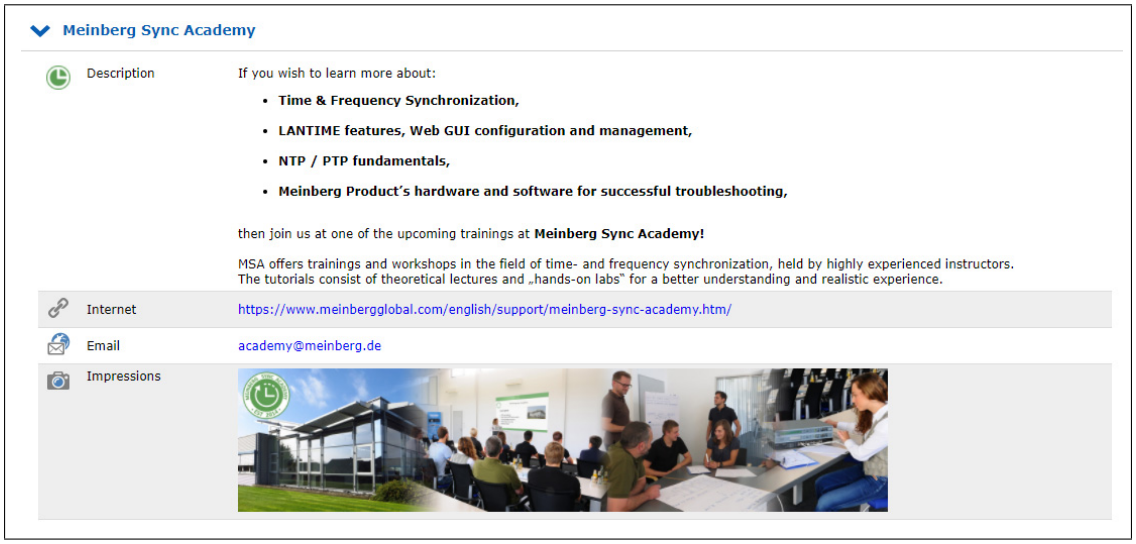
CLI - REST API documentation (online)
https://www.meinbergglobal.com/download/firmware/lantime/v7/lt-cli-help/

CLI - REST API documentation (ZIP archive for offline use*)
https://www.meinbergglobal.com/download/firmware/lantime/v7/lt-cli-help/lt-cli-help.zip

** Using this link, you can download a ZIP archive of the help files to your local PC, unzip it and then view it like a web page in your favorite Internet browser.*

The Support Information chapter provides all necessary information on how to contact Meinberg Technical Support, and also includes a link to Meinberg's firmware update page.

The "Docs & Support" tab also provides some important weblinks and contains information about the Meinberg Sync Academy - MSA.



The Meinberg Sync Academy develops and offers training courses in the field of time and frequency synchronization, covering topics such as NTP, IEEE 1588 PTP, and many more. This part of the LANTIME "Docs & Support" tab provides some basic information about the Sync Academy, along with some links to helpful information at: https://www.meinbergglobal.com/english/support/meinberg-sync-academy.htm

10.2 Via Front Panel Display

10.2.1 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).

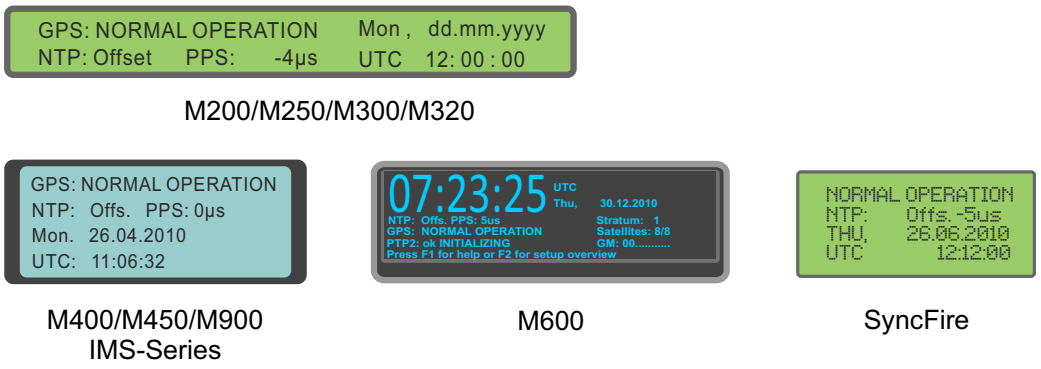


Figure 1.0 - LANTIME Displays

SyncFire	LC-Display, 4 x 20 characters
M200/M250/M300/M320	LC-Display, 2 x 40 characters
M400/M450/M900/IMS	LC-Display, 4 x 16 characters
M600	Vacuum Fluorescent Graphic Display (VFD), 256 x 64 Dots

10.2.1.1 Description of the graphical menu: VF-Display

The graphical menu is used to graphically display offset values [1] between a given input signal [2] 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).

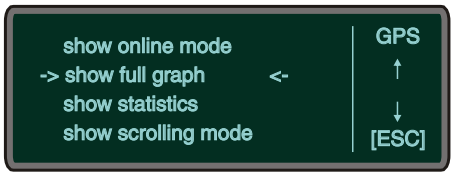
The main menu of the Lantime (where time and date in the selected time zone are displayed).

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.

[1] 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.

[2] Input signals: GPS, PTP, PPS, NTP, TCR, FRQ- which of these input signals are available can be identified from the numerical status (Numerical Status)

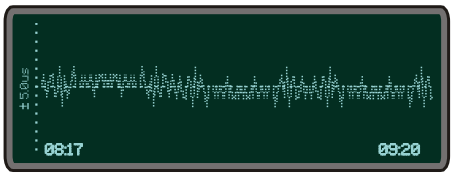
Each graphic mode is displayed within a range of values: [3]

Display of the selected mode (here: SCROLLING MODE)

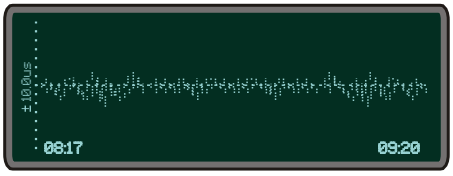
After one of the graphical menu options is selected, the current mode appears for one second on the display. Under the current mode the origin file from which the graphic is generated appears in small fonts.

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)

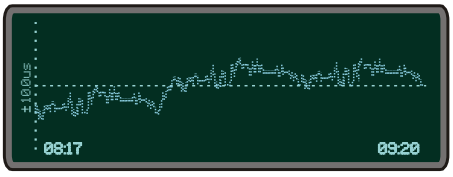


With the ↑ (zoom in) and ↓ (zoom out) buttons the range of the y-axis can be changed any time in order to display graph larger or smaller.
Graph of Online Mode (zoomed out)



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 [4] is displayed.

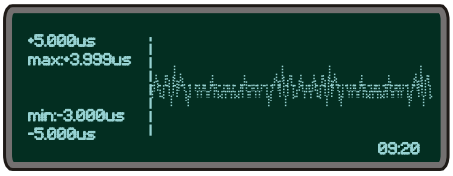
Thus a mean value graph is generated which looks similar to this one: An example of a generated graph with the corresponding range of values (here: FULL GRAPHIC)



[3] 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.
[4] 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.



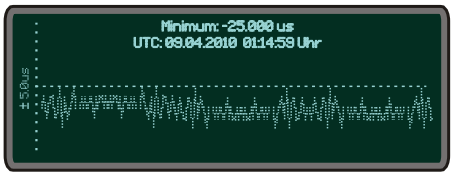
The help menu appears by pressing the F1- information button in the "FULL GRAPHIC MODE". It shows all available options in this mode. Other options are only partially available from here. To end this function one has to press ESC-, OK- or again the F2- button.

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.

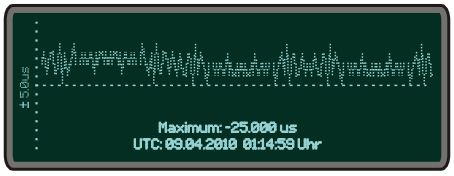
The „Statistic" - option comes next in the graphic menu. When you select it, you can decide if the minimum or the maximum value of the current statistics file shall be displayed or not.

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 [5].

Display of the minimum including the legend:



Display of the maximum including the legend:

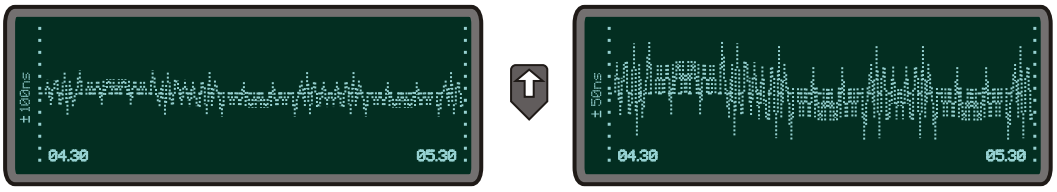


The "SCROLLING MODE" comes as last in the graphical mode

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

[5] 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.

10.2.2 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 excisting 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:

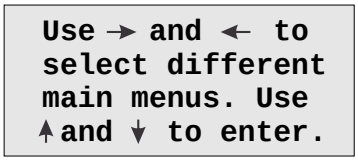
„Ref. Time“
green: the reference clock produce valid time.
red: the reference clock produce no valid time (e.g. not synchronized)

„Time Service“
green: NTP has been synchronized to reference clock.
red: NTP is not synchronous to reference clock or sync to „local clock“

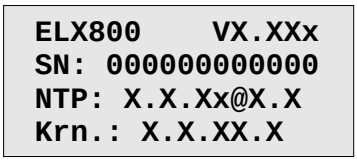
„Network“
green: all watched network ports has been “link up“ detected
red: at least one of the watched network ports (look at „Setup Device Parameter / Check Network Linkup“) is not connected

„Alarm“
off: no error at moment
red: general error – more information will be shown on display.

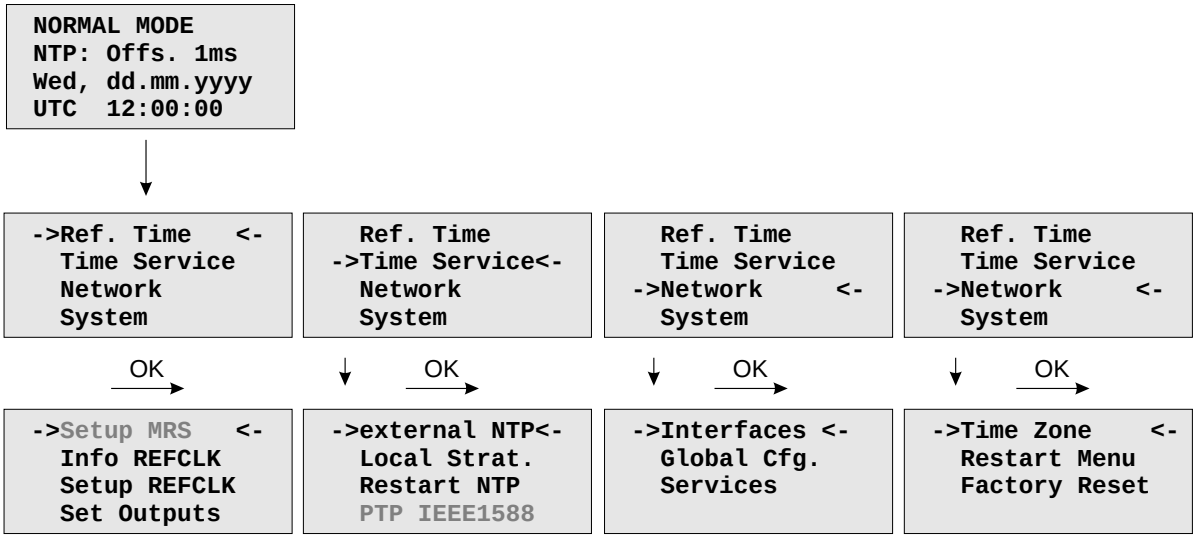
If the symbol „F1“ will be shown in the upper right corner a help page can be displayed when pressing the „F1“ button. When pressing „F1“ from main menu a short description for menu navigation will be displayed:



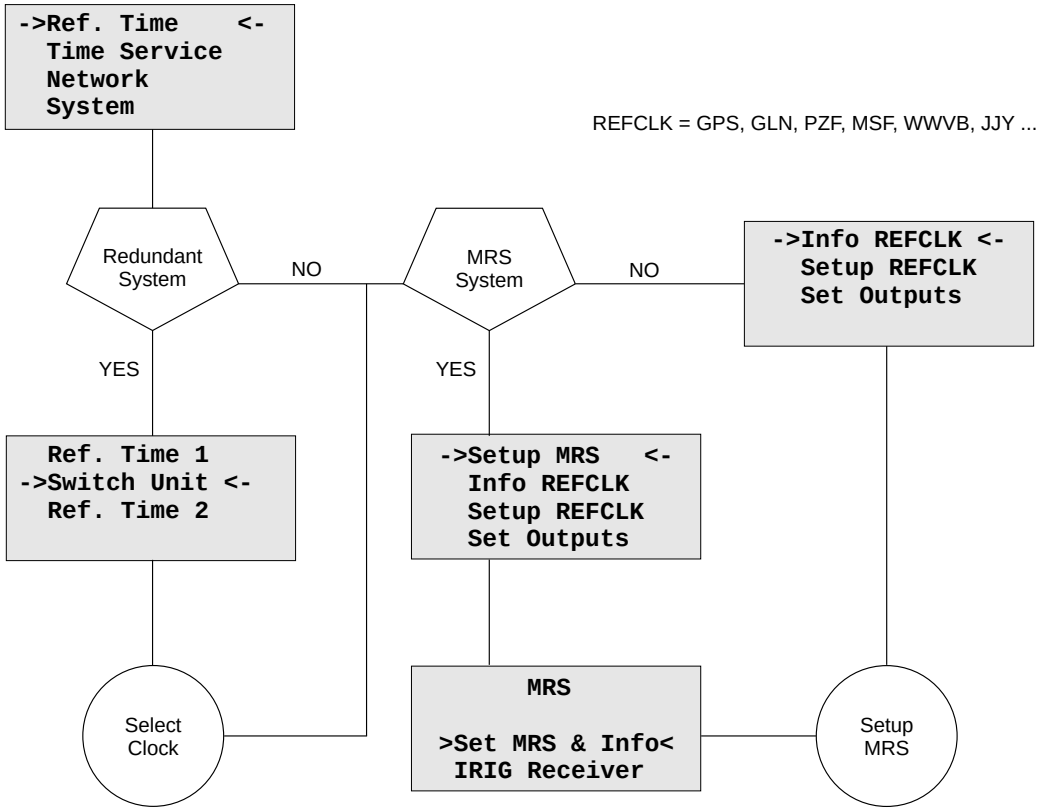
When pressing the „OK“ button from main menu the version of the LANTIME software, the NTP and the LINUX kernel version will be displayed.



The following main menus will be displayed when pressing the arrow buttons:

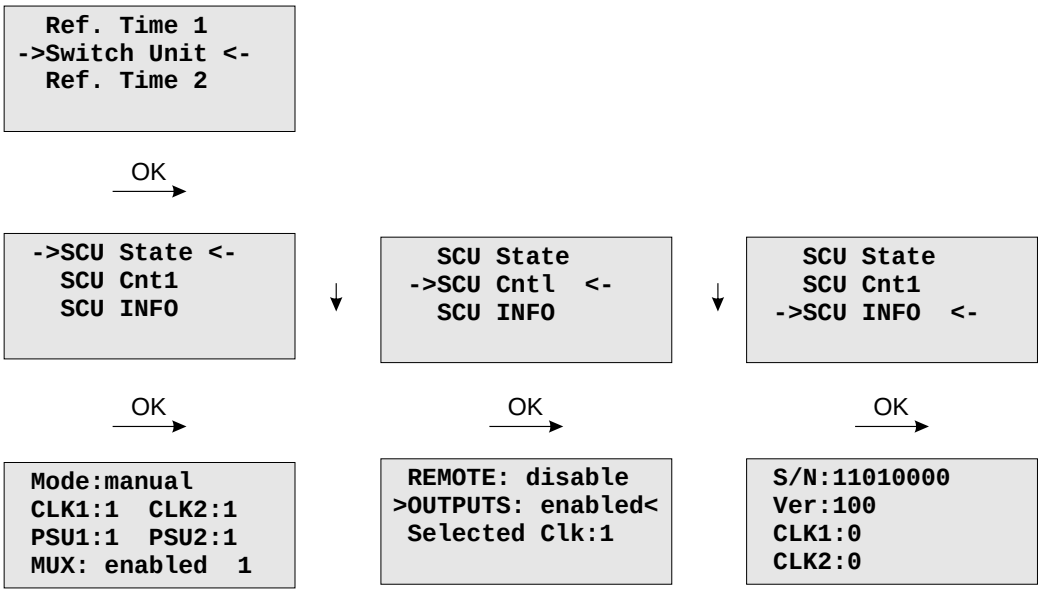


10.2.3 Menu: Reference Time



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.

10.2.3.1 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:

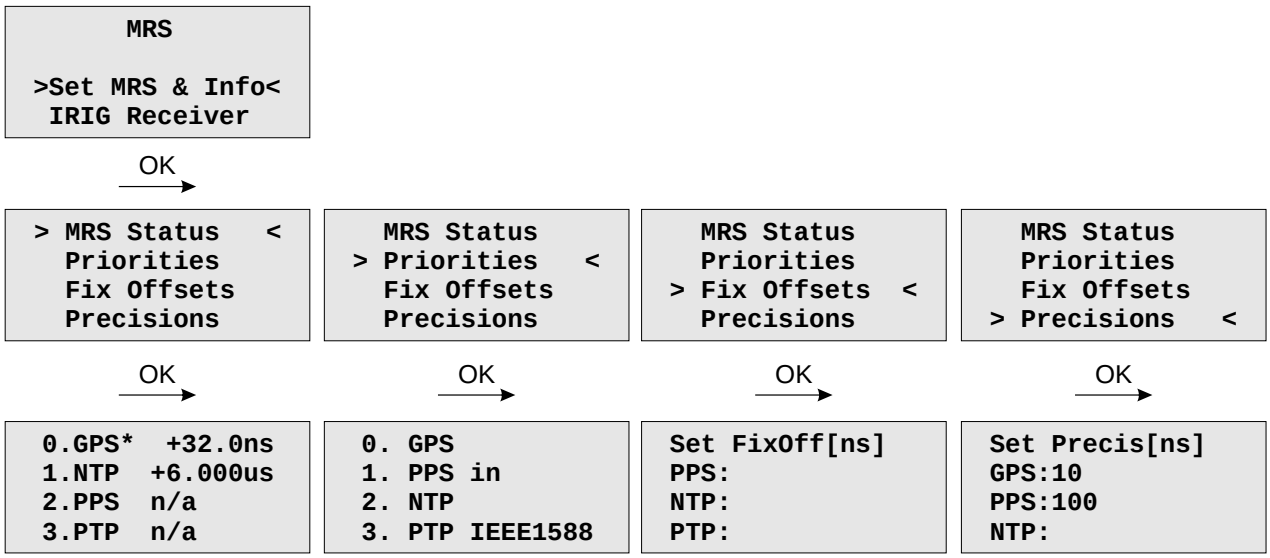
REMOTE: disabled/enabled
disable or enable remote control of the SCU

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.

10.2.3.2 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.

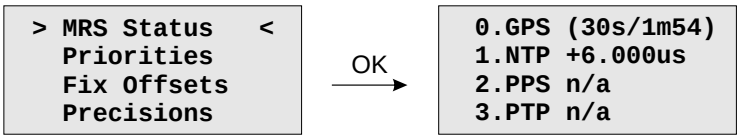
In the next menu the user can define in which order the references will be used to control the internal oscillator. The reference clock with the highest priority will be used always if this is available.

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 then 0 the time for switching to the next reference (hold over time) will be calculated by the following formula:

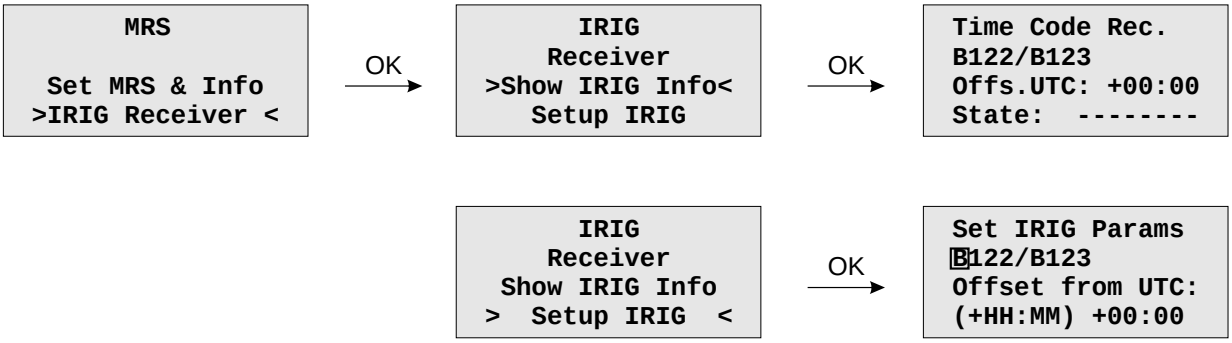
(precision of next reference) / (precision of current master) * constant [s]
The parameter „constant" depends on the quality of the internal oscillator.

Example:
The 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 ((100ns/10ns)*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.

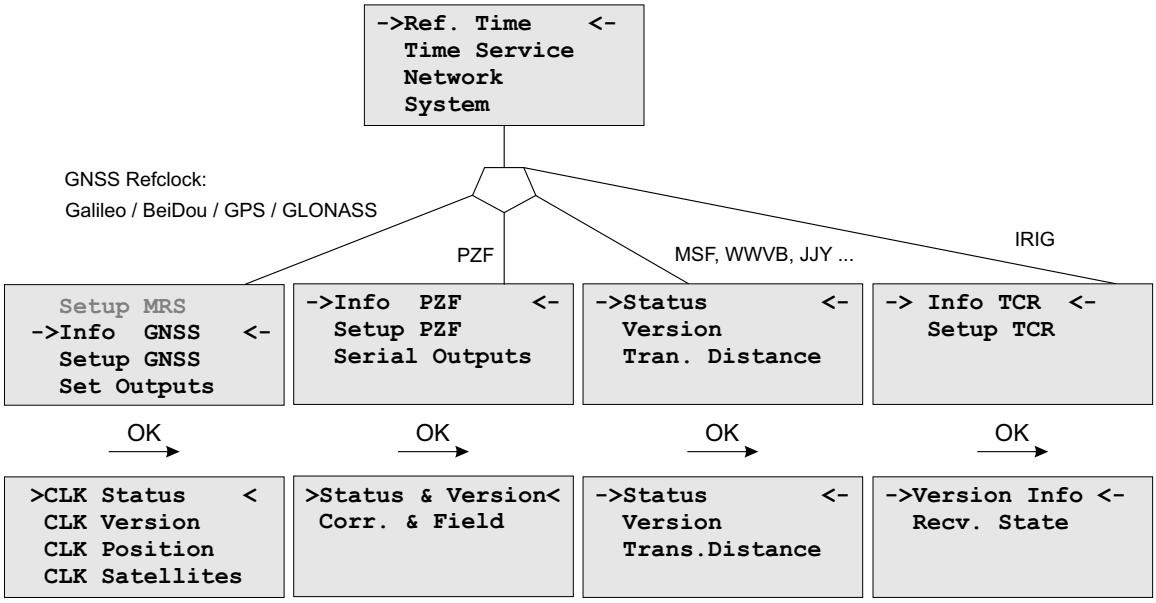


10.2.3.3 Menu Option MRS - Setup Time Code Receiver

With this menu, the parameters for the time code input signals can be displayed and adjusted.

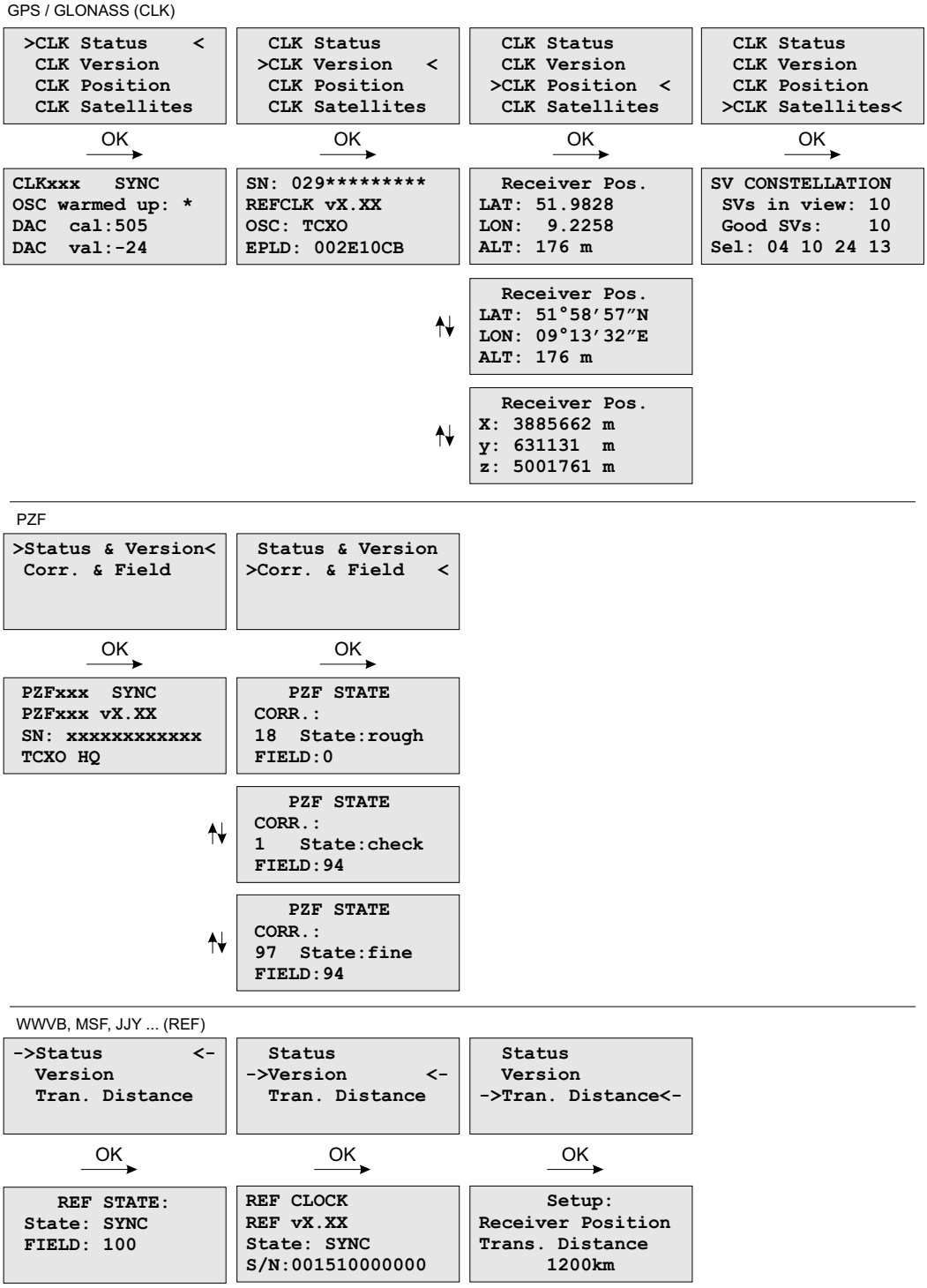


10.2.3.4 Menu: Info Receiver



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.

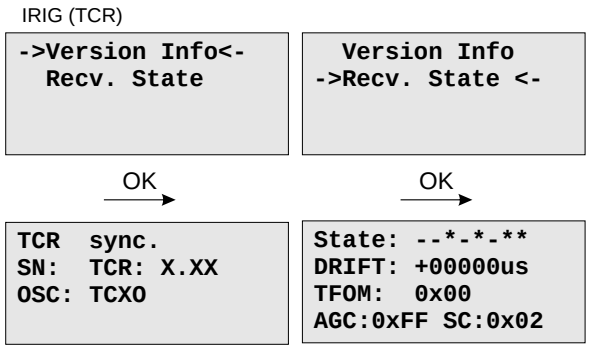
10.2.3.5 Receiver Status and Version



The first line provides a readout of the current state of the clock (either "sync" or "not sync"). The subsequent lines provide information on the firmware version, the serial number of the internal clock, and the integrated oscillator type.

10.2.3.6 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.

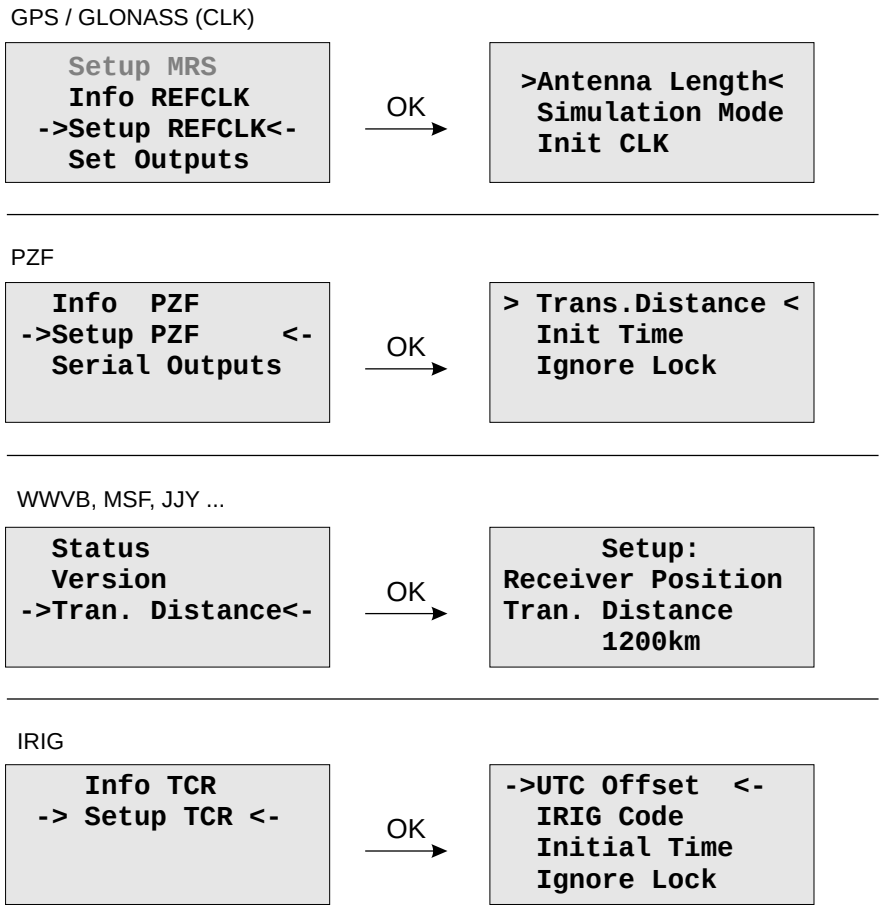
Data available: 'data available' is set if the receiver can read the timecode.

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

10.2.3.7 Menu: Setup Meinberg Receiver



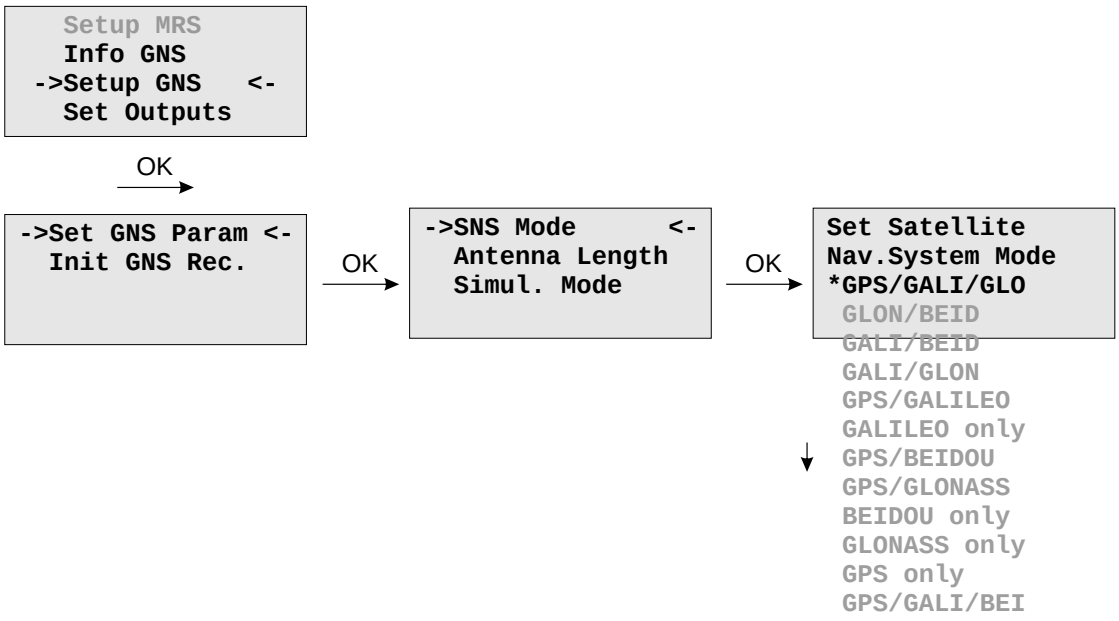
In the Reference Time -> Setup Clock menu the receiver clock parameters can be configure. The antenna cable length of satellite based receivers must be entered here. The GPS and GLONASS reference clocks can be run in simulation mode.

Meinbergs PZF correlation receivers can be operate 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.

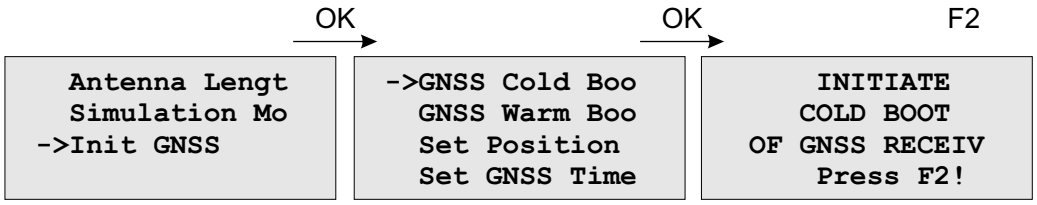
10.2.3.8 SNS Mode - Satellite Navigation System Mode

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:



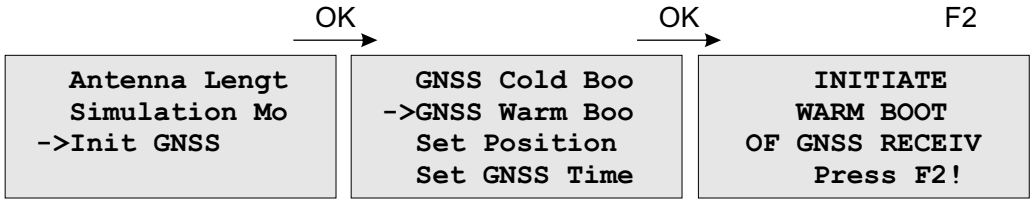
10.2.3.9 Initiate Cold Boot

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.



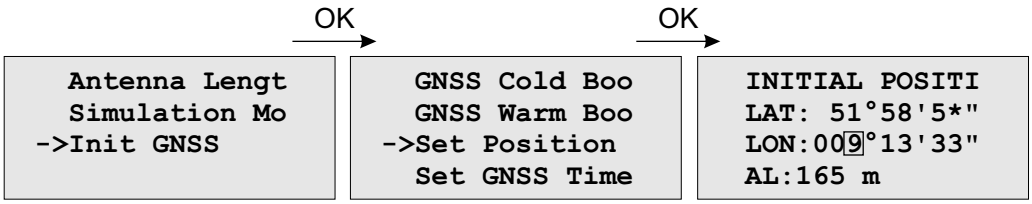
10.2.3.10 Initiate Warm Boot

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 kilometers 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.



10.2.3.11 Init Receiver Position

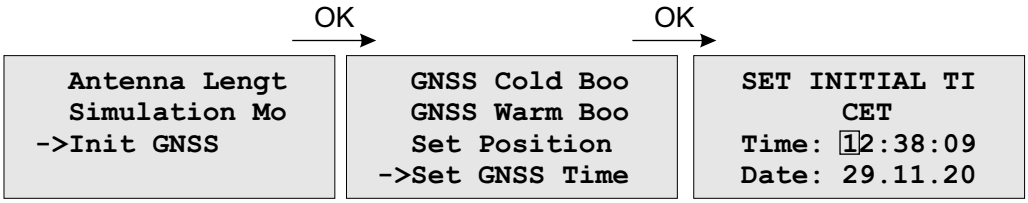
When the receiver is primarily installed at a new location far away from the last position saved in the receiver's memory the satellites in view and their doppler will differ so much from those expected due to the wrong position that the GNSS receiver has to scan for satellites in Warm Boot mode. Making the new approximately known position available to the receiver can avoid Warm Boot and speed up installation.



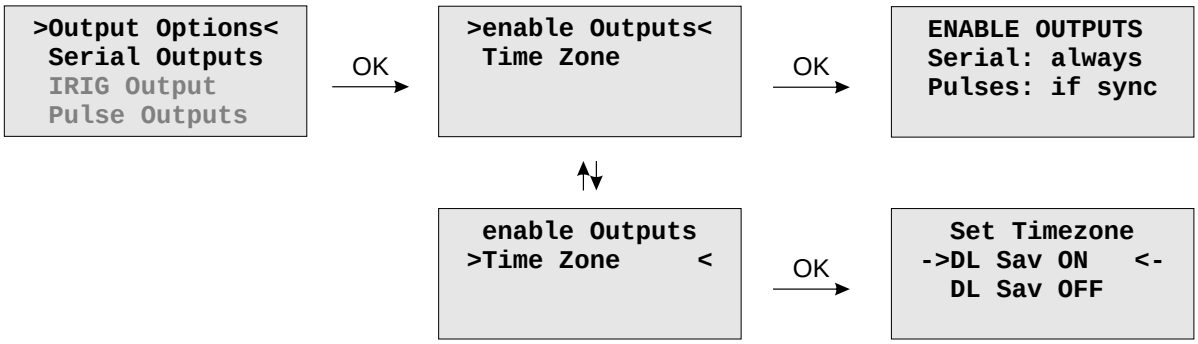
10.2.3.12 Init Receiver Time

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.



10.2.3.13 Menu: Output Options



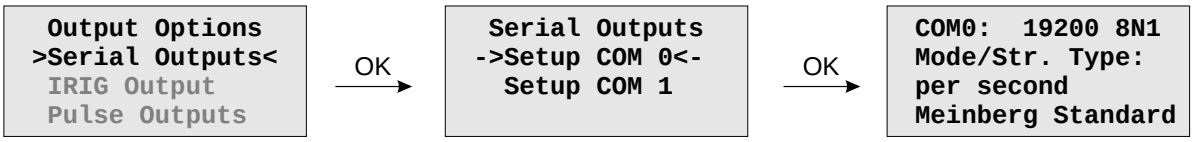
Enable Outputs:
The submenu *Output Options -> Enable Outputs* lets the user configure at which time after power up the serial ports and pulse/frequency outputs are to be enabled. Outputs which are shown to be enabled 'always' will be enabled immediately after power-up. Outputs which are shown to be 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".

10.2.3.14 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.

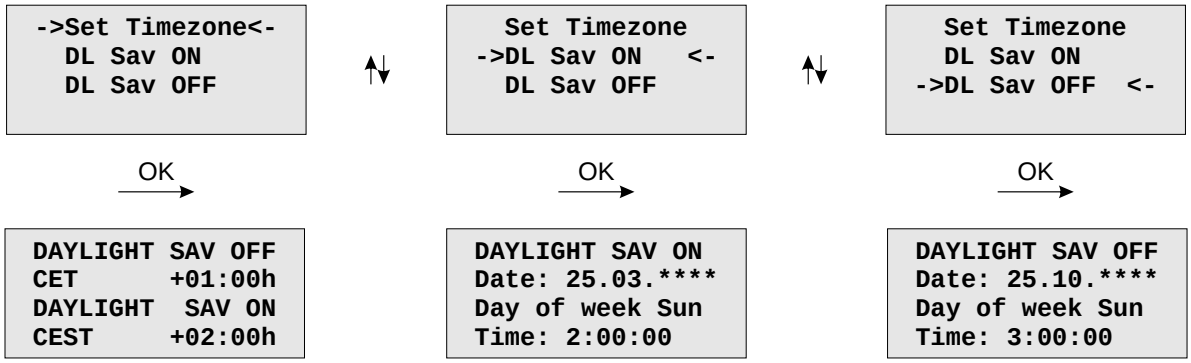
The following time strings can be selected. All time strings are described in the appendix at the end of this documentation.

- 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

10.2.3.15 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.



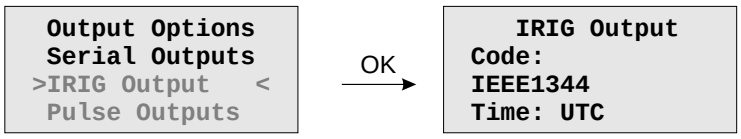
Beginning and ending of daylight saving may either be defined by exact dates for a single year or using an algorithm which allows the receiver to re-compute the effective dates year by year.The figure show how to enter parameters for the automatic mode. If the number of the year is displayed as wildcards '****', 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.

10.2.3.16 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".

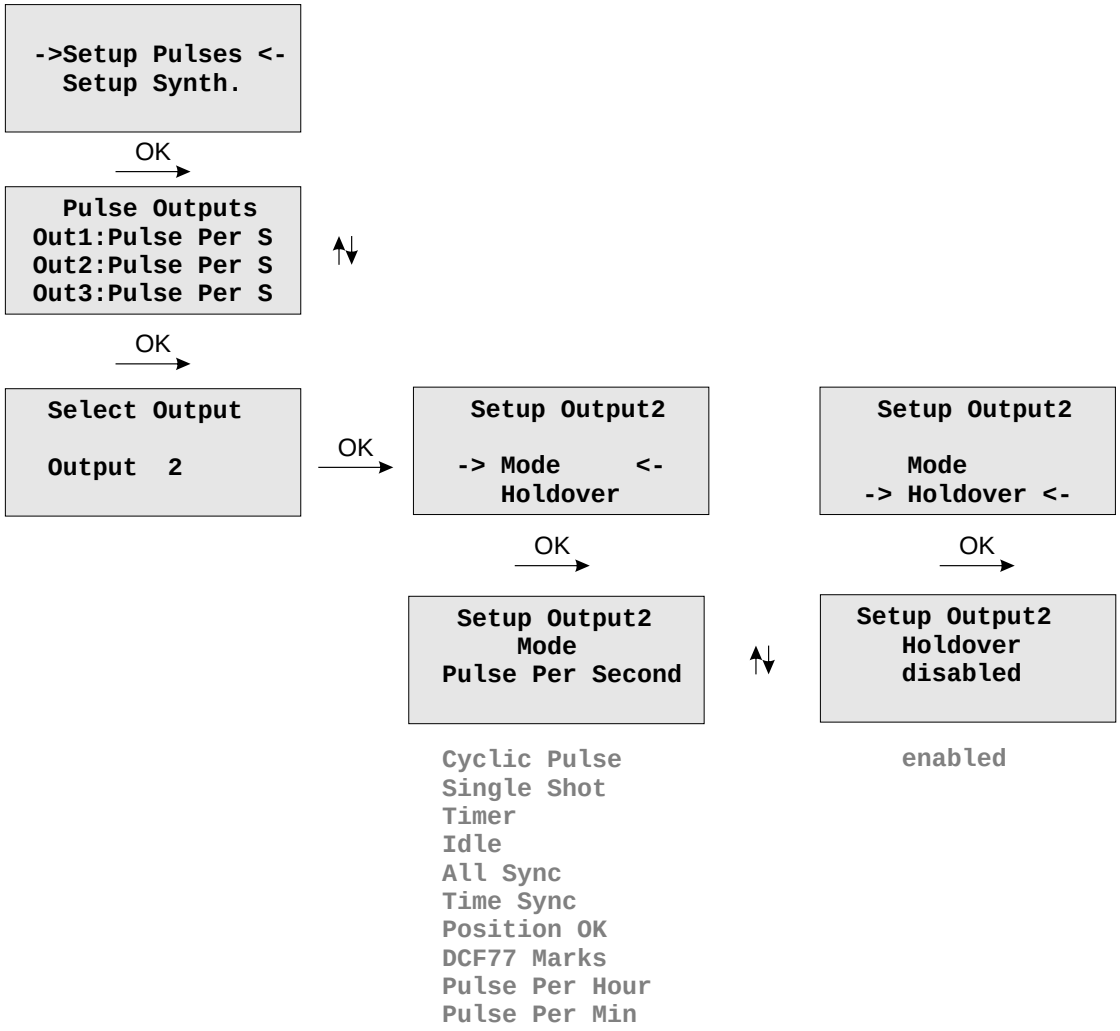
The following codes can be selected:

- IRIG B002+B122
- IRIG B006+B126
- IRIG B007+B127
- AFNOR NF S87-500
- C37.M8
- IEEE1344

Refer to chapter **Timecode** for details.

10.2.3.17 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 switchtime, 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 ouput 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 Singls 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.

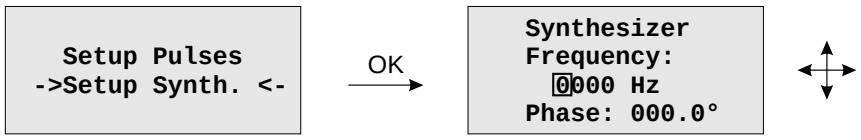
Pulses Per Second, Per Min, Per Hour Modes
These modes generate pulses of defined length once per second, once per minute or once per hour. "Length" determines the pulse length (10 msec...10 sec).

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.

10.2.3.18 Option: Synthesizer Frequency Output

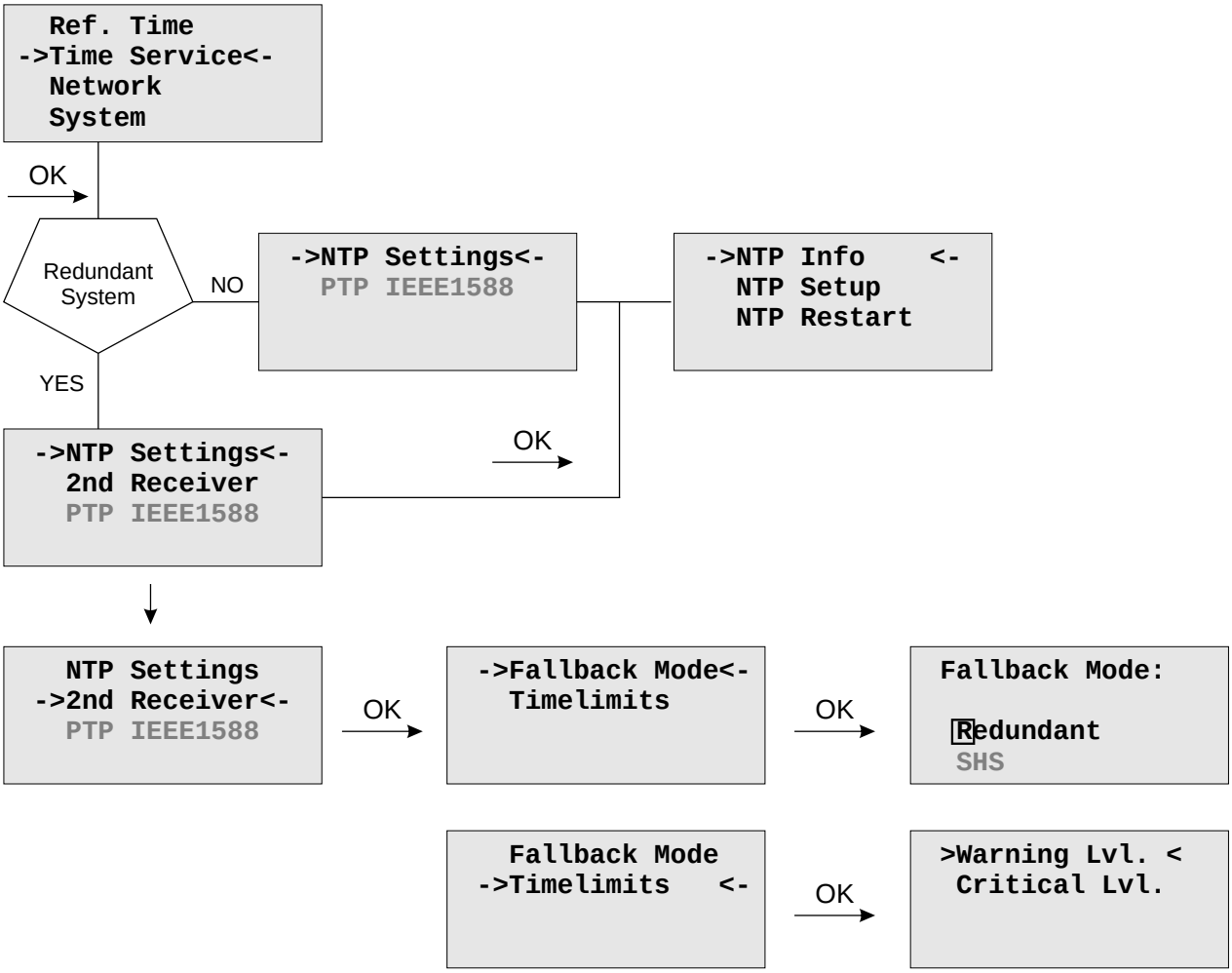


This setup menu lets the user edit the frequency and phase to be generated by the on-board synthesizer. Frequencies from 1/8 Hz up to 10 MHz can be entered using four digits and a range. The range can be selected if the „UP“ or „DOWN“ key is pressed while the cursor is positioned on the frequency's units 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.

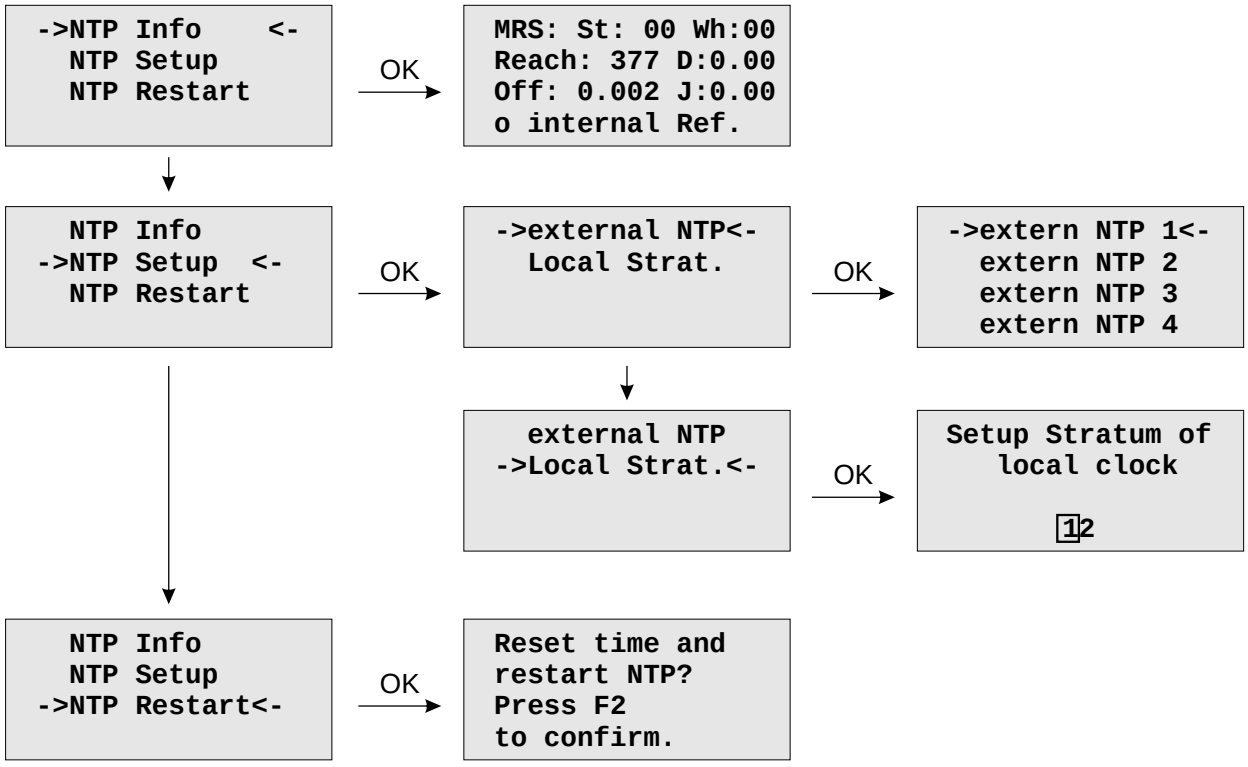
The last line of the display lets the user enter the phase of the generated frequency from -360° to +360° with a resolution of 0.1°. Increasing the phase lets the signal come out later. Phase affects frequencies less than 10.00 kHz only, if a higher frequency is selected a message "(phase ignored)" informs the user that the phase value is ignored.

10.2.4 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.



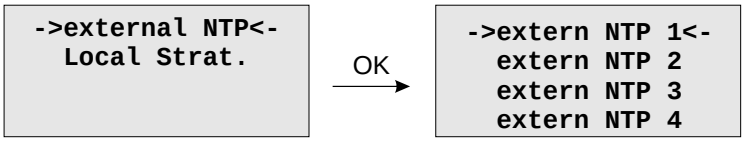
10.2.4.1 Menu NTP



10.2.4.2 Menu: external NTP

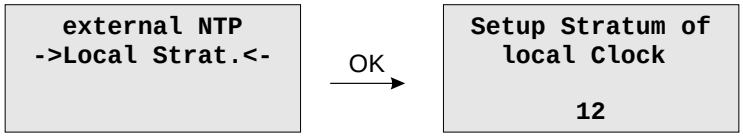
Additional external NTP servers can be set up to provide a high grade of redundancy for the internal reference clock.

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.



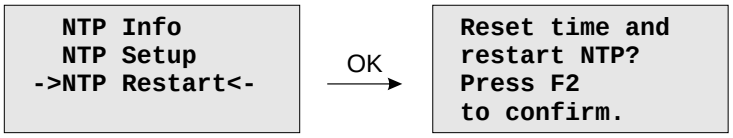
10.2.4.3 Menu: Stratum of local clock

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.

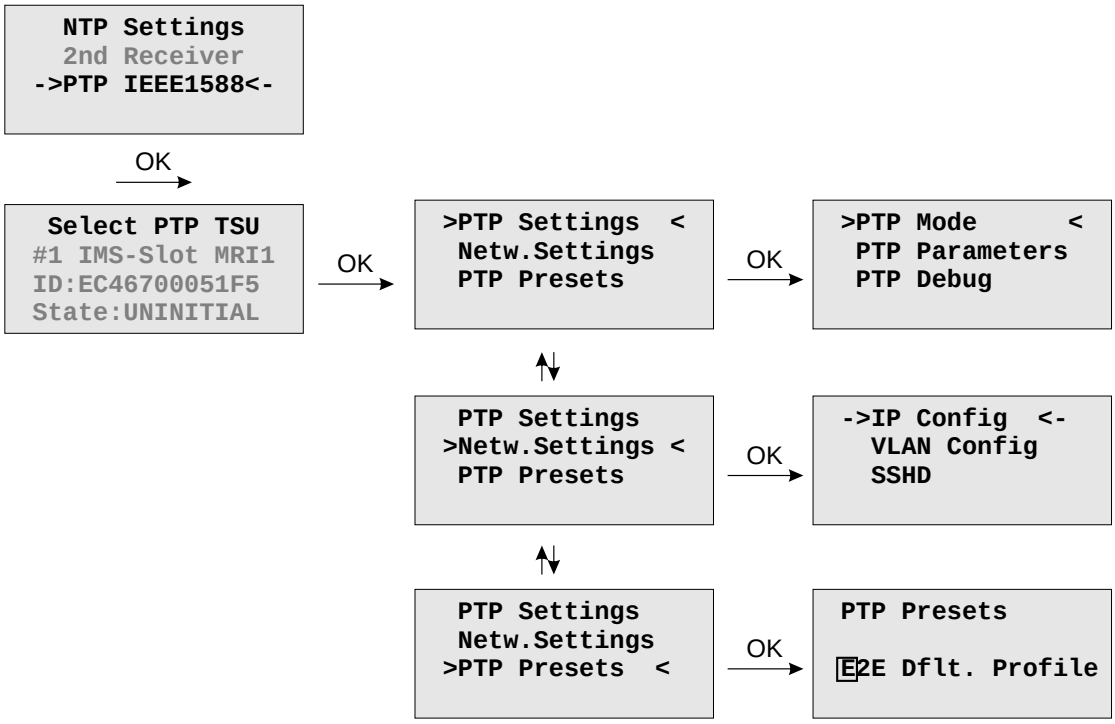


10.2.4.4 Menu: Restart NTP

The system time is setup, together with the reference time and the NTP service is rebooting.

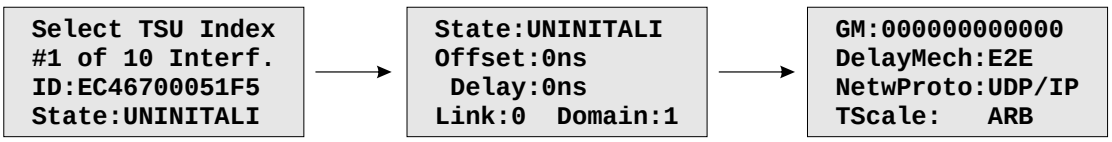


10.2.4.5 Option: Menu PTPv2 - IEEE 1588-2008



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.

10.2.4.6 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).

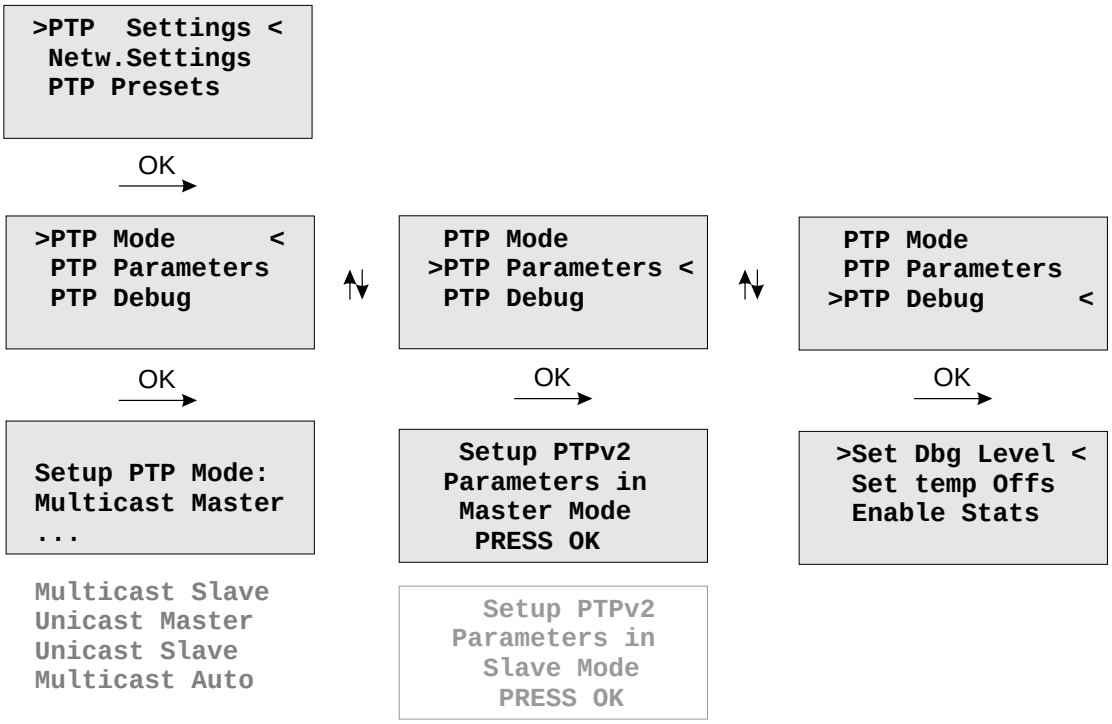
P2P (Peer-to-peer): where each device (a peer) in the network exchanges peer-delay measurement messages. This way each device can keep track of the delays between itself and its immediately connected neighbors. P2P mechanism can be used in 1588 PTP-capable networks only.

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.

10.2.4.7 Menu TSU Setup

With this menu, all PTP parameters can be configured for the selected interface:

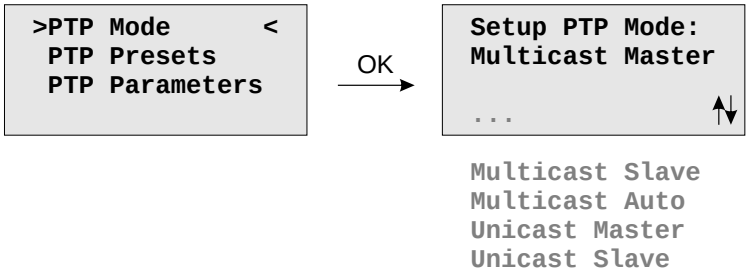


The **Set Dbg Level** menu is for maintenance and debugging purposes only, therefore leave it unchanged unless advised by a technician. The Level of debugging can be increased from 0 (default) to 3 with additional data being logged at each increased debugging level.

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.

10.2.4.8 Menu PTP Mode



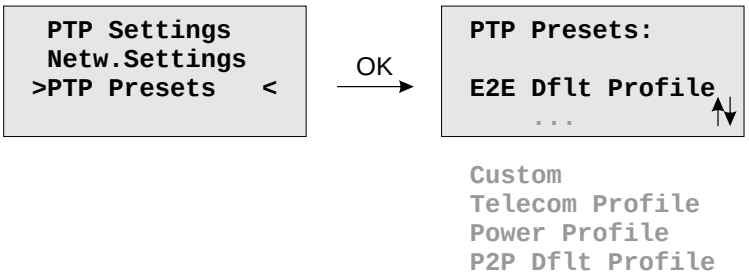
The number of different PTP operation modes depends on the feature set of the purchased unit.

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

10.2.4.9 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:

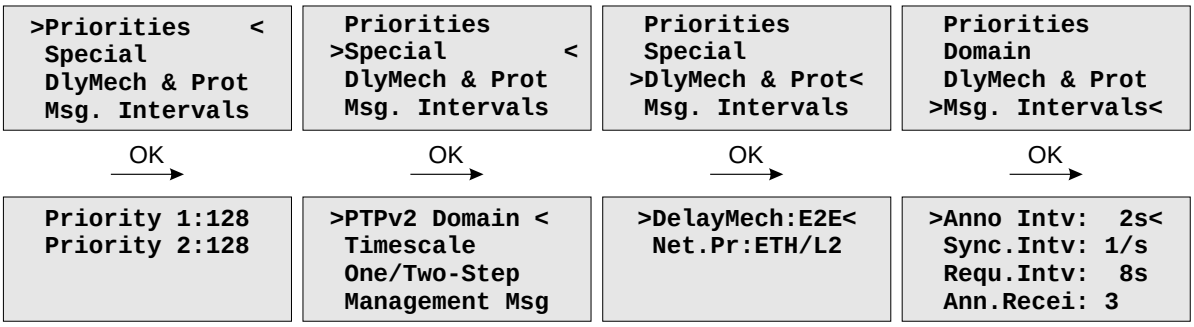
SMPTE ST 2059-2
-Ann Msg. Rate: 4/sec
-Sync Msg. Rate: 8/sec
-Del Req Rate: 8/sec
-Priority 1: 128
-Priority 2: 128
-Delay Mech: "E2E" or "P2P"

Custom Profile
By selecting "Custom" settings all parameters are ready for editing.

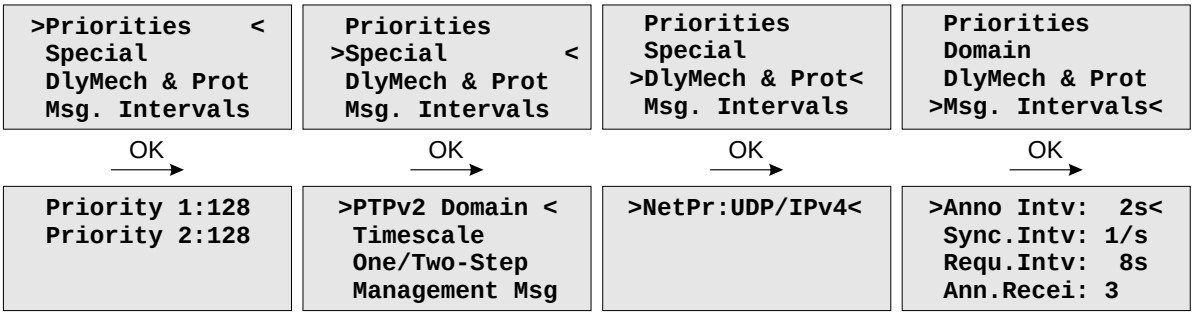
10.2.4.10 PTP Parameters

Depending on the selected mode, different sub menus will appear for configuring the PTP parameters.

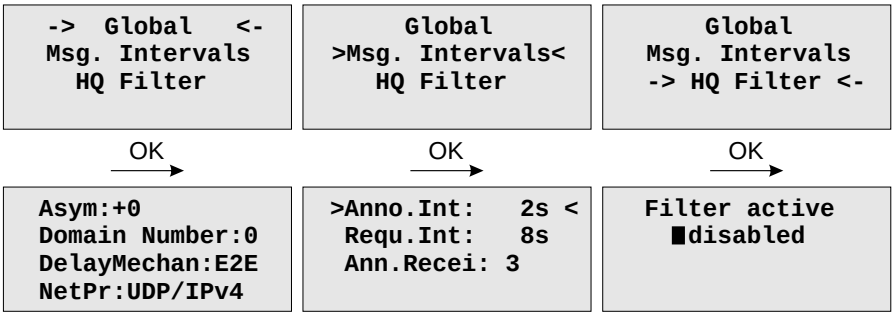
MULTICAST MASTER



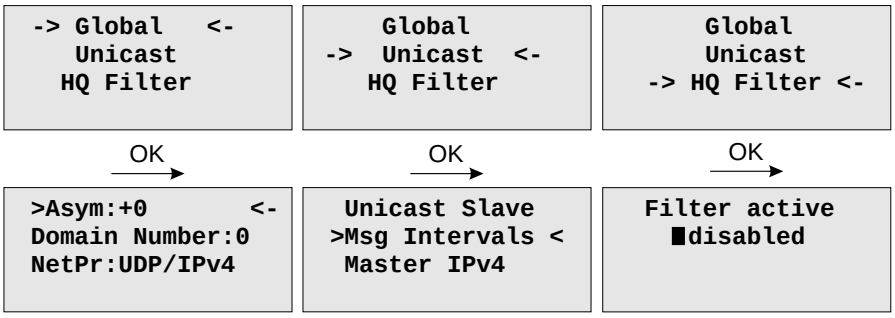
UNICAST MASTER



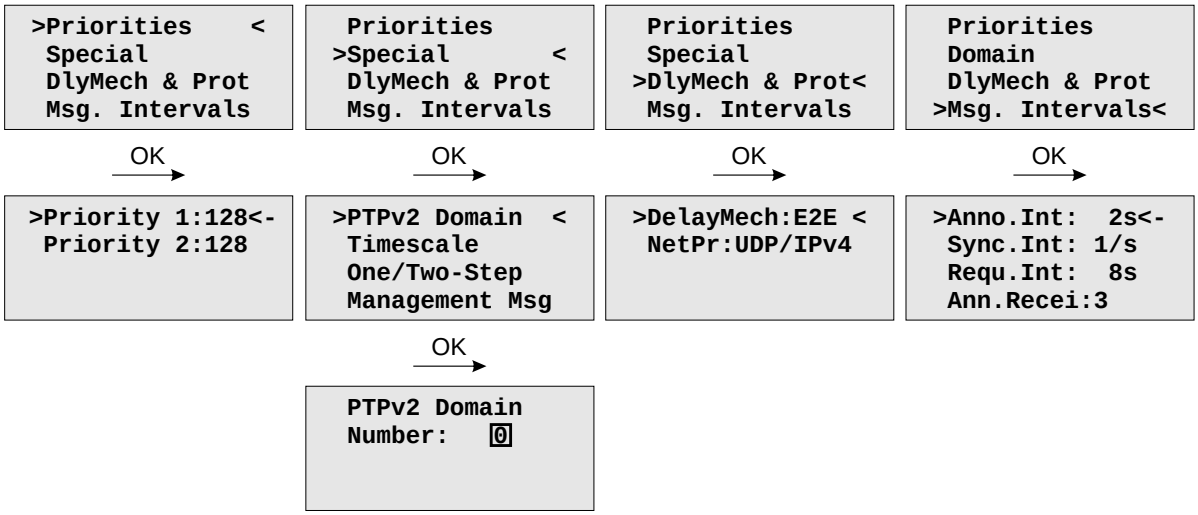
MULTICAST SLAVE



UNICAST SLAVE



10.2.4.11 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 newtorks 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.

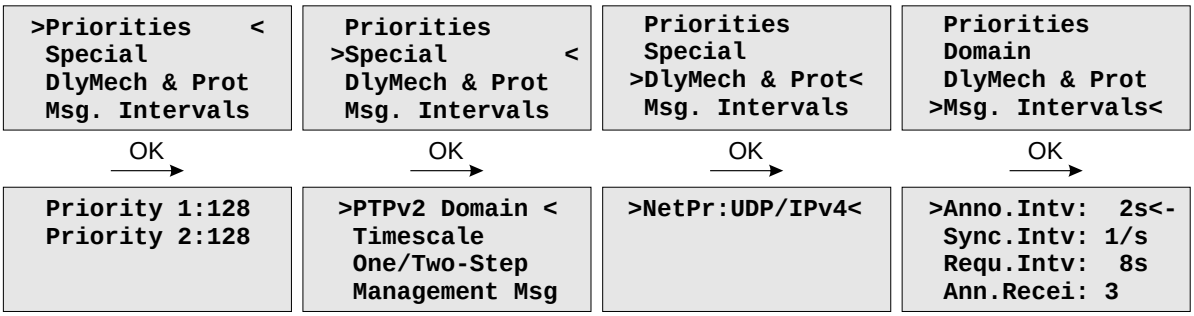
10.2.4.12 Unicast Master

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.

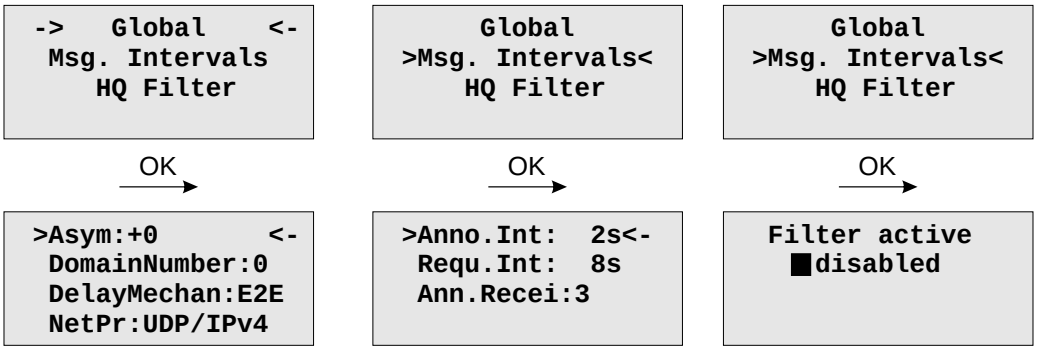
Msg. Intervals: specify the settings for the PTP timing messages.
Anno. Intv specifies the time for sending announce messages between masters to select the Grand Master. Available settings are: 16/s, 8/s, 4/s ... 2s, 4s, 8s, 16s with a default value 2 seconds.

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.

10.2.4.13 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.

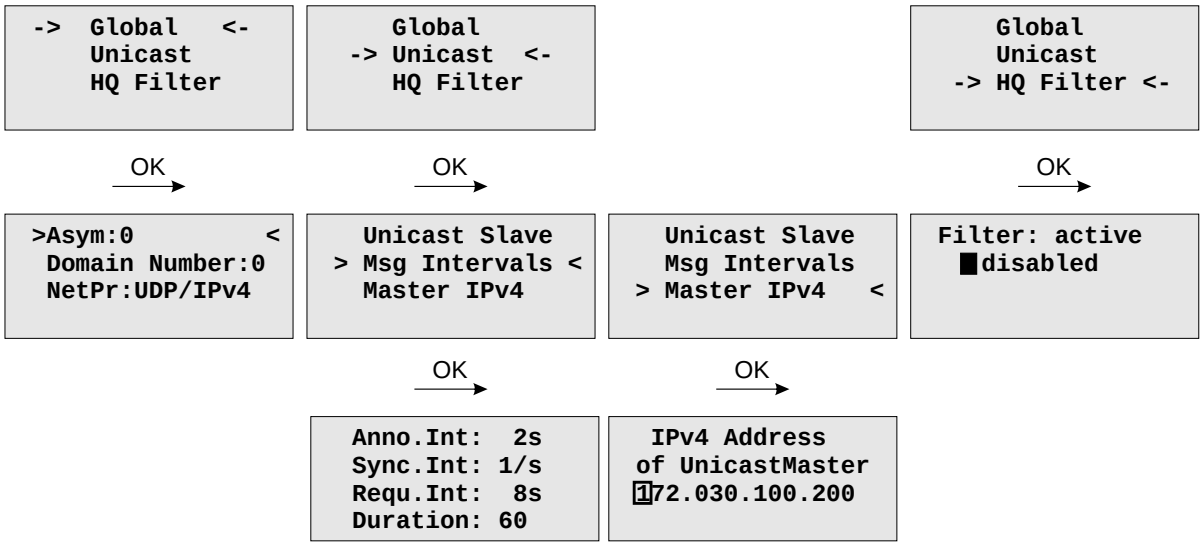
Sync. Intv specifies the time for sending sync messages from a master to a slave. Available settings are: 128/s, 64/s ... 64s, 128s, with a default value 1 second.

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.

10.2.4.14 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.

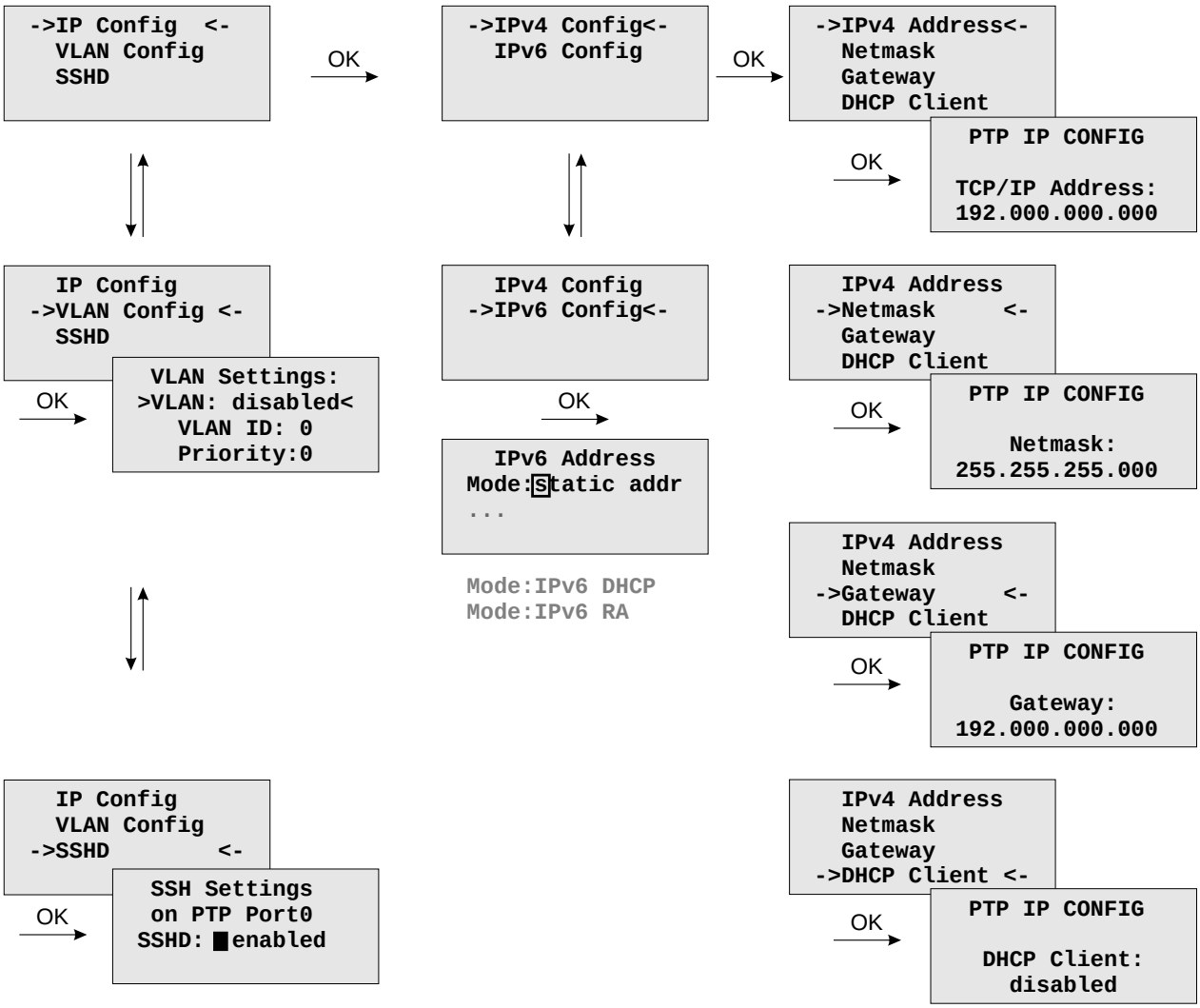
The **Duration** parameter is used to set a timeout for the grandmaster that sends out the sync packages until the timeout expires. A slave sends a new signaling message to refresh the request before the end of the Duration timeout. Thus it is receiving the requested sync packages continuously. The duration 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 in chapter PTP Option. The Default setting is with HQ Filter disabled.

10.2.4.15 Menu PTP Network Settings

Configuration for the PTP network port



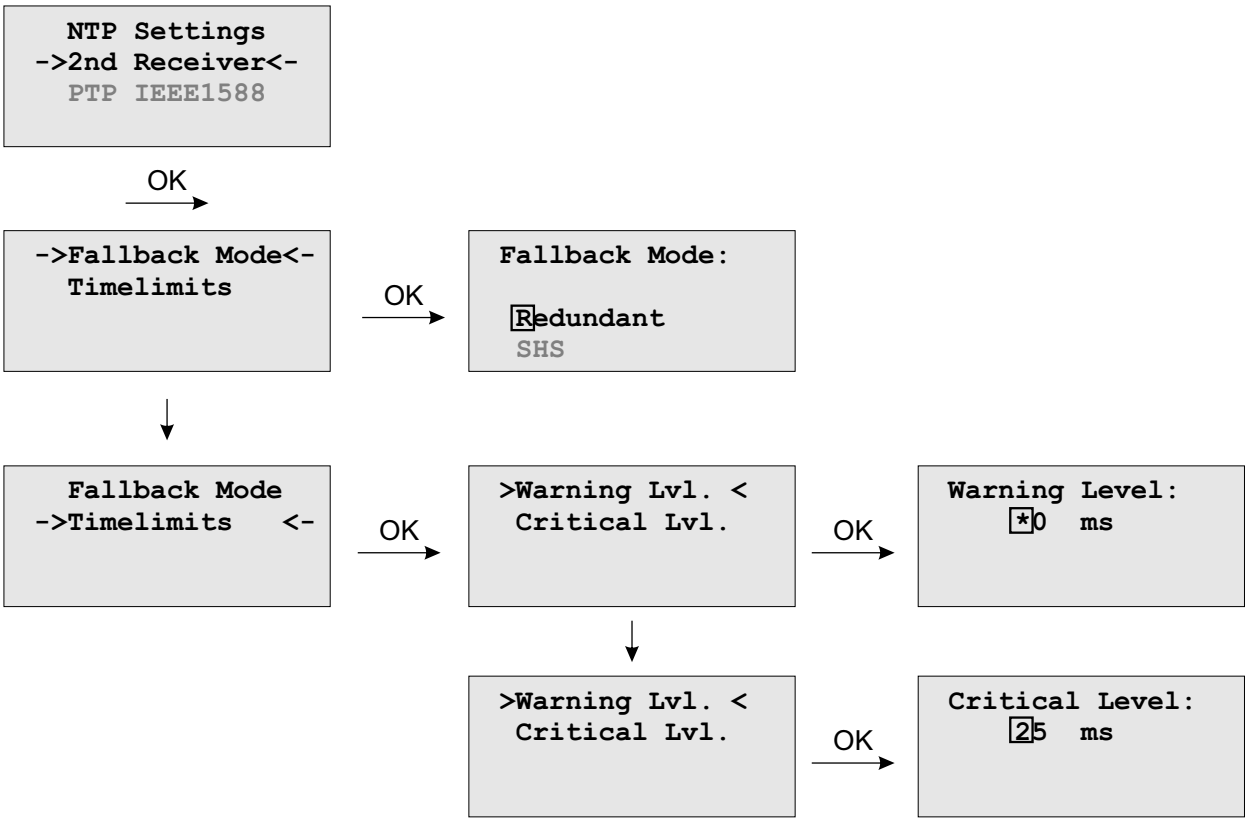
IP configuration for the PTPx interface. It can be selected if either a static IP address shall be used or if a dynamic IP address via DHCP should be assigned.

VLAN Config:
Configuration of Virtual LAN (IEEE 802.1Q) settings for the PTPx interface:

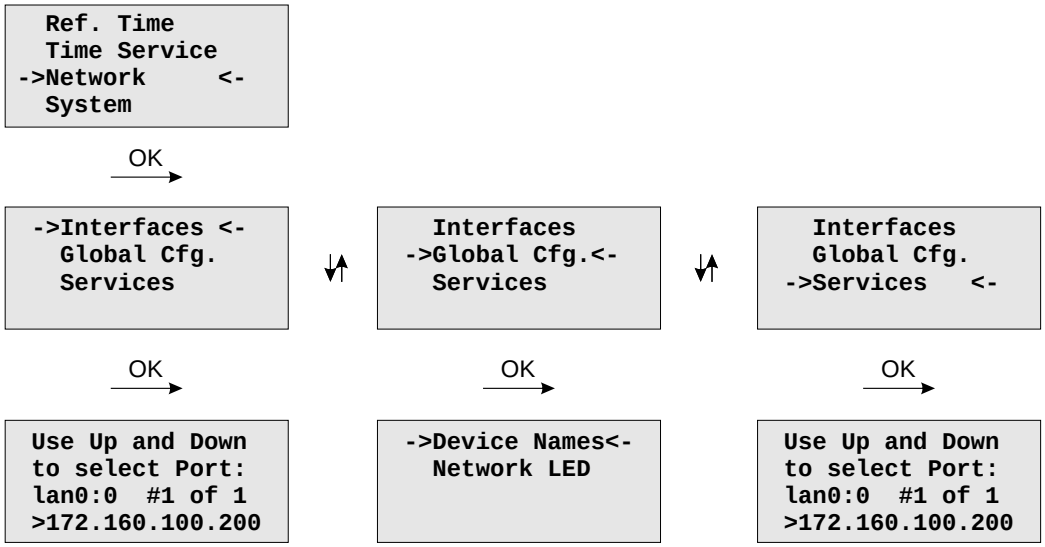
- VLAN ID: A 12-bit value (0..4096) specifying the VLAN to which the network port belongs.
- VLAN Priority: The priority indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data,...)

10.2.4.16 Optional Menu: 2nd Receivere

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.



10.2.5 Menu: Network

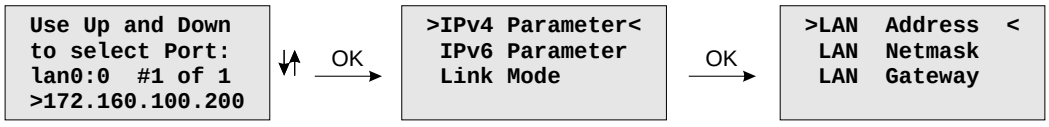


In this submenu the network configuration parameters related to the network interfaces can be changed. The submenus can be selected with the arrow keys and the "OK" button:

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.

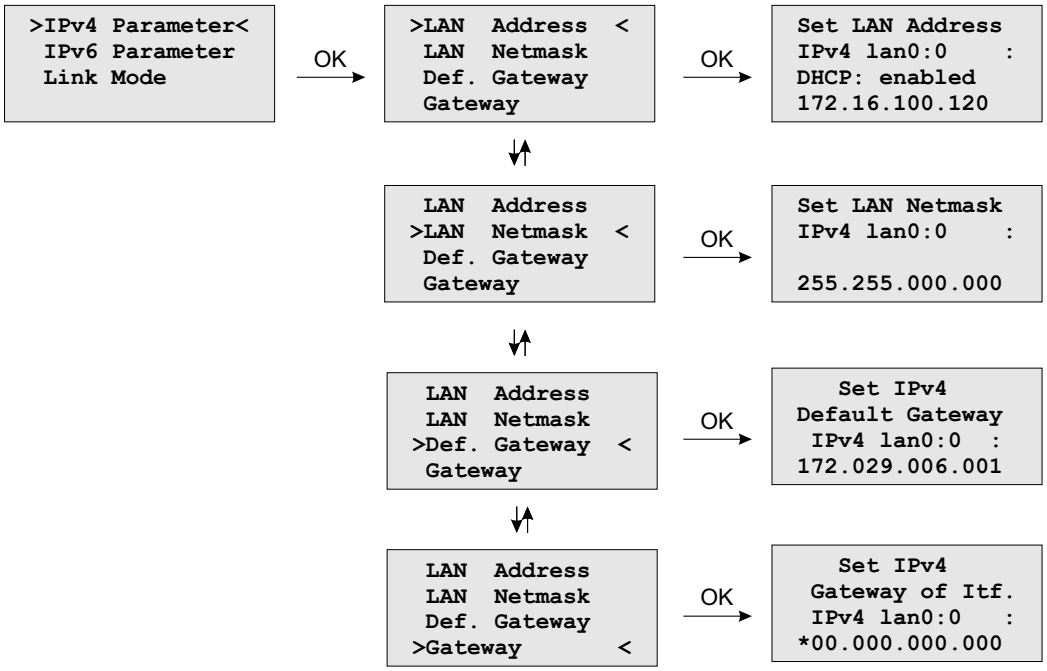
10.2.5.1 Menu: Setup Network Interfaces

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.

10.2.5.2 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

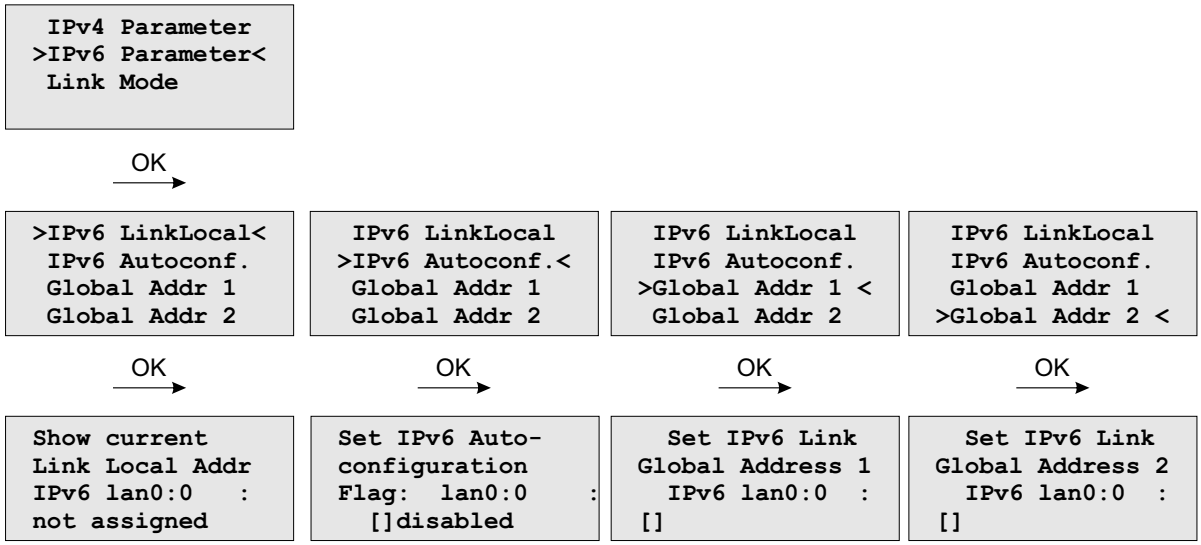
Additionally you can specify the IPv4 netmask and your default gateway address.

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).

10.2.5.3 Menu: Setup IPv6 Parameter

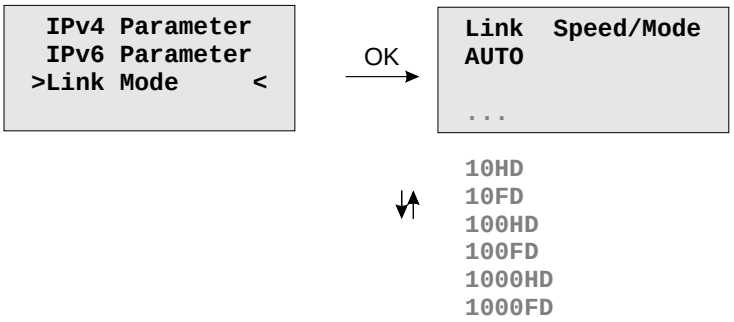


The IPV6 parameter can be configured via the front panel display for the first ethernet port (ETH0) only. Additionally IPV6 configuration can be done via network connection with TELNET, SSH or the WEB interface.

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.

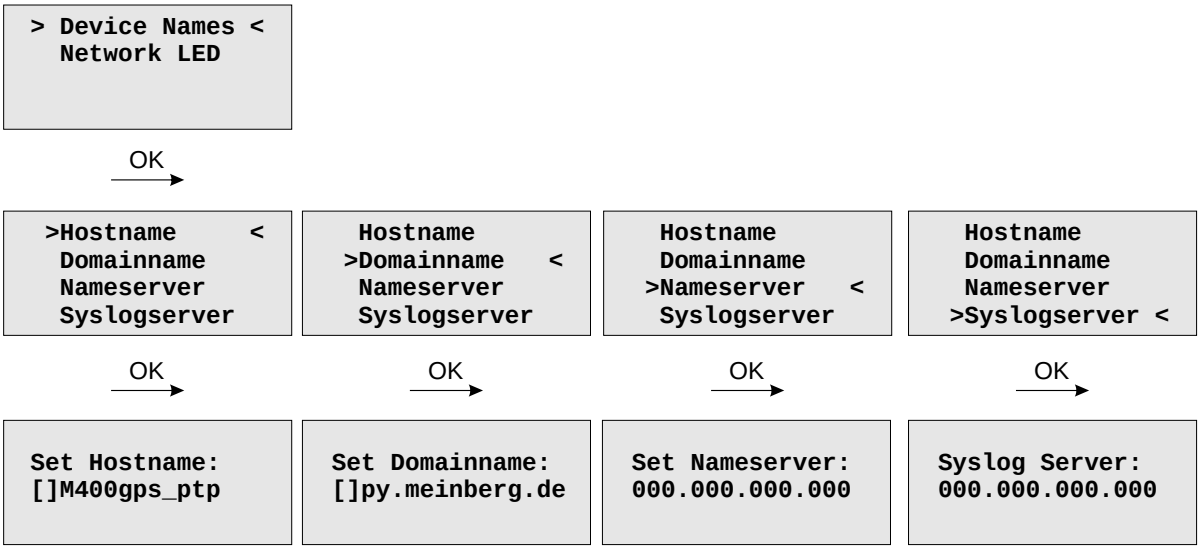
10.2.5.4 Menu: Link Mode



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.

10.2.5.5 Menu: Global Configuration



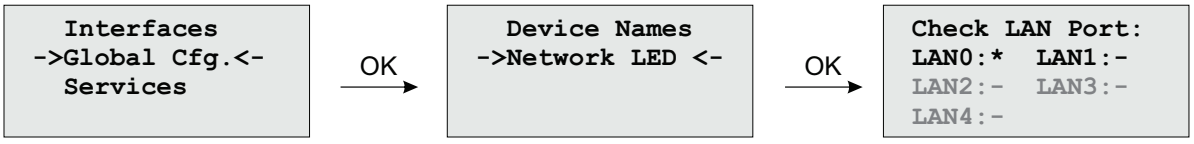
In this sub menu you can change the global network settings like host and domain name, nameserver and syslog server. Further name- or syslog servers can be set up via HTTP interface or CLI Setup. In the nameserver and syslog server fields you have to enter an Ipv4 address.

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.

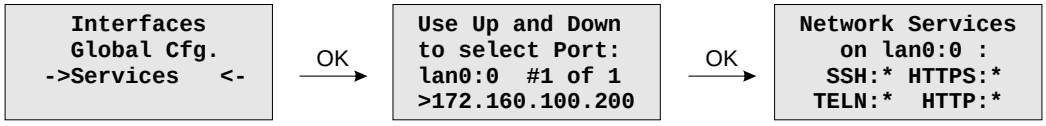
Please be aware of the fact that all SYSLOG entries of the timeserver are stored in „/var/log/messages“ and will be deleted when you power off or reboot the timeserver. A daily CRON job is checking for the size of the LANTIME SYSLOG and deletes it automatically if the log size is exceeding a certain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



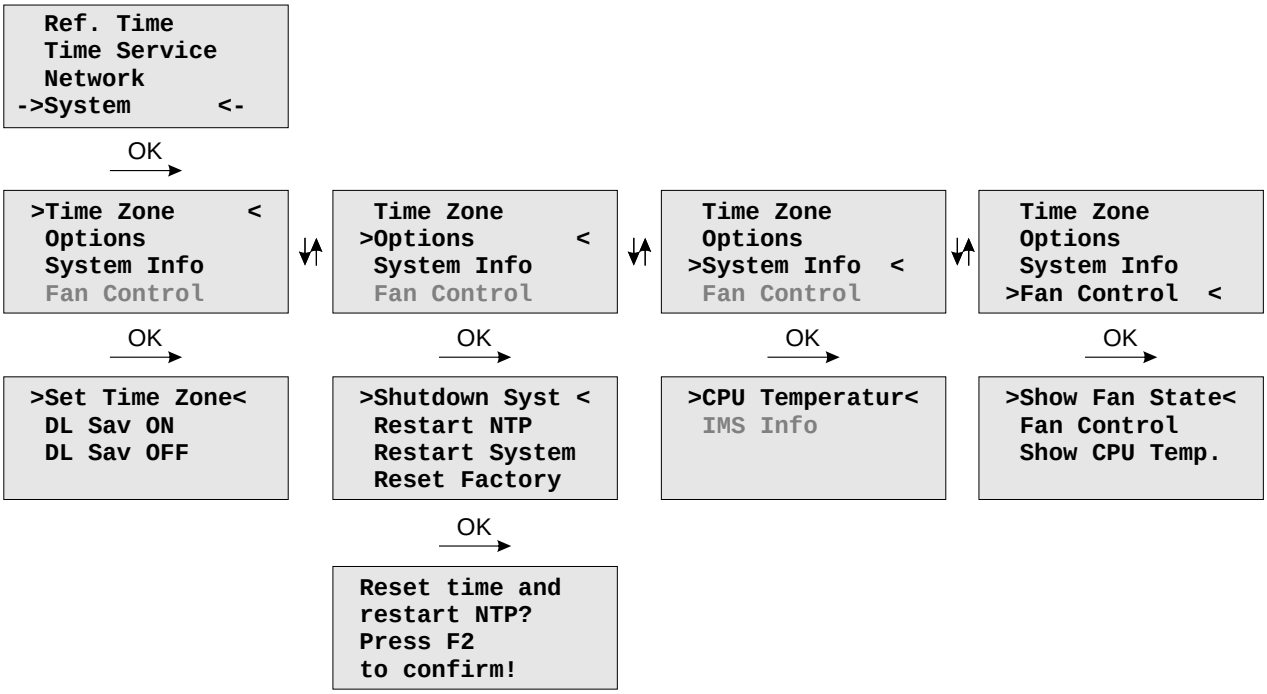
The submenu „Netw. LED“ will monitor the network ports, which will be checked continuously if the network port is „LINKED UP“. If one of these ports has no link up, the network LED on the front panel will change to red. An „L“ for „LED“ indicates if the port is checked. Please navigate through the list of ports with the LEFT/RIGHT buttons and change the setting with the UP/DOWN buttons.

10.2.5.6 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).

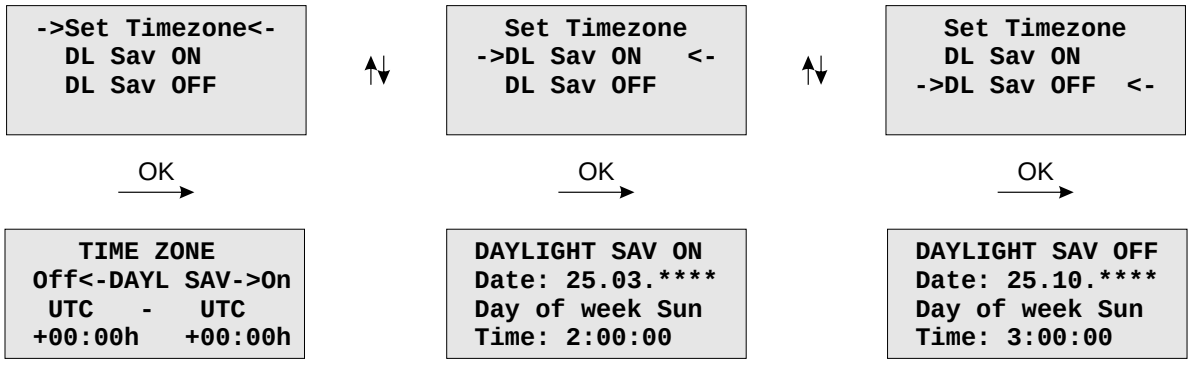
10.2.6 Menu: System



In this submenu system specific parameters can be configured.

10.2.6.1 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.

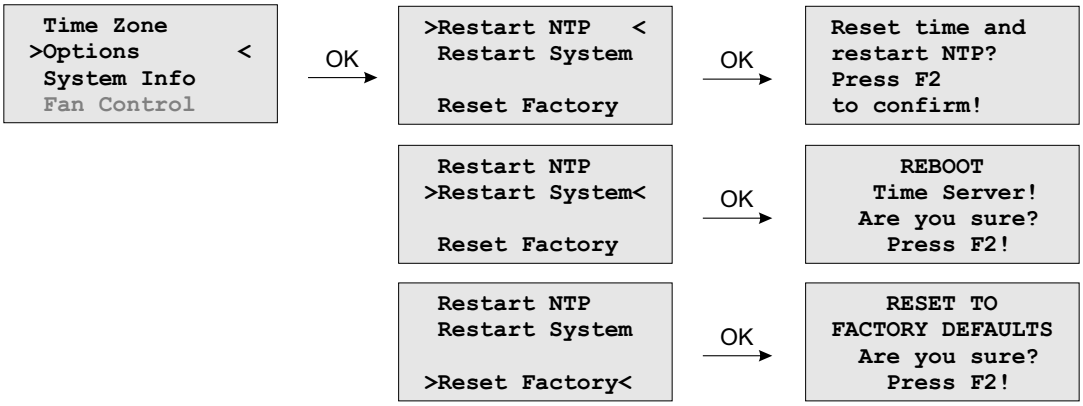
Beginning and ending of daylight saving may either be defined by exact dates for a single year or using an algorithm which allows the receiver to re-compute the effective dates year by year. The figures below show how to enter parameters in both cases. If the number of the year is displayed as wildcards ('*'), 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).

10.2.6.2 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:

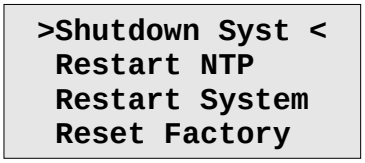
Auto: (temperature independent - the threshold value can be adjusted via the webinterface - menu "System -> Fan Control".

FAN ON: The cooling is permanently active.

FAN OFF: The cooling is permanently off.

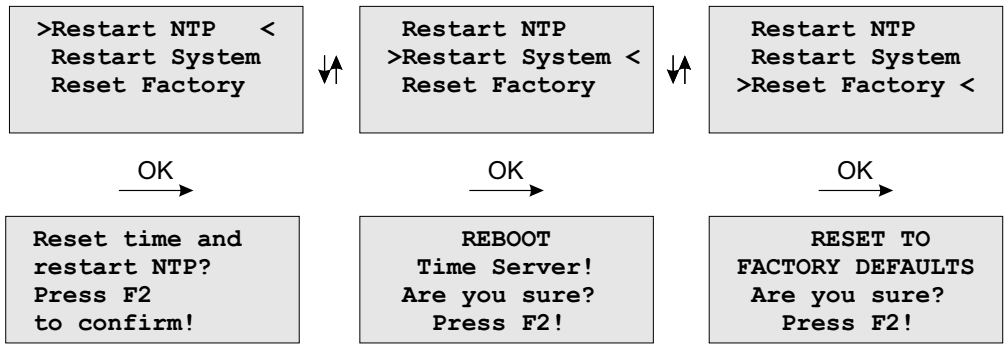
10.2.6.3 Shutdown System

Before the system is switched off by a mains switch, make sure that processes are not interrupted that have to be completed before the device is switched off. For example, if the SyncMonitor is stopped abruptly when saving data to the internal flash, this data will be lost.



The "Shutdown" stops the LANTIME deamon and the SyncMonitor and prepares the system for shutdown.

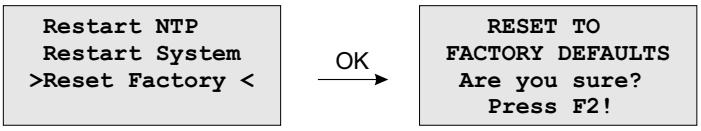
10.2.6.4 Menu: Restart System



If the time of the reference clock has changed (e.g. while testing with different times) the system time has to bet set with the time of the reference clock and the NTP has to be restarted.

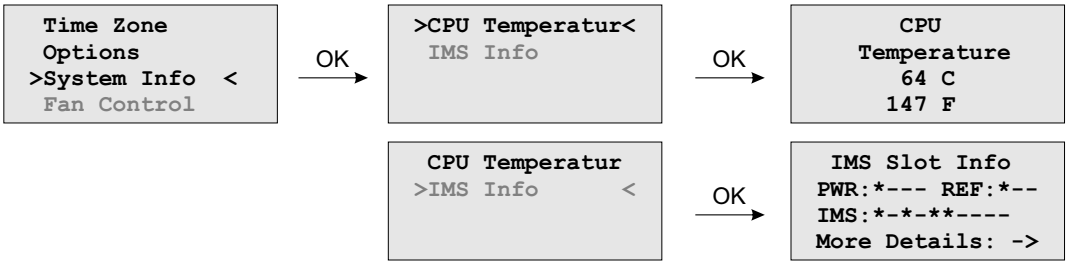
The command **Reboot System** reboots the Linux operating system – the built-in reference clock will not be restarted.

10.2.6.5 Menu Factory Reset



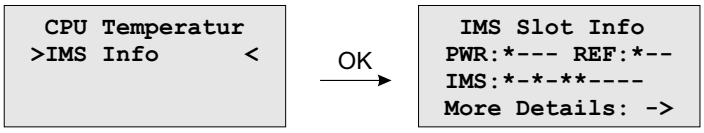
When **Reset to factory defaults** is called and confirmed, all network parameters and system parameters are reset to factory settings.

10.2.6.6 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.

10.2.6.7 Option: Menu IMS Slot Info

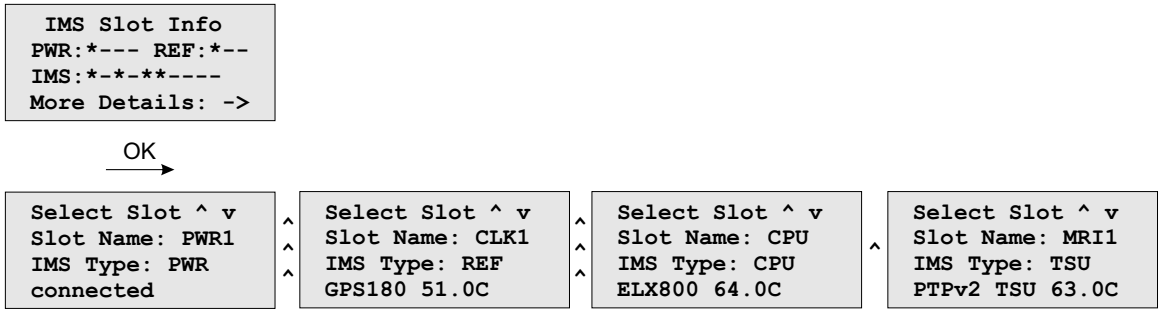


Note: This display menu is visible only in case of an IMS system. Here a detailed overview of the modules, used in the selected slots, are given.

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"

10.2.6.8 Option: IMS Menu Select Slots

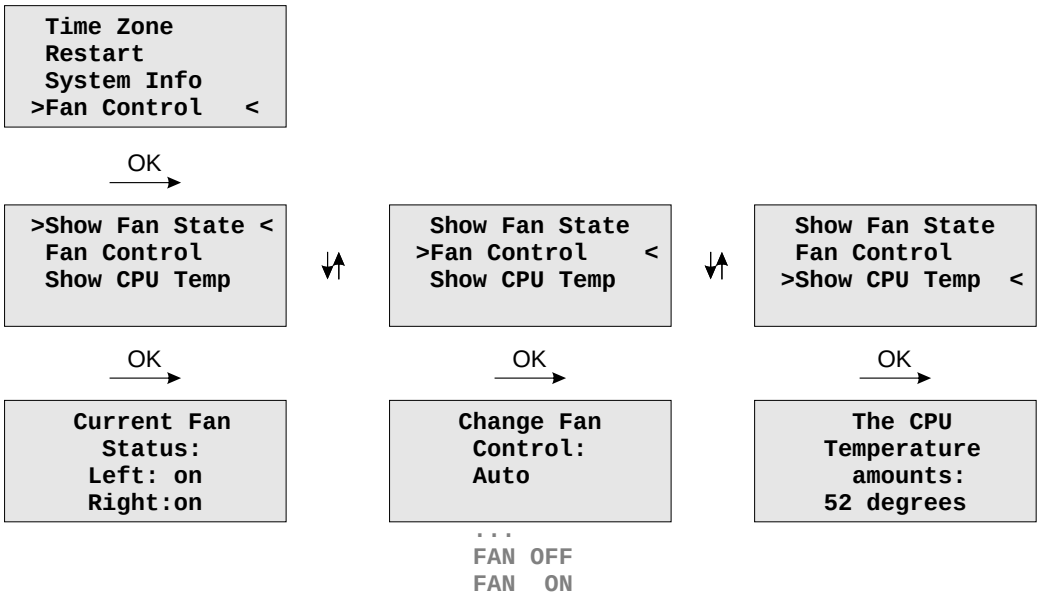


This menu shows which module is inserted into the selected slot.

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.

10.2.6.9 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.

10.2.7 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)
```

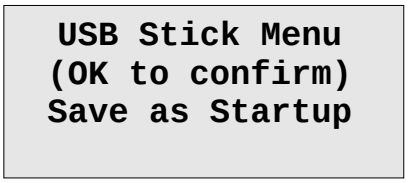
The desired menu function can be chosen by using ↑ and ↓ keys and it will be activated with the "OK" button. You can leave this menu with removing the USB storage or with the "ESC" button.

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.



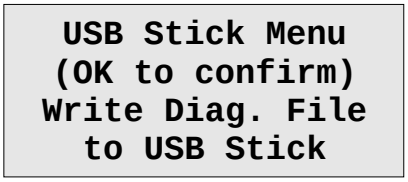
Please Note:
Even if you are currently making changes to a LANTIME, you can only save the configuration on the USB stick which you have confirmed via the web interface as "Startup configuration". This has the advantage that you can save your "old" configuration even if you make extensive changes to the 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.

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"



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:

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.

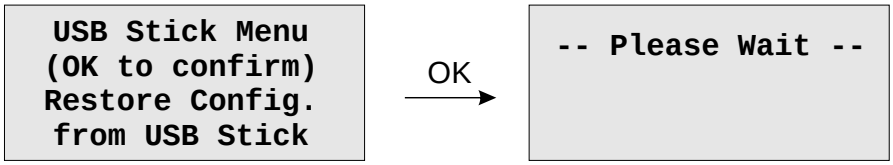
Note:
Make sure, that you never loose the "Keypad_Lock" file or the USB storage device! If you have problems, please contact Meinberg Radio clocks: Mail to techsupport@meinberg.de .

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.



10.3 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):

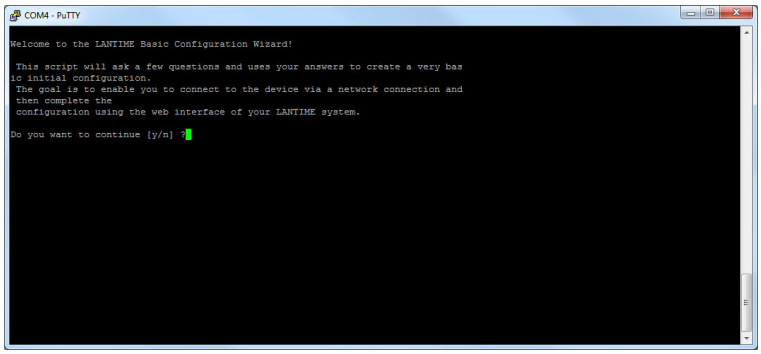
After the connection is successfully established use your login credentials in the welcome screen to enter a console.

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

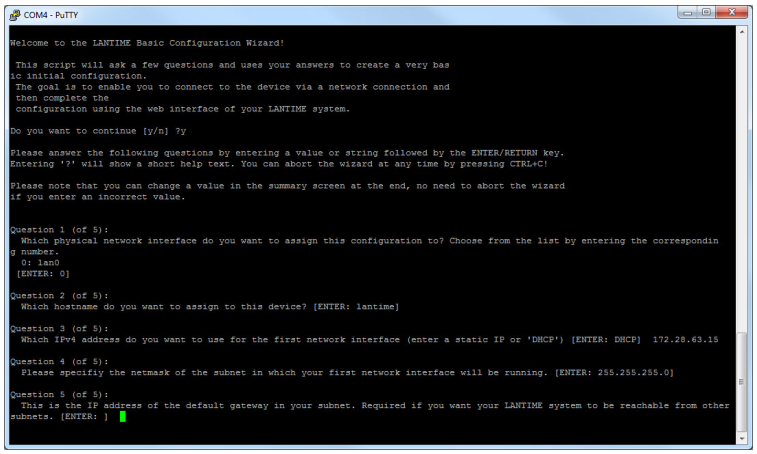
Default settings are:
Login: **root**
Password: **timeserver**
(It may be the case to press a RETURN button again).

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.

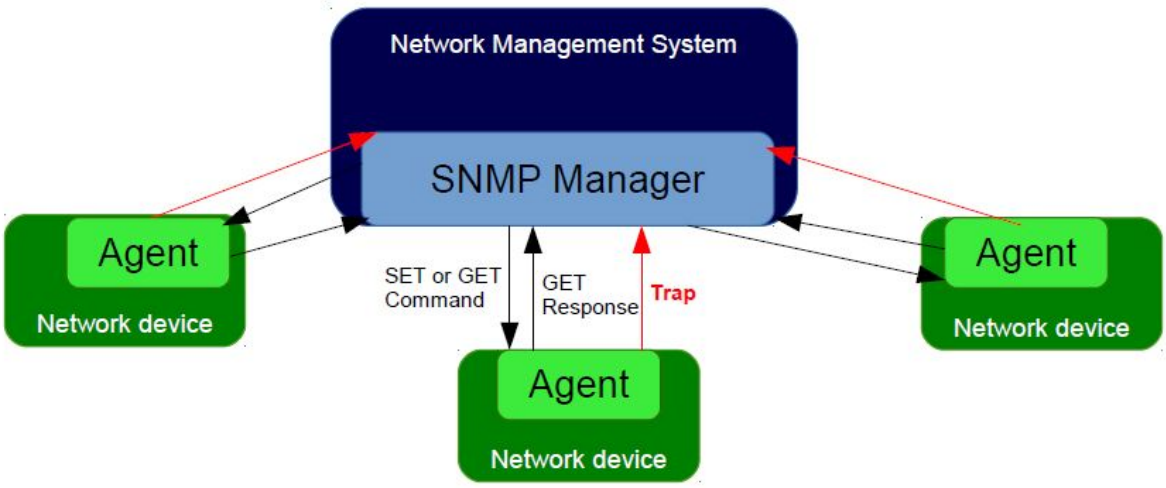
After the lantime has been assigned to a correct IP address, all other settings can be done via the extensive and powerful web interface (see chapter Via Web GUI).

10.4 Via SNMP

10.4.1 The Simple Network Managment 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.

10.4.2 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.

10.4.2.1 Refclock subtree

Here is a short list of OIDs from the NGStatus subtree with corresponding descriptions:

mbgLtNgRefclockState
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:	*refclock is not available:* See the possible troubleshooting: 1. Refclock module cannot be accessed. 2. Check if it is damaged and replace it if necessary.
1:	*synchronized:* 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. 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.
2:	*not synchronized:* Obviously the refclock is not synchronized to its time source. Here is the possible troubleshooting: 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. B) If GPS is the current time source, check number of satellites in view. There should be at least four to provide sync information. 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. D) Start "cold boot" to update a satellite almanac. E) If nothing from above helps, the GPS clock module needs to be changed.

```
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.

10.4.2.2 NTP subtree

Here is a short list of OIDs from the NGStatus subtree with corresponding descriptions:

mbgLtNgNtpCurrentState
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:	*not available:* See the possible troubleshooting: 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. B) Check if it is damaged and replace it if necessary.
1:	*not synchronized:* In case of "not synchronized" the NTP service is not yet synchronized to a reference clock. Possible causes for this state are as follows: 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. 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.
2.	*synchronized:* The NTP service is in normal operation. The LANTIME is now working properly.

```
It is recommended to check NTP status regularly,
but not more than every 64 s.
```

10.4.2.3 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:	*notAvailable:* The queried power supply unit is not recognized by a system. Check to see if it is damaged, and replace it if necessary.
1:	*down:* The power supply unit of interest is not in service. Check to see if it is damaged, and replace it if necessary.
2:	*up:* The queried power supply module is in operation.

```
It is recommended to check this OID every 60 s.
```

10.4.2.4 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:	*notAvailable:* The queried port is down, check the link LED. If faulty, replace the network card.
1:	*up:* The port of interest is in normal operation.

```
It is recommended to check this OID every 60 s.
```

10.4.2.5 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:

mbgLtNgPtpPortState
The following PTP Port States are possible:

Status	Description
0:	*uninitialized:* The port is booting up, the software daemon has not yet started, the IP address is not yet assigned.
1:	*initializing:* In this state the port initializes its data sets, hardware, and communication facilities.
2:	*faulty:* Not defined in a LANTIME.
3:	*disabled:* PTP service has been disabled on this port, either by user configuration or because the module is in a standby mode.
4:	*listening:* The port is waiting for the announceReceiptTimeout to expire or to receive an Announce message from a master.
5:	*preMaster:* A short transitional state while the port is becoming a master.
6:	*master:* The port is a current master.
7:	*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 due to a failure/service degradation of the current master.
8:	*uncalibrated:* One or more master ports have been detected in the domain.
9:	*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.

```
It is recommended to monitor the PtpPortState OID every 3 s
```

10.4.3 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 Rsponding
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:	-

SNMP Trap Name:	mbgLtNgTrapConfigChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.8
Severity:	Info
Short explanation:	trap to be sent when timeserver reloaded its configuration
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapLeapSecondAnnounced
OID:	.1.3.6.1.4.1.5597.30.3.0.9
Severity:	Info Warning
Short explanation:	trap to be sent when a leap second has been announced
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → Leap Second Announced LTOS 6 Managm./Mon. → NTP → Leap Second Handling
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitError
OID:	.1.3.6.1.4.1.5597.30.3.0.10
Severity:	Critical
Short explanation:	trap to be sent when SHS timelimit exceeded
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → SHS Time Limit Warning LTOS 6 Managm./Mon. → Web GUI → Introduction LTOS 6 Managm./Mon. → Web GUI → Security → SHS Mode LTOS 6 Managm./Mon. → Web GUI → Security → SHS Time Limit
Cleared By:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.11
Severity:	Warning
Short explanation:	trap to be sent when secondary receiver is not synchronised
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → CLK Not Sync
Cleared By:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapPowerSupplyFailure
OID:	.1.3.6.1.4.1.5597.30.3.0.12
Severity:	Critical
Short explanation:	trap to be sent when one of the redundant power supplies fails
Reference to other chapters:	Important Safety Information → Security during Installation Important Safety Information → Safety during Operation
Cleared By:	mbgLtNgTrapPowerSupplyUp

SNMP Trap Name:	mbgLtNgTrapAntennaShortCircuit
OID:	.1.3.6.1.4.1.5597.30.3.0.13
Severity:	Critical
Short explanation:	trap to be sent when a connected antenna fails due to a short circuit
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → Antenna Short Circuit
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapReceiverSync
OID:	.1.3.6.1.4.1.5597.30.3.0.14
Severity:	Clearing event
Short explanation:	trap to be sent when receiver is synchronised
Reference to other chapters:	Antenna and Receiver Information → Reference Time Sources
Cleared By:	-

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

SNMP Trap Name:	mbgLtNgTrapMrsRefReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.32
Severity:	Clearing event
Short explanation:	trap to be sent when a reference signal recovered
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapFdmError
OID:	.1.3.6.1.4.1.5597.30.3.0.33
Severity:	Critical
Short explanation:	trap to be sent when the Fdm module generates an alarm
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → FDM → FDM Configuration
Cleared By:	mbgLtNgTrapFDMOk

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitWarning
OID:	.1.3.6.1.4.1.5597.30.3.0.34
Severity:	Warning Critical
Short explanation:	trap to be sent when SHS warning limit exceeded
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Introduction LTOS 6 Managm./Mon. → Web GUI → Security → SHS Configuration LTOS 6 Managm./Mon. → Web GUI → Security → SHS Mode Troubleshooting and Alarming → Ref. Clock → SHS Time Limit Warning
Cleared By:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecSync
OID:	.1.3.6.1.4.1.5597.30.3.0.35
Severity:	Clearing event
Short explanation:	trap to be sent when secondary receiver is synchronised
Reference to other chapters:	Antenna and Receiver Information → Reference Time Sources
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPSync
OID:	.1.3.6.1.4.1.5597.30.3.0.36
Severity:	Clearing event
Short explanation:	trap to be sent when NTP is synchronised
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPtpPortDisconnected
OID:	.1.3.6.1.4.1.5597.30.3.0.37
Severity:	Warning or critical
Short explanation:	trap to be sent when PTP network port got disconnected
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → PTP → PTP Global Status
Cleared By:	mbgLtNgTrapPtpPortConnected

SNMP Trap Name:	mbgLtNgTrapPtpPortConnected
OID:	.1.3.6.1.4.1.5597.30.3.0.38
Severity:	Clearing event
Short explanation:	trap to be sent when PTP network port got connected
Reference to other chapters:	no further Information
Cleared By:	-

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:	-

SNMP Trap Name:	mbgLtNgTrapSufficientSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.48
Severity:	Clearing event
Short explanation:	trap to be sent when system has regained sufficient resources
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.49
Severity:	Clearing event
Short explanation:	trap to be sent when oscillator is warmed up
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorNotWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.50
Severity:	Info
Short explanation:	trap to be sent when oscillator is not warmed up
Reference to other chapters:	Troubleshooting and Alarming → Ref. Clock → Oscillator not Adjusted
Cleared By:	mbgLtNgTrapOscillatorWarmedUp

SNMP Trap Name:	mbgLtNgTrapMrsRefChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.51
Severity:	Info Warning
Short explanation:	trap to be sent when MRS reference source changed
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapClusterMasterChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.52
Severity:	Warning
Short explanation:	trap to be sent when cluster mode is active and cluster changed
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Network → Network Interf. - Cluster
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerDetected
OID:	.1.3.6.1.4.1.5597.30.3.0.53
Severity:	Warning
Short explanation:	trap to be sent when cluster mode is active and a cluster member is dectected as falseticker
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Network → Network Interf. - Cluster
Cleared By:	mbgLtNgTrapClusterFalsetickerCleared

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerCleared
OID:	.1.3.6.1.4.1.5597.30.3.0.54
Severity:	Clearing event
Short explanation:	trap to be sent when cluster mode is active and a cluster member is no longer a falseticker
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.55
Severity:	Info
Short explanation:	trap to be sent when SHS timelimit error has been acknowledged or time difference drops below warning limit
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → Introduction
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapIMSError
OID:	.1.3.6.1.4.1.5597.30.3.0.56
Severity:	Critical
Short explanation:	trap to be sent when an IMS module is not responsive anymore has got temperature issues, etc.
Reference to other chapters:	Troubleshooting and Alarming → Miscellaneous → IMS Error
Cleared By:	mbgLtNgTrapIMSOk

SNMP Trap Name:	mbgLtNgTrapIMSOk
OID:	.1.3.6.1.4.1.5597.30.3.0.57
Severity:	Clearing event
Short explanation:	trap to be sent when an IMS module returns to healthy state
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapFDMOk
OID:	.1.3.6.1.4.1.5597.30.3.0.58
Severity:	Clearing event
Short explanation:	trap to be sent when an FDM module returns to healthy state
Reference to other chapters:	LTOS 6 Managm./Mon. → Web GUI → FDM → FDM Configuration
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.59
Severity:	Error
Short explanation:	trap to be sent when monitoring an NTP client and its offset limit is exceeded
Reference to other chapters:	Troubleshooting and Alarming → NTP → NTP Offset Limit Exceeded
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.60
Severity:	Info
Short explanation:	trap to be sent when monitoring an NTP client and its offset limit is back again in a valid range
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapNTPOffsetLimitExceeded

SNMP Trap Name:	mbgLtNgTrapXheRubError
OID:	.1.3.6.1.4.1.5597.30.3.0.61
Severity:	Info
Short explanation:	trap to be sent when external rubidium announces OK
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapXheRubError
OID:	.1.3.6.1.4.1.5597.30.3.0.62
Severity:	Error
Short explanation:	trap to be sent when external rubidium announces error
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.63
Severity:	Warning
Short explanation:	trap to be sent when device consumes too much power
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapPowerConsumptionOk

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionOk
OID:	.1.3.6.1.4.1.5597.30.3.0.64
Severity:	Info
Short explanation:	trap to be sent when device has got enough power
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyNotAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.65
Severity:	Warning
Short explanation:	trap to be sent when there currently is no power supply backup avail
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapPowerRedundancyAvail

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.66
Severity:	Info
Short explanation:	trap to be sent when there is at least one power supply as backup
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapTrustedSourceError
OID:	.1.3.6.1.4.1.5597.30.3.0.67
Severity:	Warning
Short explanation:	trap to be sent when a MRS source's time deviation exceeds a configured limit
Reference to other chapters:	no further information
Cleared By:	mbgLtNgTrapTrustedSourceOk

SNMP Trap Name:	mbgLtNgTrapTrustedSourceOk
OID:	.1.3.6.1.4.1.5597.30.3.0.68
Severity:	Clearing Event
Short explanation:	trap to be sent when a MRS source's time deviation returns to its configured bounds
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapNormalOperation
OID:	.1.3.6.1.4.1.5597.30.3.0.77
Severity:	Clearing event
Short explanation:	trap to be sent when the system returned to a healthy state
Reference to other chapters:	no further information
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapHeartbeat
OID:	.1.3.6.1.4.1.5597.30.3.0.88
Severity:	Info
Short explanation:	trap to be sent periodically to indicate that time server is still alive
Reference to other chapters:	LTOS 6 Managm./Mon. → Notifications → Miscellaneous - Enable Heartbeat
Cleared By:	-

SNMP Trap Name:	mbgLtNgTrapTestNotification
OID:	.1.3.6.1.4.1.5597.30.3.0.99
Severity:	Info
Short explanation:	trap to be sent when a test notification has been requested
Reference to other chapters:	no further information
Cleared By:	-

11 Troubleshooting and Alarming

11.1 NTP Messages

Error and System message / Explanation	Troubleshooting / Additional information
NTP Not Sync / The NTP service of a LANTIME is not sync.	• 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.

11.2 Ref. Clock Messages

Error and System message / Explanation	Troubleshooting / Additional information
CLK Not Responding / The LANTIME can no longer communicate with its internal reference clock.	• Contact your Meinberg TechSupport and provide a LANTIME diagnostic file.
CLK Not Sync / Performance and system ressources issue of the NTP	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 Tech-Support 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.

MRS 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.

MRS 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.

MRS Source: Invalid Signal
The LANTIME server will generate this message if an MRS input signal is present but does not satisfy certain requirements such as signal quality. Example: The PTP GM is receiving a PTP signal, but this signal is not of the minimum clock class required by the Slave.

- Contact your Meinberg TechSupport and provide a LANTIME diagnostic file, if you need further assistance at solving the problem.

11.3 Network Messages

Error and System message / Explanation	Troubleshooting / Additional information
Network Link Down / There was no link detected at one of the LANTIME's network interface.	• 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.

11.4 Miscellaneous Messages

Error and System message / Explanation	Troubleshooting / Additional information
Fan Failure / The LANTIME has detected a fault on a fan module, or a fan module has been removed during system operation.	• 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.

12 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
- Meinberg Customer Portal

12.1 Basic Customer Support

Contact Meinberg via e-mail or phone.

Technical Support	
E-Mail	techsupport@meinberg.de
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	info@meinberg.de
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).

12.2 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 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.

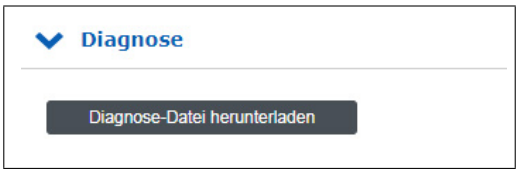
12.3 How to download a Diagnostic File

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 storage device connected to the time server. The file format of the diagnostic file is a tgz-archive. The archive contains all the important configuration and logfiles.

12.3.1 Download via Web GUI

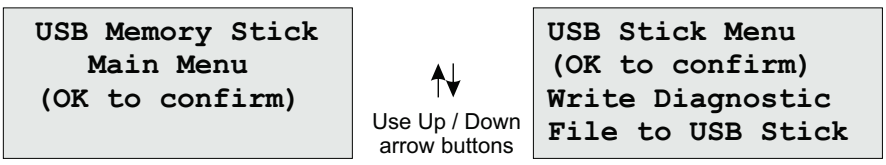
- Connect to the Web GUI by putting the IP address into the address field of the web browser.
- Open the „System“ page and the submenu "Diagnostics".
- Press the "Download Diagnostic File" button.



- 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/).

12.3.2 Download via USB Stick

- The USB storage device 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 storage device.
- You can find the Diagnostic File by opening the LANTIME folder and continue on to the Diag folder.



12.4 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=ZTJMKSI8OGY (YouTube video)

12. NTP support page and documentation:
    http://support.ntp.org/bin/view/Support/WebHome

12.5 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.

12.6 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

12.7 Meinberg Newsletter

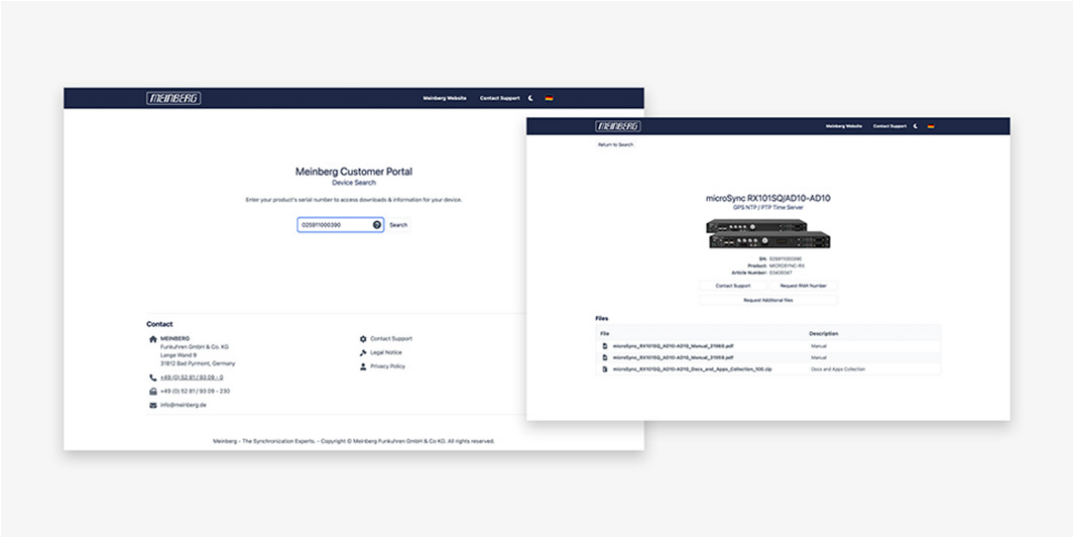
Meinberg publishes regularly up-to-date information, technical news, firmware updates and security advisory by the Meinberg Newsletter in both the English and German language.

Subscribe to the newsletter here:

https://www.meinbergglobal.com/english/contact/newslett.htm

12.8 Meinberg Customer Portal - Software and Documentation

End users of Meinberg products are provided with technical support, full documentation and software downloads through our Support Centre – all in one place: https://meinberg.support



No Registration required

There's no need to register; simply enter your product's serial number at https://www.meinberg.support and you'll have everything you need to get your Meinberg system up and running—or perhaps back up and running, as the case may be—with up-to-date installation and reference manuals, downloads for drivers, remote monitoring, configuration tools, and SNMP MIB files, direct links to contact Meinberg's Technical Support team, and the ability to easily request additional files.

The Meinberg Customer Portal vastly simplifies how you access support, software, and documentation, and ensures that you always have the latest versions of downloadable tools and manuals at your disposal.

13 Appendix

13.1 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.

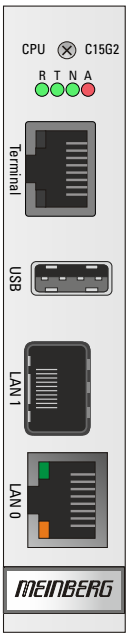
13.1.1 Technical Specifications LAN CPU

CPU Module Type C05F1:

Processor:	AMD Geode™ LX 800 (500 MHz, 128 KB L2 cache, 3.6 W)
Main Memory:	onboard 256 MByte
Flashdisk:	1 GB
Network Connector:	10/100 MBIT with RJ45-Jack
Power Requirements:	5 V +- 5 %, @ 1 A
Frontpanel:	3U / 4TE (128 mm high x 20,3 mm wide)
Ambient Temperature:	0 ... 50 °C
Storage Temperature:	-20 ... 70 °C
Humidity:	85 % max.

13.1.2 Technical Specifications - IMS CPU-C15G2

As the central management and control element, the CPU module in an LANTIME system is responsible for management, configuration and alarm notifications. It additionally provides NTP and SNTP services on its network interface. The CPU-C15G2 is equipped with two integrated network interfaces, additional network ports can be added by installing LNE modules.



Processor: Intel® Atom™ Processor E Series
(2 Cores, 1.33GHz, TDP 3W)

Main Memory: onboard 2 GB

Cache Memory: 1MB 2nd Level Cache

Flash Disk: 4 GB

Network Connector:
1 x 10/100/1000 Base-T with RJ45-Jack
1 x 1000Base-T with SFP-Jack

Serial Interface: RJ45 connector
console: 38400 / 8N1,
connection via CAB-CONSOLE cable

USB Port: install firmware upgrades
backup and restore configuration files
copy security keys
lock / unlock front keys

Operating System: GNU/Linux 4.x

State LEDs:

LAN 0 Interface
LED - Connect, Activity and Speed of the network connection

LAN-CPU
R - Reference Time
T - Time Service
N - Network
A - Alarm

Supported Protocols:

Network Time Protocol (NTP):	NTP v2 (RFC 1119), NTP v3 (RFC 1305), NTP v4 (RFC 5905) SNTP v3 (RFC 1769), SNTP v4 (RFC 4330)
OSI Layer 2 (Data Link Layer):	PRP (IEC 62439-3)
OSI Layer 3 (Network Layer):	IPv4, IPv6
OSI Layer 4 (Transport Layer):	TCP, UDP, TIME (RFC 868), DAYTIME (RFC 867), SYSLOG
OSI Layer 7 (Application Layer):	HTTP / HTTPS (RC 2616), DHCP, FTP, NTPv3 / NTPv4, SNTP, RADIUS, TACACS, FTP, SSH (incl. SFTP, SCP) - SSH v1.3 / SSH v1.5 / SSH v2 (OpenSSH), SNMPv1 (RFC 1157) / SNMPv2c (RFC 1901-1908) / SNMP v3 (RFC 3411-3418), Telnet (RFC 854-RFC 861)

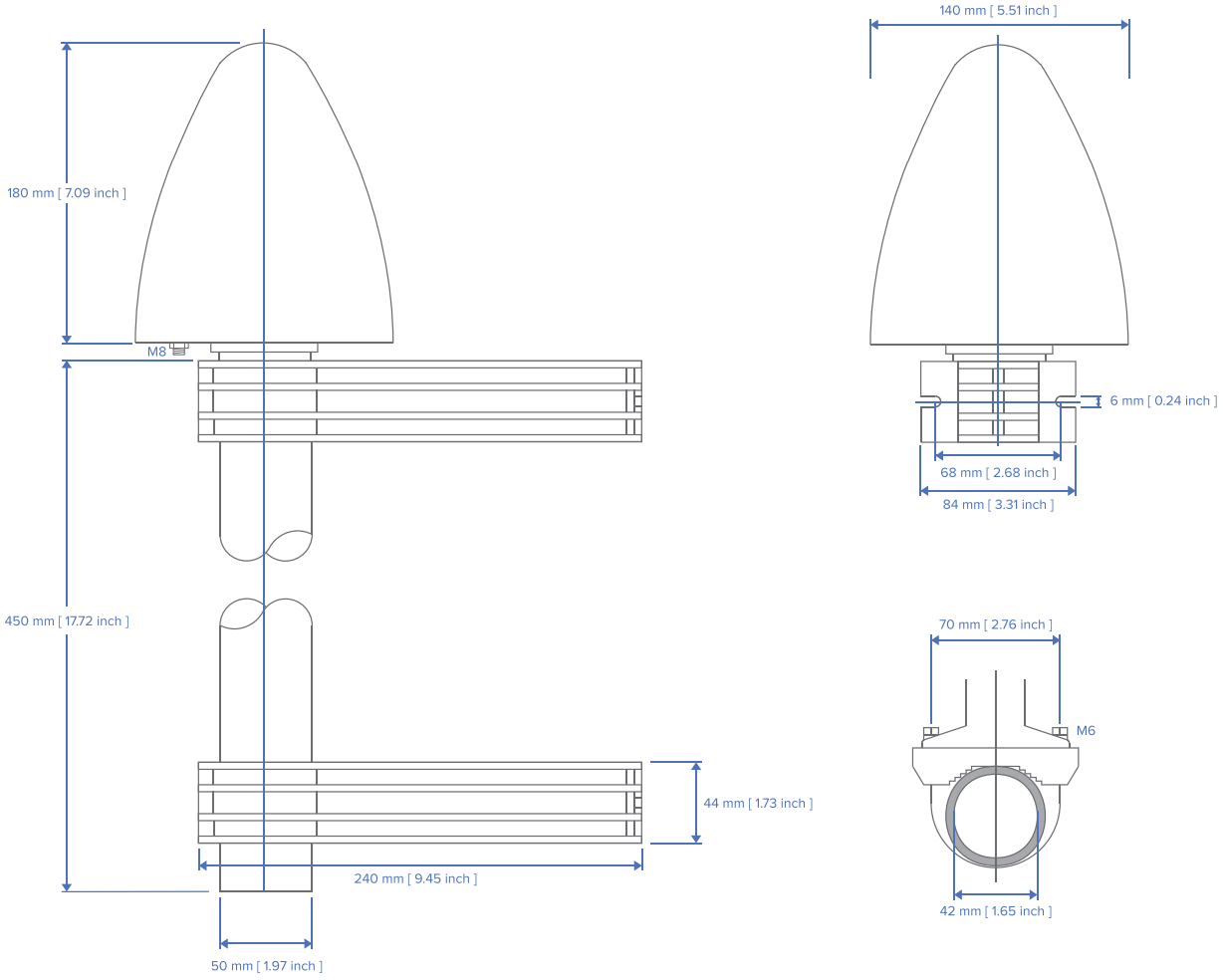
Environmental:

Ambient Temperature:	0 ... 50°C / 32 ... 122°F
Humidity:	Max. 85%

13.2 Technical Data - Antennas for LANTIME Systems

13.2.1 Technical Specifications: GPSANTv2 Antenna

Physical Dimensions



Electrical Specifications

Power Supply: (via Antenna Cable)	15 V ± 3 V
Nominal Current Draw: (via Antenna Cable)	Approx. 100 mA at 15 V, max. 115 mA

Signal Reception & Processing

Reception Frequency:	1575.42 MHz (GPS L1/Galileo E1 Band)
Axial Ratio:	≤ 3 dB at zenith
Element Gain:	Typically 5.0 dBic at zenith
Mixing Frequency:	10 MHz
Intermediate Frequency:	35.4 MHz
Out-of-Band Rejection:	≥ 70 dB @ 1555 MHz ≥ 55 dB @ 1595 MHz
Conversion Gain: Antenna Input to IF Output	59 dB ± 3 dB
Noise Figure:	Typically 1.8 dB, maximum 3 dB at +25 °C
Input Filter Survival Capacity:	Exposure to > 13 dBm for 24 h without destruction
Conversion Delay: (Patch Connector to IF Output)	Typically 152 ns ± 5 ns
Group Delay Ripple within 2.4 MHz System Bandwidth:	Max. 15 ns
Polarization:	Right-Hand Circular Polarization
ETSI-Compliant Frequency Blocking:	Blocked frequency range further extended to 6 GHz
	–40 dBm
P1dB Input:	
Antenna Pattern:	Vertical 3 dB Angle Width: 100° centered around azimuth

Connection

Connector Type:	Type-N, Female
Nominal Impedance:	50 Ω
Voltage Standing Wave Ratio (VSWR):	≤ 1.5 : 1
Grounding:	M8 threaded bolt and hexagon nut for use with corresponding ring lug

Specifications for Interference Immunity

Surge Protection:	Level 4 (per IEC 61000-4-5) Test Voltage: 4000 V Max. Peak Current @ 2 Ω: 2000 A
ESD Protection:	Level 4 (per IEC 61000-4-2) Contact Discharge: 8 kV Air Discharge: 15 kV

Mechanical and Environmental Specifications

Housing Material:	ABS Plastic Case for Outdoor Installation
Specified Environment:	Outdoor Environments
IP Rating:	IP65
Temperature Range (Operation):	–60 °C to +80 °C (–76°C to +176 °F)
Temperature Range (Storage):	–20 °C to +70 °C (–4°C to +158 °F)
Relative Humidity (Operation):	5 % to 95 % (non-condensing)
Weight:	1.4 kg (3.09 lbs), including mounting kit

13.2.2 Technical Specifications: 40 dB Multi-GNSS Antenna for Fixed-Location Applications

The LANTIME LANTIME is typically shipped with an active 40 dB Multi-GNSS Antenna manufactured by PCTEL.

Detailed specifications and installation instructions for the PCTEL 40 dB Multi-GNSS Antenna are provided in the third-party manufacturer's data sheet under the following links:

Data Sheet:

https://www.meinbergglobal.com/download/docs/datasheets/english/ds_gps-gln-l1-antenna.pdf

Manual:

https://www.meinbergglobal.com/download/docs/manuals/english/gps-gln-l1-antenna.pdf

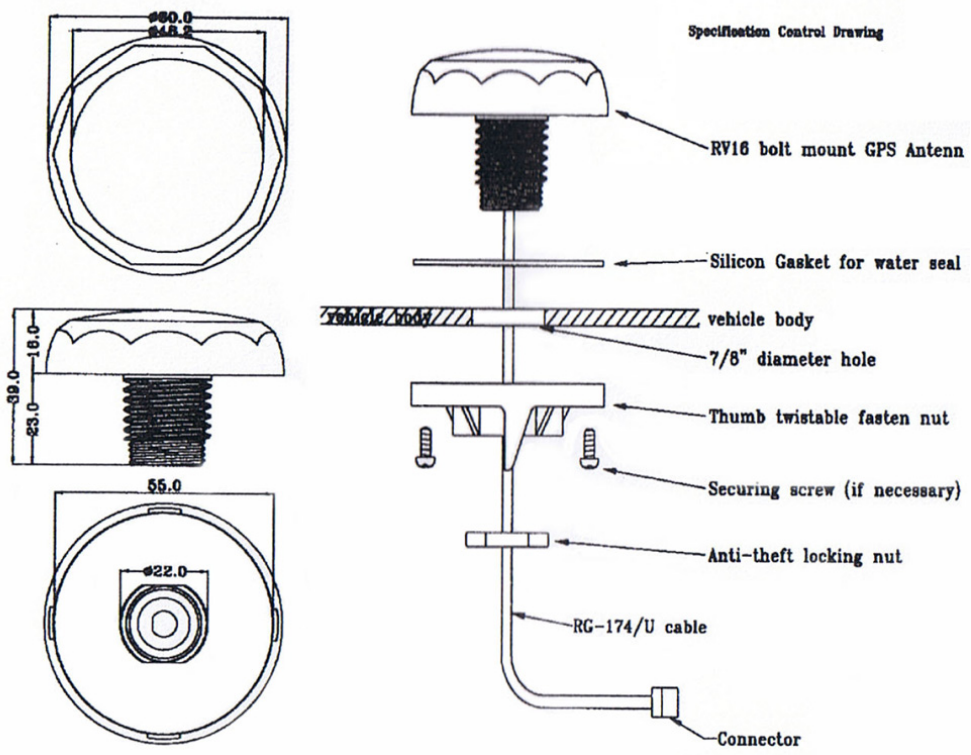
For any updated information about the product, please also visit the product website of the manufacturer PCTEL at:

https://www.pctel.com/antenna-product/gps-timing-reference-antenna-2/

13.2.3 Technical Specifications: 27 dB Mobile Multi-GNSS Antenna for Mobile Applications

The LANTIME LANTIME can also optionally be shipped with a 27 dB Multi-GNSS Antenna manufactured by SANAV. This antenna is intended for *mobile applications*.

Installation Diagram

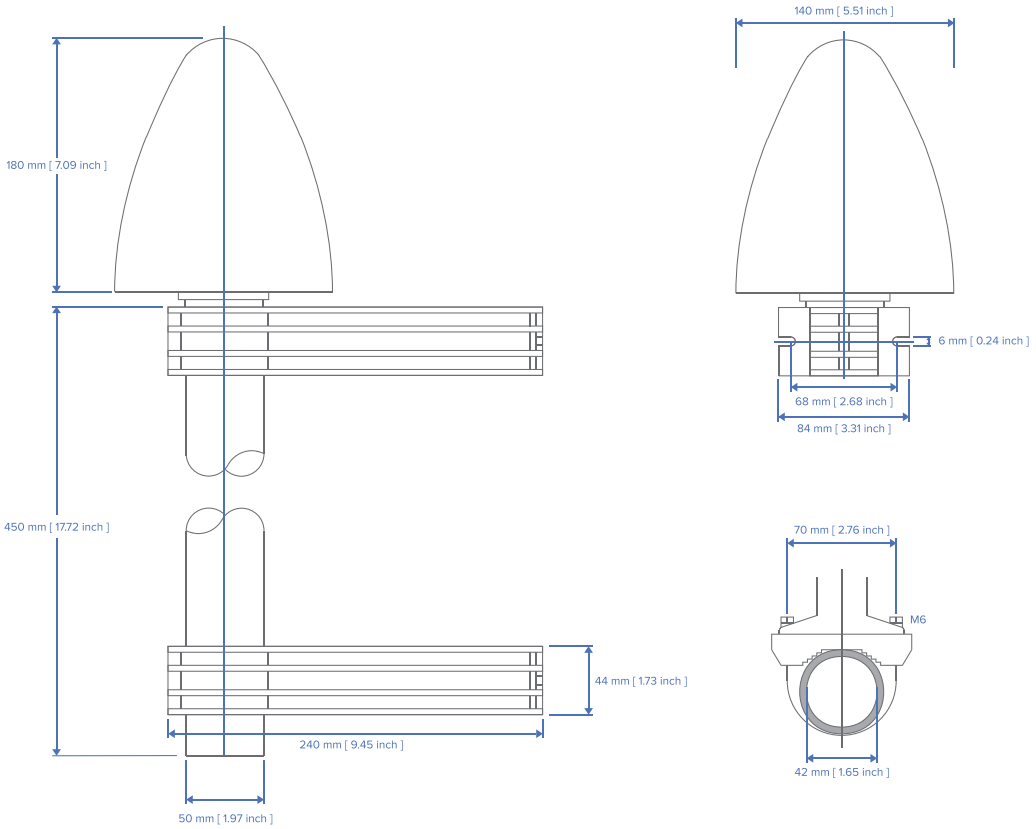


Detailed specifications are provided in the manufacturer's data sheet. The data sheet for the SANAV RV-76G Mobile Multi-GNSS Antenna can be downloaded via the following link:

https://www.meinbergglobal.com/download/docs/other/rv-76g_en.pdf

13.2.4 Technical Specifications: GNSS Multi-Band Antenna

Physical Dimensions



General Specifications

Power Supply:	5 V ⎓ – 16 V ⎓, 24 mA (provided via antenna cable)
Connector Type:	Type-N, Female
Form Factor:	ABS Plastic Case for Outdoor Installation
IP Rating:	IP66
Supported Relative Humidity:	95 %
Supported Temperature Range:	–40 °C to +85 °C (–40 °F to 185 °F)
Weight:	1.6 kg (3.53 lbs), including mounting kit
Frequency Ranges:	1164 MHz – 1254 MHz, 1525 MHz – 1606 MHz
Total LNA Gain:	Minimum 35 dB, Typically 37 dB
Noise Figure:	Typically 2.5 dB at 25 °C

Supported Frequency Bands

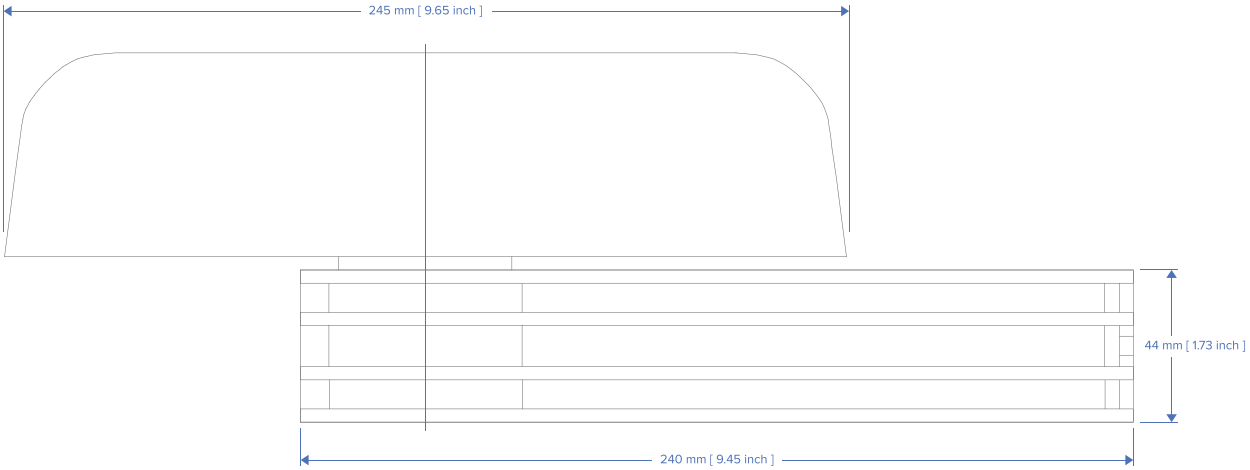
GPS:	L1/L2/L5
GLONASS:	G1/G2/G3
Beidou:	B1/B2/B3
Galileo:	E1/E5a+b plus L-band/E6

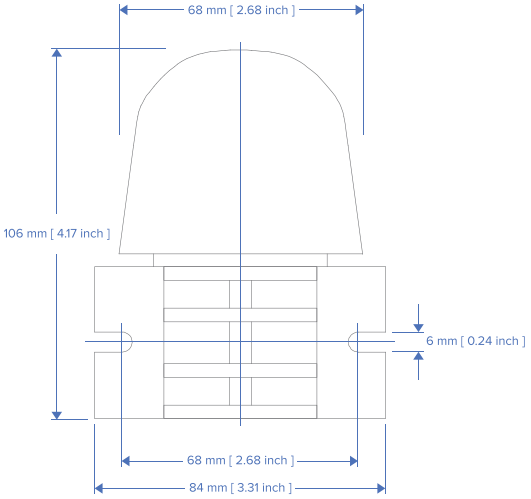
Out-of-Band Rejection

Freq. Band E5/L2/G2:	Frequency	
	< 1050 MHz	> 45 dB
	< 1125 MHz	> 30 dB
	< 1350 MHz	> 45 dB
Freq. Band L1/E1/B1/G1:	Frequency	
	< 1450 MHz	> 30 dB
	< 1690 MHz	> 30 dB
	< 1730 MHz	> 40 dB

13.2.5 Technical Specifications: AW02 Antenna

Physical Dimensions





Electrical Specifications

Power Supply Voltage:	3.5 V ⎓ – 5 V ⎓
Bandwidth:	1 kHz
Signal Level:	50 μV – 5 mV

Mechanical and Environmental Specifications

Connector Type:	Type-N, Female
Housing Material:	ABS Plastic Case for Outdoor Installation
IP Rating:	IP56
Supported Temperature Range (Operation):	-60 °C to +80 °C (–76 °F to 176 °F)
Supported Temperature Range (Storage):	-20 °C bis +70 °C (—4 °F to 158 °F)
Weight:	0.55 kg (1.2 lbs) including mounting kit for wall installation

13.2.6 Technical Specifications: MBG-S-PRO Surge Protector

The MBG-S-PRO is a surge protector (Phoenix CN-UB-280DC-BB) for coaxial connections. It is patched directly into the antenna line and consists of a replaceable gas discharge tube that redirects the energy from the cable shielding to the ground potential when ignited. Connect the MBG-S-PRO using a ground conductor cable that is as short as possible.

The MBG S-PRO has no dedicated input/output polarity and no preferred installation orientation.

Phoenix CN-UB-280DC-BB

Features:

- Excellent RF Performance
- Multiple Strike Capability
- 20 kA Surge Protection
- Bidirectional Protection

Contents of Package:	Surge Protector with Mounting Bracket and Accessories
Product Type:	Surge Protector for Transmission and Receiver Devices
Construction Type:	In-Line Breaker
Connector Types:	Type-N, Female/Type-N, Female

The original product page of the supplier (see link) of the CN-UB-280DC-BB surge protector provides detailed specifications, as well as a variety of product-specific documents under the link below:

Data Sheet (Download):

https://www.meinbergglobal.com/download/docs/shortinfo/english/cn-ub-280dc-bb_pc.pdf

13.3 Time String Formats

13.3.1 Meinberg Standard Time String

The Meinberg Standard time string is a sequence of 32 ASCII characters, starting with the character <STX> (Start of Text, ASCII code 02h) and terminated with the character <ETX> (End of Text, ASCII code 03h). 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:		
	dd	Day of the month	(01–31)
	mm	Month	(01–12)
	yy	Year of the Century	(00–99)
w	The day of the week		(1–7, 1 = Monday)
hh.mm.ss	The time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	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 pattern synchronized DCF77: Clock has synchronized since last reset
	v:	"*"	GPS: Receiver has not yet verified its position PZF/DCF77: Clock currently in free-run mode
		" "	(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 Time active
	"S"	(CEST) Central European Summer Time, Daylight Saving Time inactive	
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		

13.3.2 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, it does not contain UTC time or time adjusted to any local time zone. Instead, it contains GPS time without the UTC adjustments. 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

dd.mm.yy The date:

dd	Day of the month	(01–31)
mm	Month	(01–12)
yy	Year of the Century	(00–99)

w The day of the week (1–7, 1 = Monday)

hh.mm.ss The time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 while leap second)

uv Clock status characters:

u:	"#"	Clock is in free-run mode (no exact synchronization)
	" "	(Space, ASCII code 20h) Clock is synchronized (base accuracy is achieved)
v:	"*"	Receiver has not yet verified its position
	" "	(Space, ASCII code 20h) Receiver has determined its position

G Time zone identifier "GPS Time"

y Announcement of clock jump during last hour before discontinuity comes into effect:

"A"	Announcement of leap second insertion
" "	(Space, ASCII code 20h) nothing announced

lll Number of leap seconds between GPS time and UTC (UTC = GPS time + number of leap seconds)

<ETX> End of Text, ASCII code 03h

13.3.3 Meinberg Capture Time String

The Meinberg Capture time string is a sequence of 31 ASCII characters, terminated with the sequence <CR> (Carriage Return, ASCII code 0Dh) and <LF> (Line Feed, ASCII code 0Ah). The format is as follows:

CH*x*<*SP*>*dd.mm.yy_hh:mm:ss.fffffff*<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, number of input		
<SP>	Space (ASCII code 20h)		
dd.mm.yy	Capture date:		
	dd	Day of the month	(01–31)
	mm	Month	(01–12)
	yy	Year without century	(00–99)
hh:mm:ss.fffffff	Capture Time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
	fffffff	Fractions of second, 7 digits	
<CR>	Carriage Return, ASCII code 0Dh		
<LF>	Line Feed, ASCII code 0Ah		

13.3.4 ATIS Time String

The ATIS standard Time String is a sequence of 23 ASCII characters terminated with a <CR» (Carriage Return) character. The standard interface configuration for this string type is 2400 Baud, 7E1. The format is as follows:

<GID><ABS><TSQ><CC><CS><ST>*yymmddhhmmsswcc*<GID><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:

<GID>	Address of the Receiver, ASCII code 7Fh	
<ABS>	Originator of Message, '0', ASCII code 30h	
<TSQ>	Telegram Number, '0', ASCII code 30h	
<CC>	Command Code 'S' (for 'SET'), ASCII code 53h	
<CS>	Command Code 'A' (for 'ALL'), ASCII code 41h	
<ST>	Time Status 'C' (for valid time), ASCII code 43h	
yymmdd	The current date:	
	yy Year of the Century	(00–99)
	mm Month	(01–12)
	dd Day of month	(01–31)
hhmmss	the current time:	
	hh hours	(00–23)
	mm minutes	(00–59)
	ss seconds	(00–59, or 60 during leap second)
w	Day of the Week	(1–7, 1 = 31h = Monday)
cc	Checksum in hexadecimal, generated from all characters including GID, ABS, TSQ, CC, ST, etc.	
<CR>	Carriage Return, ASCII code 0Dh	

13.3.5 SAT Time String

The SAT time string is a sequence of 29 ASCII characters, starting with the character <STX> (Start of Text, ASCII code 02h) and terminated with the character <ETX> (End of Text, ASCII code 03h). The format is as follows:

<STX>*dd.mm.yy/w/hh:mm:ss*xxxx*u*v<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:

dd	Day of the month	(01–31)
mm	Month	(01–12)
yy	Year without century	(00–99)

w The day of the week (1 = Monday, ... 7 = Sunday)

hh:mm:ss The current time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during leap second)

xxxx Time zone identifier:

"UTC"	Universal Time Coordinated, formerly GMT
"CET"	European Standard Time, daylight saving disabled
"CEST"	Central European Summer Time, Daylight Saving Time active

u Clock status characters:

"#"	Clock has not synchronized since last reset
" "	(Space, ASCII code 20h) Clock has synchronized since last reset

v Announcement for time jump during last hour before event:

"!"	Announcement of start or end of Daylight Saving Time
" "	(Space, ASCII code 20h) nothing announced

<CR> Carriage Return, ASCII code 0Dh

<LF> Line Feed, ASCII code 0Ah

<ETX> End of Text, ASCII code 03h

13.3.6 Uni Erlangen Time String (NTP)

The Uni Erlangen time string (NTP) is a sequence of 66 ASCII characters, starting with the character <STX> (Start of Text, ASCII code 02h) and terminated with the character <ETX> (End of Text, ASCII code 03h). The format is as follows:

<STX>*dd.mm.yy; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn lll.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 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:

dd	Day of the month	(01–31)
mm	Month	(01–12)
yy	Year (without century)	(00–99)

w The day of the week (1–7, 1 = Monday)

hh.mm.ss The time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during leap second)

v Positive/negative sign for offset of local time zone relative to UTC

oo:oo Offset of local time zone relative to UTC in hours and minutes

ac Clock status:

a:	"#"	Clock has not synchronized since reset
	" "	(Space, ASCII code 20h) Clock has synchronized since reset
c:	"*"	GPS receiver has not verified its position
	" "	(Space, ASCII code 20h) GPS receiver has determined its position

d Time zone identifier:

"S"	CEST	Central European Summer Time
" "	CET	Central European Time

f Announcement of clock jump during last hour before discontinuity comes into effect:

"!"	Announcement of start or end of Daylight Saving Time
" "	(Space, ASCII code 20h) nothing announced

g Announcement of clock jump during last hour before discontinuity comes into effect:

"A"	Announcement of leap second
" "	(Space, ASCII code 20h) nothing announced

i Leap second

"L"	Leap second is currently to be inserted (only active in 60th second)
" "	(Space, ASCII code 20h) No leap second announced

bbb.bbbb Geographical latitude of the receiver position in degrees
Leading zeroes are padded with spaces (ASCII code 20h)

n	Geographical hemisphere, possible characters are: "N" North of Equator "S" South of Equator
lll.llll	Geographical longitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)
e	Prime meridian hemisphere, possible characters are: "E" East of Greenwich Meridian "W" West of Greenwich Meridian
hhhh	Altitude in meters of receiver position above WGS84 ellispoid Leading zeroes are padded with spaces (ASCII code 20h)
<ETX>	End of Text, ASCII code 03h

13.3.7 NMEA 0183 String (RMC)

The NMEA 0183 RMC time string is a sequence of 65 ASCII characters, starting with the string "$GPRMC" and terminated with the sequence <CR> (Carriage Return, ASCII code 0Dh) und <LF> (Line Feed, ASCII code 0Ah). The format is as follows:

$GPRMC,*hhmmss.ff*,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 as defined below:

$	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second		
GP	Device ID, in this case "GP" for GPS		
RMC	Message type ID, in this case "RMC"		
hhmmss.ss	The current time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
	ff	Fractional seconds	(1/10 ; 1/100)
A	Status (A = Time data valid, V = Time data not valid)		
bbbb.bb	Geographical latitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)		
n	Geographical hemisphere, possible characters are:		
	"N"	North of Equator	
	"S"	South of Equator	
lllll.ll	Geographical longitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)		
e	Prime meridian hemisphere, possible characters are:		
	"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	Current Date:		
	dd	Day of the month	(01–31)
	mm	Month	(01–12)
	yy	Year of Century	(00–99)
a	Magnetic variation E/W		
hh	Checksum (XOR sum of all characters except "$" and "*")		
<CR>	Carriage Return, ASCII code 0Dh		
<LF>	Line Feed, ASCII code 0Ah		

13.3.8 NMEA 0183 Time String (GGA)

The NMEA 0183 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*,*lllll.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 as defined below:

$	Start character, ASCII code 24h sent with one-bit accuracy at the change of each second
GP	Device ID, in this case "GP" for GPS
GGA	Message type ID, in this case "GGA"
hhmmss.ss	The current time: *hh* Hours (00–23) *mm* Minutes (00–59) *ss* Seconds (00–59, or 60 while leap second) *ff* Fractional seconds (1/10 ; 1/100)
bbbb.bbbbb	Geographical latitude of receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)
n	Geographical hemisphere, possible characters are: "N" North of Equator "S" South of Equator
lllll.lllll	Geographical longitude of the receiver position in degrees Leading zeroes are padded with spaces (ASCII code 20h)
e	Prime meridian hemisphere, possible characters are: "E" East of Greenwich Meridian "W" West of Greenwich Meridian
A	Position determined (1 = yes, 0 = no)
vv	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	Meters (unit as fixed value)
ggg.g	Geoid Separation (WGS84 Altitude - MSL Altitude)
M	Meters (unit as fixed value)
cs	Checksum (XOR sum of all characters except "$" and "*")
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

13.3.9 NMEA 0183 Time String (ZDA)

The NMEA 0183 ZDA time 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 sent 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)		

13.3.10 ABB SPA Time String

The ABB SPA string is a sequence of 32 ASCII characters, starting with the string ">900WD:" and terminated with the character <CR> (Carriage Return). The format is as follows:

>900WD:*yy-mm-dd[lt]SP>hh.mm;ss.fff:cc*<CR>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are directly part of the time string. The groups of characters as defined below:

yy-mm-dd	Current Date:		
	yy	Year without century	(00–99)
	mm	Month	(01–12)
	dd	Day of the month	(01–31)
	<SP>	Space (ASCII code 20h)	
hh.mm;ss.fff	Current Time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 during leap second)
	fff	Milliseconds	(000–999)
cc	Checksum. This is calculated as the XOR sum of the preceding characters. The resultant 8-bit value is reported as a hex value in the form of two ASCII characters (0–9 or A–F)		
<CR>	Carriage Return (ASCII code 0Dh)		

13.3.11 Computime Time String

The Computime time string is a sequence of 24 ASCII characters, starting with the character T and terminated with the character <LF> (Line Feed, ASCII code 0Ah). The format is as follows:

T:*yy:mm:dd:ww:hh:mm:ss*<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are unalterable parts of the time string. The groups of characters as defined below:

T	Start character Sent with one-bit accuracy at the change of each second		
yy:mm:dd	The current date:		
	yy	Year without century	(00–99)
	mm	Month	(01–12)
	dd	Day of the month	(01–31)
	ww	Day of the week	(01–07, 01 = Monday)
hh:mm:ss	The 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		
<LF>	Line Feed, ASCII code 0Ah		

13.3.12 RACAL Time String

The RACAL time string is a sequence of 16 ASCII characters started by a X character and terminated by the <CR> (Carriage Return, ASCII code 0Dh) character. The format is as follows:

XGU*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	Start character (ASCII code 58h) Sent with one-bit accuracy at the change of each second		
G	Control character (ASCII code 47h)		
U	Control character (ASCII code 55h)		
yymmdd	Current date:		
	yy	Year of Century	(00–99)
	mm	Month	(01–12)
	dd	Day of Month	(01–31)
hh:mm:ss	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)		

13.3.13 SYSPLEX-1 Time String

The SYSPLEX 1 time string is a sequence of 16 ASCII characters, starting with the character <SOH> (Start of Header, ASCII code 01h) and terminated with the character <LF> (Line Feed, ASCII code 0Ah).

Important!

To ensure that the time string can be correctly output and displayed through your terminal software of choice, a "C" must be sent (once, without quotes).

The format is as follows:

<SOH>*ddd:hh:mm:ssq*<CR><LF>

The letters printed in italics are replaced by ASCII numbers whereas the other characters are unalterable parts 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 the Year	(001–366)	
hh:mm:ss	The current time:		
	hh Hours	(00–23)	
	mm Minutes	(00–59)	
	ss Seconds	(00–59, or 60 during leap second)	
	q Clock Status:	Space (ASCII code 20h)	Time Sync (GPS Lock)
		"?" (ASCII code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage Return, ASCII code 0Dh		
<LF>	Line Feed, ASCII code 0Ah		

13.3.14 ION Time String

The ION time string is a sequence of 16 ASCII characters, starting with the character <SOH> (Start of Header, ASCII code 01h) and terminated with the character <LF> (Line Feed, ASCII code 0Ah). The format is as follows:

<SOH>*ddd:hh:mm:ss*q<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 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 while leap second)	
	q	Quality Indicator	Space (ASCII code 20h)	Time Sync (GPS Lock)
			"?" (ASCII code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage Return (ASCII code 0Dh)			
<LF>	Line Feed (ASCII code 0Ah)			

13.3.15 ION Blanked Time String

The ION time string is a sequence of 16 ASCII characters, starting with the character <SOH> (Start of Header, ASCII code 01h) and terminated with the character <LF> (Line Feed, ASCII code 0Ah). The format is as follows:

<SOH>*ttt:hh:mm:ss*q<CR><LF>

Important!

The blanking interval lasts for 2 minutes and 30 seconds and is inserted every five minutes.

The letters printed in italics are replaced by ASCII numbers whereas the other characters are unalterable parts 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 the year		(001–366)	
hh:mm:ss	The current time:			
	hh	Hours	(00–23)	
	mm	Minutes	(00–59)	
	ss	Seconds	(00–59, or 60 during leap second)	
	q	Clock Status:	Space (ASCII code 20h)	Time Sync (GPS Lock)
			"?" (ASCII code 3Fh)	No Time Sync (GPS Fail)
<CR>	Carriage Return, ASCII code 0Dh			
<LF>	Line Feed, ASCII code 0Ah			

13.3.16 IRIG-J Timecode

The IRIG-J timecode consists of a string of ASCII characters sent in “701” format, i.e.,:

- 1 start bit
- 7 data bits
- 1 parity bit (odd)
- 1 stop bit

The start of the second is marked by the leading edge of the start bit of the string. The string is 15 characters long and is sent once a 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 numbers whereas the other characters are unalterable elements of the string. The groups of characters as defined below:

<SOH>	Start of Header (ASCII code 01h)
DDD	Day of the year (ordinal date, 1–366)
HH, MM, SS	Time of the start bit in hours (HH), minutes (MM), seconds (SS)
<CR>	Carriage Return, ASCII code 0Dh
<LF>	Line Feed, ASCII code 0Ah

13.3.17 6021 Time String

The 6021 time string is a sequence of 18 ASCII characters starting with the <STX> (Start of Text, ASCII code 02h) ASCII control character and terminated with the sequence <LF> (Line Feed, ASCII code 0Ah), <CR> (Carriage Return, ASCII code 0Dh), <ETX> (End of Text, ASCII code 03h).

It is broadly identical to the ➜ "Freelance Time String", but with a different order to the termination sequence.

The format is as follows:

<STX>*C9hhmmssddmmyy*<LF><CR><ETX>

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:

<STX> Start of Text, ASCII code 02h

C Clock status. This is represented as an ASCII nibble*, whereby each bit in the binary sequence has the following meaning:

Bit 0 (LSB)	Leap second announced (1) / not announced (0)
Bit 1	Leap second active (1) / not active (0)
Bit 2	Real-time clock time valid (1) / invalid (0)
Bit 3 (MSB)	Clock is synchronized (1) / not synchronized (0)

Example: If the clock outputs C (ASCII code 0x43h) at this position, this corresponds to a binary value of *1100*, indicating that the RTC time is valid and the clock is synchronized, and that no leap second has been announced, nor is one in effect.

9 UTC status of clock and day of the week. This is represented as an ASCII nibble*, whereby the three least significant bits represent the day of the week and may be any value between 1 and 7 (corresponding to Monday to Sunday). The most significant bit represents the UTC state and will be 1 if set to UTC and 0 if it is a local time zone. Thus, if the clock is outputting local (non-UTC) time, this will be in a range of 1–7, whereas if the clock is outputting UTC time, this value will be in a range of 9–F.

Example: If the clock outputs 9 (ASCII code 0x39h) at this position, this corresponds to a binary value of *1001*. The most significant bit of *1* here indicates that the clock is running on UTC time, while the 3-bit value represented by the least significant bits *001* indicates that the day is Monday.

hhmmss Current time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during leap second)

ddmmyy Current date:

dd	Day	(01–31)
mm	Month	(01–12)
yy	Last two digits of year	(00–99)

<LF> Line Feed (ASCII code 0Ah)

<CR> Carriage Return (ASCII code 0Dh)

<ETX> End of Text (ASCII code 03h)

* With ASCII nibbles, the actual ASCII character itself (0–9, A–F, ASCII codes *0x30h–0x39h* and *0x41h–0x46h*) represents the hexadecimal equivalent of a 4-bit binary sequence. For example, if the clock outputs "A" at these positions, this is equivalent to a binary sequence of *0x1010b*. Please note that it is not the binary equivalent of the ASCII code (*0x41h*) itself.

13.3.18 Freelance Time String

The Freelance time string is a sequence of 18 ASCII characters starting with the <STX> (Start of Text, ASCII code 02h) ASCII control character and terminated with the sequence <CR> (Carriage Return, ASCII code 0Dh), <LF> (Line Feed, ASCII code 0Ah), <ETX> (End of Text, ASCII code 03h).

It is broadly identical to the ➜ "6021 Time String", but with a different order to the termination sequence.

The format is as follows:

<STX>*C9hhmmssddmmyy*<CR><LF><ETX>

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:

<STX> Start of Text, ASCII code 02h

C Clock status. This is represented as an ASCII nibble*, whereby each bit in the binary sequence has the following meaning:

Bit 0 (LSB)	Leap second announced (1) / not announced (0)
Bit 1	Leap second active (1) / not active (0)
Bit 2	Real-time clock time valid (1) / invalid (0)
Bit 3 (MSB)	Clock is synchronized (1) / not synchronized (0)

Example: If the clock outputs C (ASCII code 0x43h) at this position, this corresponds to a binary value of *1100*, indicating that the RTC time is valid and the clock is synchronized, and that no leap second has been announced, nor is one in effect.

9 UTC status of clock and day of the week. This is represented as an ASCII nibble*, whereby the three least significant bits represent the day of the week and may be any value between 1 and 7 (corresponding to Monday to Sunday). The most significant bit represents the UTC state and will be 1 if set to UTC and 0 if it is a local time zone. Thus, if the clock is outputting local (non-UTC) time, this will be in a range of 1–7, whereas if the clock is outputting UTC time, this value will be in a range of 9–F.

Example: If the clock outputs 9 (ASCII code 0x39h) at this position, this corresponds to a binary value of *1001*. The most significant bit of *1* here indicates that the clock is running on UTC time, while the 3-bit value represented by the least significant bits *001* indicates that the day is Monday.

hhmmss Current time:

hh	Hours	(00–23)
mm	Minutes	(00–59)
ss	Seconds	(00–59, or 60 during leap second)

ddmmyy Current date:

dd	Day	(01–31)
mm	Month	(01–12)
yy	Last two digits of year	(00–99)

<CR> Carriage Return (ASCII code 0Dh)

<LF> Line Feed (ASCII code 0Ah)

<ETX> End of Text (ASCII code 03h)

* With ASCII nibbles, the actual ASCII character itself (0–9, A–F, ASCII codes *0x30h–0x39h* and *0x41h–0x46h*) represents the hexadecimal equivalent of a 4-bit binary sequence. For example, if the clock outputs "A" at these positions, this is equivalent to a binary sequence of *0x1010b*. Please note that it is not the binary equivalent of the ASCII code (*0x41h*) itself.

13.3.19 ITU-G8271-Y.1366 Time-of-Day Message

The ITU-G8271-Y.1366 standard stipulates the transmission of this time message at 9600 Baud with framing of 8N1. The message data should be sent no sooner than 1 ms after the rising edge of the PPS signal and transmission must be completed within 500 ms. The message should be sent once a second and mark the rising edge of the PPS.

The ITU-G8271-Y.1366 time message itself output by Meinberg clocks is always a sequence of 21 bytes. While the standard briefly references the use of two ASCII characters for the first two characters, it should be noted that this message is not an ASCII string in the typical sense. Multi-octet values are transmitted as big-endian values, while each byte is transmitted with the least-significant bit **first**. Accordingly, while the first two characters are deemed to represent the ASCII characters "C" (ASCII code 0x43h, binary 00101011) and "M" (ASCII code 0x4Dh, binary 01001101) respectively, these are transmitted as 11010100 and 10110010.

The standard byte sequence (least significant bit first in each byte) is as defined below:

Byte No.	Meaning
0–1	Always 0x43h followed by 0x4Dh. These are Sync Characters 1 & 2 respectively and are used as a delimiter between messages.
2	The message class. This will always carry a value of 0x01h.
3	The message ID. In the time-of-day messages provided by Meinberg clocks this will always be 0x01h.
4–5	The payload length, expressed as an unsigned 16-bit integer, not including the sync characters, message class, message ID, or checksum. In the time-of-day messages provided by Meinberg clocks this will always be 0x0Eh.
6–11	PTP time, or the number of seconds in the TAI timescale. This is expressed as an unsigned 48-bit integer.
12	This byte is reserved for future use and is set to 0x00h.
13	Contains a number of time status flags: **Bit 0:** Positive leap second pending **Bit 1:** Negative leap second pending **Bit 2:** UTC offset valid **Bit 3:** Reserved **Bit 4:** Time is traceable to a primary frequency standard **Bit 5:** Frequency is traceable to a primary frequency standard **Bit 6:** Reserved **Bit 7:** Reserved
14–15	Current offset between TAI and UTC in seconds, expressed as an unsigned 32-bit integer.
16–19	This byte is reserved for future use and is set to 0x00h.
20	An 8-bit cyclic redundancy check value calculated on the basis of bytes 2–19.

13.3.20 CISCO ASCII Time String

The CISCO ASCII time string is a sequence of at least 73 ASCII characters. The format is as follows:

*.A.*mjdxx*,*yy/mm/dd*,*hh*:*mm*:*ss*,*+3600.0*,*12N34.567*,*123W45.678*,+1234,
EV<SP>GPS<SP>FLT

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:

*	Sync state of clock: *: Clock is synchronized to reference !: Clock is not synchronized
A	The format revision. With Meinberg clocks, this will always be 'A'.
mjdxx	The current date in Modified Julian Date format.
yy/mm/dd	The current date in Gregorian *yy*/*mm*/*dd* format.
hh:mm:ss	The current time in 24-hour format.
+3600	The current local time offset in seconds. If the clock is outputting UTC time, this will be 00000.0. If the clock is outputting local time, however, the first character will be the sign (– or +) and the subsequent digits up to the period character are the offset. For example, if CET is set as the time zone, this will show +3600.
0	Indicator of a pending leap second.
12N34.567	The current latitude of the GNSS receiver. If the time reference is not a GNSS receiver, this will show 00 00.000.
123W45.678	The current longitude of the GNSS receiver. If the time reference is not a GNSS receiver, this will show 000 00.000
+1234	The current altitude above sea level of the GNSS receiver. If the time reference is not a GNSS receiver, this will show +0000.
EV	Indicates the level of any current alarm state of the clock: EV: Non-error event MN: Minor error MJ: Major error CL: Critical error
GPS	Indicates the source of the current error (e.g., 'GPS' for GPS receiver).
FLT	Indicates the cause of the current error (e.g., 'FLT' for hardware fault).

13.3.21 NTP Type 4 Time String

The NTP Type 4 time string is a sequence of 24 ASCII characters. The format is as follows:

?<SP>*yy*<SP>*ddd*<SP>*hh:mm:ss.SSS*L<SP>S

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:

?	Sync state of clock:		
	Space:	Clock is synchronized to reference	
	'?':	Clock is not synchronized	
yy	Year of the century		(00–99)
ddd	Day of the year		(001–366)
hh:mm:ss.SSS	Current time:		
	hh	Hours	(00–23)
	mm	Minutes	(00–59)
	ss	Seconds	(00–59, or 60 while leap second)
	SSS	Milliseconds	(000–999)
L	Leap second announcement:		
	Space:	No leap second announcement	
	'L':	Leap second pending	
S	Daylight Savings Time indicator:		
	'S':	Standard Time (wintertime)	
	'D':	Daylight Savings Time (summertime)	

13.4 Time Code Formats

Each IRIG format carries a designation comprising a letter followed by three numerical digits. The letter and each of the digits represents a characteristic property of the corresponding IRIG code.

Depending on your Meinberg product, more or less time code formats are supported.

A002: 1000 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD)

A003: 1000 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD), time of day (SBS)

A132: 1000 pps, AM sine-wave signal, 10 kHz carrier frequency
Time of year (BCD)

A133: 1000 pps, AM sine-wave signal, 10 kHz carrier frequency
Time of year (BCD), time of day (SBS)

B002: 100 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD)

B003: 100 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD), time of day (SBS)

B006: 100 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD), calendar year (BCD)

B007: 100 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD), year, time of day (SBS)

B122: 100 pps, AM sine-wave signal, 1 kHz carrier frequency
Time of year (BCD)

B123: 100 pps, AM sine-wave signal, 1 kHz carrier frequency
Time of year (BCD), time of day (SBS)

B126: 100 pps, AM sine-wave signal, 1 kHz carrier frequency
Time of year (BCD), calendar year (BCD)

B127: 100 pps, AM sine-wave signal, 1 kHz carrier frequency
Time of year (BCD), calendar year (BCD), time of day (SBS)

E002: 10 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD)

E112: 10 pps, AM sine wave signal, 100 Hz carrier frequency
Time of year (BCD)

G002: 10000 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD)

G006: 10000 pps, DCLS, pulse-width coded, no carrier
Time of year (BCD), calendar year (BCD)

G142: 10000 pps, AM sine-wave signal, 100 kHz carrier frequency
Time of year (BCD)

G146: 10000 pps, AM sine-wave signal, 100 kHz carrier frequency
Time of year (BCD), calendar year (BCD)

Abbreviations:
BCD = Binary-Coded Decimal, SBS = Straight Binary Seconds

In addition to the original IRIG standards, there are also other specifications issued by other bodies that define specific extensions.

AFNOR:	Code according to NF S87-500, 100 pps, AM sine-wave signal, 1 kHz carrier frequency, BCD time of year, complete date, SBS time of day, signal level specified by standard.
IEEE 1344:	Code according to IEEE 1344-1995, 100 pps, AM sine wave signal, 1kHz carrier frequency, BCD time of year, SBS time of day, IEEE 1344 extensions for date, time zone, Daylight Saving Time, and leap seconds in Control Functions (CF) segment. (See also table "Structure of CF segment in IEEE 1344 mode")
IEEE C37.118:	Identical to IEEE 1344, but with UTC offset +/- sign bit reversed
NASA 36:	100 pps, AM sine wave signal, 1 kHz carrier frequency, resolution: 10 ms (DCLS), 1 ms (modulated carrier) BCD time of year: 30 bits - seconds, minutes, hours, and days

13.5 Overview of Programmable Signals

Meinberg systems with programmable pulse outputs provide the following signal options; the actual range of available signal options will vary from system to system:

Idle

Selecting "**Idle**" allows individual programmable outputs to be disabled individually.

Timer

In "**Timer**" mode, the output simulates a timer with a fixed daily schedule. It is possible to configure three switch-on and three switch-off times for each day and each output. In order to set a timer, both the switch-on time ("**ON**") and the corresponding switch-off time ("**OFF**") must be set. If the switch-on time is later than the switch-off time, the switching scheduler will interpret this to mean that the switch-off time is on the next day, which will keep the signal enabled through midnight.

Thus, if a program was set with a switch-on time of *23:45:00* and a switch-off time of *0:30:00*, this would cause the output to be enabled on day *n* at 11:45 p.m., and then to be disabled on day *n+1* at 12:30 a.m. If any of these three programs are to be left disabled, simply enter the same times into the **ON** and **OFF** fields. The "**Signal**" selector specifies the active state for the timer periods. Selecting "*Normal*" will put the output in a low state outside of switch-on periods and in a high state during switch-on periods ("active high"). Conversely, selecting "*Inverted*" will place the output in a high state outside of switch-on periods and in a low state during switch-on periods ("active low").

Single Shot

"**Single Shot**" mode generates a single pulse of defined length once per day. The time of day when the pulse is to be generated can be set via the "**Time**" value. The value "**Length**" allows the pulse length to be set in 10 ms increments and may be any value in the range of *10 ms* to *10000 ms* (10 seconds). Entries that are not multiples of 10 ms will be rounded down.

Cyclic Pulse

"**Cyclic Pulse**" mode is used to generate cyclically repeating pulses. The time between two pulses is defined, and this value must always be provided in hours, minutes, and seconds. It is important to note that the pulse train is always synchronized with 0:00.00 local time, so that the first pulse on any given day will always be output at midnight, and is repeated at the specified cycle interval henceforth. Thus, if a cycle duration of *2 s* is specified, this will result in pulses being triggered at 0:00.00, 0:00.02, 0:00.04 and so on. While it is possible to set any cycle time between 0 and 24 hours, these repetitions are usually only useful if the time between pulses is always the same. For example, if a cycle time of *1:45.00* is set, this will output pulses at intervals of 6300 seconds. However, between the last pulse of any given day and the pulse at midnight on the following day, there will be an interval of just 4500 seconds.

Pulse-per-Second, Pulse-per-Minute, Pulse-per-Hour

These three modes generate pulses of defined length once per second, once per minute, or once per hour respectively. The configuration options for all three modes are the same. The value "**Pulse Length**" specifies the length of the pulse and can be between *10 ms* and *10000 ms* (10 seconds).

DCF77 Marks

In "**DCF77 Marks**" mode the selected output simulates the time string transmitted by the German DCF77 time code transmitter. The output pulses are the 100 ms and 200 ms pulses (logical 0/1) typical for the DCF77 code. The absence of the 59-second mark is used to signal that the next minute will begin with the following second mark.

DCF77-like M59

Sends a 500 ms pulse at the 59-second mark.

The "**Timeout**" field can be used to enter how many minutes the system should wait while in free-run mode before DCF77 simulation is suspended. Entering *0* here will disable the timeout function, so that the DCF77 simulation will continue running perpetually until manually disabled.

Position OK, Time Sync, All Sync

There are three different modes available for outputting the synchronization status of the clock. The "**Position OK**" mode outputs a signal whenever the GNSS receiver is receiving enough satellites to determine its position.

In "**Time Sync**" mode, a signal is only output as long as the clock's internal timebase is synchronized to the GNSS reference. The "**All Sync**" mode requires both of the above states to be true—for a signal to be output, there must be sufficient satellites for positioning, and the internal timebase must be synchronized to the reference constellation's timebase.

DCLS Timecode

DC level shift timecode. The timecode output here is configured in the "**Clock**" → "**IRIG Settings**" section of the Web Interface.

1 MHz Frequency, 5 MHz Frequency, 10 MHz Frequency

This mode is used to output a fixed frequency of 1, 5, or 10 MHz respectively, using a PPS signal as an absolute phase reference (i.e., the falling edge of the signal is synchronized with the rising edge of the PPS signal).

Synthesizer Frequency

This mode is used to output a custom frequency, which is defined using the "**Clock**" → "**Synthesizer**" section of the Web Interface.

Time Slots per Minute

This mode divides each minute up into a number of equal time slots, which can be individually enabled during those seconds of each minute. For example, if *six* time slots are selected, the user can set whether a signal should be output during the 0–10-second, 10–20 second, 20–30 second, 30–40 second, 40–50 second, and 50–60 second slots. If only the *10–20 second* slot is selected, a signal will only be output between 10 and 20 seconds of each minute and disabled outside of that.

PTTI 1PPS

This mode is used to pass a PPS signal of 20 μs pulse width through the output.

13.6 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
optInterfaceIp	=	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",
    "optInterfaceIp":   "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"
}
```

13.7 Fundamentals of IEC 61850

IEC 61850 is an international standard for communication protocols in electrical substations and power distribution systems.

The standard provides an extensive framework for the exchange of data and information between a variety of devices and systems within a substation. It establishes a common communication architecture, data models, and protocols to enable seamless integration and interoperability between devices from different manufacturers.

The key features of the IEC 61850 standard are:

- Communication Architecture: IEC 61850 defines a multi-layered architecture that enables multiple levels of a station automation system (e.g., process, field, station levels) to exchange information. The architecture defines the roles and responsibilities of each device and component within the system.
- Data Modeling: IEC 61850 establishes a standardized data model that serves as a common language for describing data and functions provided by substation devices. This allows data to be uniformly represented and interpreted across a variety of devices and systems.
- Communication Protocols: IEC 61850 which protocols may be used for real-time communication between devices, including Generic Object-Oriented Substation Events (GOOSE) and Sampled Measured Values (SMV). These protocols enable control commands, status information, and measurements to be exchanged reliably with minimal latency.
- Configuration and Project Management: IEC 61850 introduces a standardized approach to system configuration and development that facilitates the configuration, testing, and maintenance of station automation systems. It provides guidelines for defining system requirements, configuring devices, and the management of communication networks.
- Interoperability: One of the main objectives of IEC 61850 is to encourage interoperability between devices and systems from different manufacturers. The use of standardized data models and communication protocols in the standard facilitates the seamless integration and exchange of data, regardless of the provider or technology use.

13.7.1 Data Sets

A data set in IEC 61850 is a list of variables that share a common context and can be transmitted together efficiently. Data sets may be defined by CID/SCL files or generated by MMS clients via the MMS protocol (Manufacturing Messaging Specification, defined in IEC 61850-8-1).
Data sets in IEC 61850 are defined using the Common Information Model (CIM) that enables data and functions within a power network to be represented in a consistent fashion. The CIM provides a common language for describing data elements and their relationships within a substation.

A data set generally consists of a series of data attributes or parameters that define specific information about a device, e.g., its status, its network address, or its configuration. These attributes are organized into logical groups within the data set in order to facilitate data interpretation.

Substation Configuration Language (SCL)

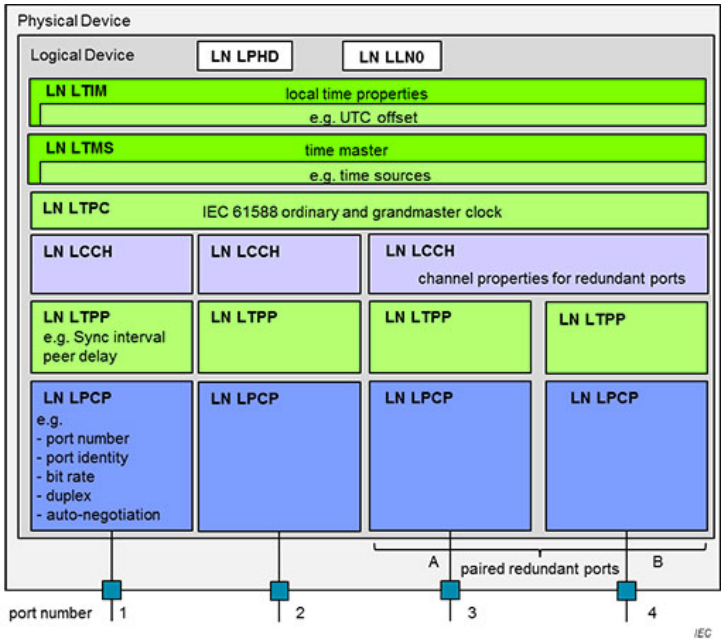
The Substation Configuration Language is an XML-based file format for describing IEDs and their relationships. It is intended to describe a whole substation and of its communication properties. SCL can be used to configure IEC 61850-compliant IEDs. The data model (how a device's data is organized) is usually defined in an SCL file. A tool is then used to convert this SCL file to a description format supported by an IEC 61850 client or server system. There are a number of types of SCL files. The most commonly used types are:

- **ICD (IED Capability Description):** ICD files describe a device's properties. It can be thought of as a template that contains a generic description of all functions and objects that are supportable by a specific device. The ICD is generated by the developer or manufacturer. The ICD file is fed into the System Configuration Tool (SCT), with which the user generates a Substation Configuration Description file (SCD).
- **SCD (Substation Configuration Description):** The SCD file contains all devices required for the system.< A Configured IED Description (CID) file, which describes the functions and objects required by the IED for this specific system, can be exported from the SCT.
- **CID (Configured IED Description):** Contains the complete configuration for a single IED. This file is normally uploaded to the IED as part of the final device configuration.

Description files are usually configured and managed using IEC 61850-compliant tools. These tools allow system integrators and engineers to define and configure data sets on the basis of the specific requirements of the substation.

13.7.2 Structure of a IEC 61850 CID File

IEC 61850 makes use of CID files (Configured IED Descriptions) to describe the configuration and data model of an Intelligent Electronic Device (IED) within a station automation system. CID files describe the properties, data attributes, communication parameters, and other relevant information pertaining to the IED in a structured form that is usually consistent with the XML format (eXtensible Markup Language).



Overview of the Structure of an IEC 61850 CID file:

- **HEAD** - Header section: The header of a CID file contains general information about the file itself, such as the version, creation date, and author. It can also contain additional metadata relating to the IED or substation.
- **LD** - Logical Device: The "Logical Device" section defines the logical position of the IED within the substation. It contains information such as logical device names, IDs, and a description. This section can also be used to specify the communication address and the network parameters for the IED.
- **LN** - Logical Nodes: A logical node within a logical device represents the functional components or devices of each IED. Each logical node corresponds to a certain function or device type, e.g., circuit breakers, transformers, or safety relays. The Logical Node section defines the attributes, data objects, and services associated with each logical node.
- **DO** - Data Objects: The data objects represent the data attributes and functions of each logical node. They define the specific parameters, status flags, and measurements associated with each data object. The Data Objects section describes the IED's data model, including its structure, data types, and also the relationships between objects.
- **Services** : The Services section of the CID file specifies the services supported by the IED, e.g., event reports, control commands, or file transfers. It defines the communication protocols, message formats, and behavior of each service. This section can also be used to allocate data objects to the services and communication protocols defined in IEC 61850.
- **Templates** - Templates allow frequently used data objects or configurations to be defined. They enable configurations to be efficiently reused for multiple IEDs or substation projects, thus avoiding repetition of work and simplifying configuration management.
- SCL Version and Namespace: The CID file can contain information on the version of the IEC 61850 standard that it seeks to be compliant with. It can also specify the namespace associated with the CID file, which is a unique identifier used to reference and identify the IED within the substation.

The structure of a CID file can vary depending on the specific implementation and the requirements of the IED

and substation. However, the elements above provide a general overview of the information typically present in an IEC 61850 CID file.

13.8 How Navigation Message Authentication Works

Spoofing is defined as the manipulation of GNSS messages with a view to tricking a receiver into believing that it is receiving a legitimate signal. Spoofing stands in contrast to *jamming*, which involves the much less sophisticated process of simply suppressing GNSS signals in a local environment by introducing noise into the band frequencies.

Types of Spoofing

Spoofing strategies largely fall into two categories: the relaying of genuine GNSS messages, known as *meaconing*, and the fabrication of artificial GNSS messages on the carrier frequency, whether in phase with the original signal carrier (synchronous spoofing) or out of phase (asynchronous spoofing).

Meaconing is the least sophisticated method of spoofing, and simply involves relaying a genuine GNSS message from another location or a previous point in time in order to confuse GNSS receivers.

Asynchronous and synchronous spoofing techniques on the other hand involve the broadcast of forged GNSS messages.

Asynchronous attacks are comparatively easier to execute but are also easier to detect; because an asynchronous attack signal is out of phase with the genuine GNSS signal, receivers will typically lose their lock on the genuine signal and require a certain amount of time to acquire the new one. Accordingly, even without bespoke spoofing detection, the unexplainable loss of a GNSS lock can in itself be interpreted as a warning sign of attempted spoofing.

Synchronous spoofing is naturally much more difficult to detect and execute; where asynchronous spoofing exhibits a tell-tale phase jump that receivers can detect to trigger an alarm, synchronous spoofing instead usually relies on phase synchronization with the genuine signal and therefore lacks this phase discontinuity. As such, it can be highly effective from an adversary's perspective, especially when combined with a very subtle and gradual divergence from the genuine GNSS source, but is logistically challenging to execute and therefore less commonly encountered.

Outside of a limited number of legitimate engineering and testing applications, there are few benign applications for spoofing. Spoofing is typically a strategy in criminal activities, espionage, and military operations for the purpose of disrupting critical applications or evading scrutiny. There are otherwise few legitimate applications for spoofing; security-centric operations geared towards shielding critical infrastructure or operations from GNSS coverage have no need for the subterfuge enabled by spoofing and will instead typically use jamming strategies in order to prevent precise geopositioning.

Protecting GNSS Signals

Military GNSS applications have long enjoyed the benefits of protecting and authenticating GNSS signals, but as civilian applications relying heavily on accurate and genuine GNSS reception—particularly critical instructure such as the finance and energy sectors—have increasingly come under attack in recent years, interest has grown in providing civilian applications with similar protection.

In military applications, such security mechanisms typically involve encrypting GNSS signals from the outset and requiring strictly controlled decryption material to decode them, or transferring authentication data over a secure channel to which only a very limited circle of authorized users have access. As such, the public availability of civilian GNSS services, make the logistical and security challenges rather different for such a civilian implementation.

The Basics of Navigation Message Authentication

Any security mechanism that involves the transmission of authentication data for GNSS navigation messages for the purpose of verifying the authenticity of the navigation message is referred to as **Navigation Message Authentication**, or simply **NMA**. Implementations of NMA aim to provide protection against spoofing by allowing receivers to identify fraudulent messages based on correlation data from a trusted source.

While NMA is a long-established feature of military-grade GNSS (such as the high-precision encrypted P(Y)-code signal), NMA mechanisms for civilian use are still relatively novel, and as such, there are still only a small number of manufacturers of commercial receivers that already support them—Meinberg being among those few.

NMA typically works by generating a digital signature or a summary of GNSS data at a highly secure point in the communication chain. Such a signature or summary might be generated by the GNSS satellites themselves or by terrestrial reference stations, and achieve their security by way of one-way cryptography or controlled access to the key material. These signatures or summaries are then sent to the receiver by some secure means—some native solutions transmit the signature on their own frequency bands, while others transmit the data over a separate satellite service on a different frequency within the L-band. NMA solutions can also differ in terms of how they split up their signature data and the key material required to decrypt or authenticate it—some may distribute the key over the same channel as the GNSS data (achieving security by delaying delivery of the key), some might use an alternative frequency or system, some might use an entirely different channel such as the public internet.

In theory, any channel capable of carrying digital data in real time with low latency, such as the public internet or terrestrial radio, could be used for the delivery of signatures and keys, although the security and reliability of such methods is naturally a topic of debate.

Current Implementations

The Galileo constellation is currently the only GNSS constellation to operationally provide native NMA for civilian use; the implementation is referred to as OSNMA (Open Service Navigation Message Authentication) and has only recently officially gone live. The drawback of OSNMA is that its usefulness is limited in a multi-GNSS receiver context, as only the Galileo E1 signals can be authenticated. This means that, without the help of third-party services, the corresponding GPS, BeiDou, and GLONASS civilian signals cannot be authenticated.

A prospective civilian NMA implementation for the GPS constellation (currently still under development) is known as Chimera (**Chi**ps **M**essage **R**obust **A**uthentication) and is not supported by any commercially available receiver at this time.

BeiDou and GLONASS do not yet offer any known NMA mechanisms for civilian use, although this may change in the future.

Real-World Cryptographic Methods

As outlined above, NMA technologies typically utilize cryptography-based algorithms to generate a robust **digital signature** or **Message Authentication Code** (MAC) for a navigation message. The message can then be authenticated by verifying the signature against a corresponding key. Such a signature might be generated by means of asymmetric or symmetric encryption methods (or a mixture of both), with each method presenting their own individual advantages and drawbacks. Regardless of the method, it is essential that the key must be *trusted*; that is, there must be no indication that an adversary could potentially forge the key or break the cryptography in order to generate a valid signature.

Purely symmetric methods are conventionally not well-suited to free-to-air NMA solutions for civilian GNSS due to their reliance on a single key for encryption and decryption (known as a 'shared secret'). If the key is public knowledge, then an adversary could simply spoof the message, the key, **and** the MAC. This key would therefore have to be provided via an alternate channel that an adversary cannot access. Because civilian GNSS signals are by definition publicly accessible, it would be impossible to provide such a trusted key without security precautions that are by definition incompatible with the principle of free public access.

For this reason, symmetric-only methods are better suited to state-level applications such as military GNSS

that enforce more granular control over key distribution by limiting it to a small circle of trusted users. Symmetric methods may also be protected with a second layer of security such as a key rotation or renewal system; new keys might be drawn at fixed time intervals from a list, generated pseudorandomly on the basis of a time-indexed seed (so that the algorithm always generates the same key depending on the current time window), or communicated ad hoc to trusted users over secure channels.

Asymmetric methods, on the other hand, rely on "private/public" key pairs. A private key is used at the transmitter end to generate a digital signature or to encrypt the entire message. The corresponding public key, as the name suggests, is publicly available and can be used to either decrypt navigation messages encrypted with the corresponding private key or to authenticate digital signatures generated using the private key. It cannot, however, be used to generate valid digital signatures or MACs.

One of the drawbacks of purely asymmetric methods when compared to symmetric-key cryptography is that private/public-key solutions can be computationally expensive—substantial hardware resources are required to authenticate or decrypt encrypted data. With the bitrates of GNSS signals also being conventionally rather low, asymmetrically generated MACs can also be rather long, leading to additional delays in authentication. Accordingly, asymmetric methods in NMA are better suited to encryption rather than hash-based signatures.

In practice, many real-life NMA mechanisms utilize hybrid solutions or novel key distribution solutions. Galileo's OSNMA, for example, uses quasi-asymmetric methods to protect the algorithm used to generate the chain of public keys, while allowing receivers to authenticate the public keys and regenerate the chain backwards.

13.8.1 Galileo OSNMA

Galileo OSNMA (**O***pen* **S***ervice* **N***avigation* **M***essage* **A***uthentication*) is a mechanism in which authentication data is integrated into the Galileo Open Service navigation messages (I/NAV messages) transmitted by a subset of the Galileo constellation satellites on the E1 band in order to allow compatible receivers to certify the integrity and authenticity of the messages received.

The project was initiated in February 2017 following a decision by the European Commission regarding the technical and operational specifications of the Galileo constellation for commercial and industrial use. In particular, it specified that:

> *The authentication capacity should increase the degree of safety and prevent risks of falsification and fraud in particular. Additional features must therefore be incorporated into satellite signals in order to assure users that the information which they receive does come from the system under the Galileo program and not from an unrecognized source. For instance, the authentication capacity of the commercial service would on the one hand integrate the capacity to authenticate data linked to geolocation, which will be contained in the signals of the open service, offered free of charge, and would on the other hand, with a view to improved protection, also comprise unique identification of the signals thanks to the reading of encrypted codes also contained in the signals, access to which would be subject to a fee.*
>
> *Commission Implementing Decision (EU) 2017/224, dated February 8, 2017*

The initial test phase for OSNMA began in November 2020 and concluded in 2023.

Backwards compatibility with existing receivers is ensured by using the reserved field "`Reserved 1`" of the E1 I/NAV message to accommodate the OSNMA data. Retaining the specified message structure in this way ensures that legacy Galileo receivers should remain operable without restrictions despite the inclusion of this data; any compliant legacy receiver lacking OSNMA support should simply disregard the 40-bit data stream in this field.

OSNMA employs a chain-of-trust mechanism known as **T**imed **E**fficient **S**treamed **L**oss-Tolerant **A**uthentication, or simply **TESLA**. This chain of trust is achieved by ensuring that the keys used to sign Message Authentication Codes are traceable back to a trusted source.

The root of this trust hierarchy consists of a **Merkle Root File**. The Merkle Root is used as a point of reference to validate the presence of a value in the corresponding *Merkle Tree*, which is a hierarchy of values that represent the iterative concatenation and hashing of two values over a fixed number of levels until all value pairs resolve to a common Merkle Root. The current OSNMA Merkle Root File is pre-installed on your clock module by Meinberg and is expected to be renewed only very rarely; if and when renewal becomes necessary, the file can be acquired from the European Union GNSS Service Center website. The Merkle Root File also specifies the **hashing algorithm** for the Merkle Tree, which at time of writing is SHA-256 and can only be modified by means of this file. Notifications that the Merkle Root is to be replaced will be issued years in advance over the Galileo E1 band and reported through your Meinberg device's management interfaces, but the Merkle Root File itself will need to be installed manually.

TESLA also requires a trusted **Public Key** to be installed on the receiver. This Public Key is combined with the key type and key ID to form a value that must match the specified leaf (node) of the current Merkle Tree. Such a Public Key is pre-installed on your clock module by Meinberg. Further Public Keys are typically acquired over the Galileo E1 band and can only be trusted once likewise verified against the locally stored Merkle Root.

Once a receiver is suitably equipped with a trusted Merkle Root and Public Key, it can acquire the **Root Key** of the week (`KROOT`) from the Galileo E1 I/NAV messages. Note that this is not the Merkle Root File specified above; the Root Key represents the end of a given TESLA key chain, which is a sequence of keys generated algorithmically and used to sign Message Authentication Codes. This Root Key must be validated using a validated Public Key before the TESLA chain can be used. All valid keys within the current TESLA chain are traceable back to the Root Key via the hashing algorithm notified in the `KROOT` data.

Once the Root Key of the TESLA chain has been validated, it can be used to trace keys back along the TESLA chain. A receiver that is in possession of both a chain's Root Key `KROOT`, any subsequent key in the same chain, and the required hashing algorithm can reconstruct any key between the root key and the latest received key in the chain and thus authenticate navigation messages using MACs for which the corresponding TESLA chain keys may have been lost in transmission for any reason (e.g., interference).

TESLA's security is enabled by the computational unfeasibility of anticipating the next key in the chain. Because the TESLA key chain is generated in advance using a one-way function with a seed that is known only to the operator of the Galileo constellation, and because the applicable TESLA key is not transmitted for a given MAC until the subsequent message, an adversary lacks the necessary key information needed to generate a valid MAC. Because all TESLA keys also need to be traceable to the validated Root Key, said adversary cannot simply generate a sequence of spoofed messages. Likewise, the Root Key also cannot be spoofed, as the adversary lacks the necessary information (function and seed) used to generate the Merkle tree.

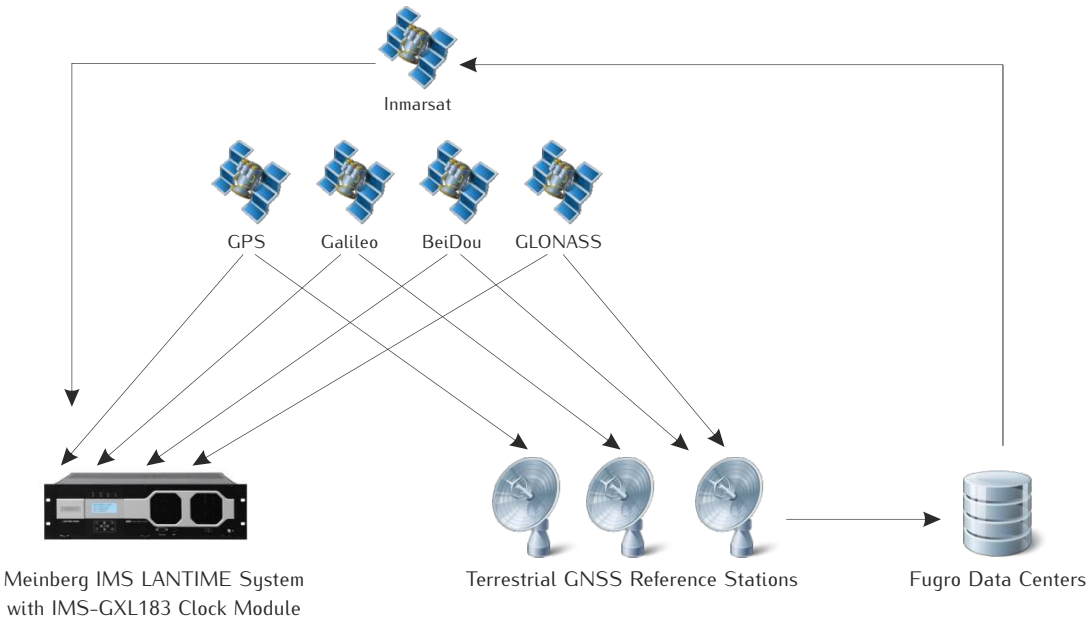
A TESLA chain typically consists of thousands of keys; the key in force at any given time is dependent on the time of the week. Accordingly, for OSNMA to correctly identify the key in force, the receiver must be *loosely* synchronized with Galileo System Time. The necessary accuracy here is 30 seconds by virtue of the transmission of individual sub-frames in the I/NAV messages lasting 30 seconds, such that MACs and keys are transmitted with the same regularity. By extension, each key in the TESLA chain is also in force for 30 seconds.

This synchronization is essential in order to limit the risk of *meaconing*; a receiver can determine when a given chain key should have been transmitted by counting the number of iterative hash operations required to regenerate the root key and can therefore determine if it is likely that an authenticated Galileo I/NAV message is simply a time-delayed reproduction of a previous message.

However, a clock that is accurate to five minutes can also make use of the 'slow MAC' mechanism, whereby the public key of the MAC transmitted 300 seconds previously is retransmitted. If the local clock has an offset exceeding five minutes and the clock is configured to only synchronize with authenticated Galileo E1 messages, the clock will need to be manually adjusted.

Using a suitably configured receiver, OSNMA therefore allows any navigation message to be authenticated not only in terms of its origin from the genuine Galileo constellation but also in terms of its timing. While the delayed nature of key distribution prevents subtle manipulation from being detected quickly, the hardware-level signal monitoring functionality of the clock module combined with Meinberg's various other anti-spoofing functions such as Trusted Source greatly limits the scope of adversaries to falsify timing data in GNSS messages.

13.8.2 Fugro AtomiChron®



While native GNSS NMA solutions such as Galileo OSNMA and the GPS Chimera mechanism (the latter at time of writing being still in development) are essential for the security of civil GNSS reception going forward, they exhibit a number of flaws. In the case of OSNMA, only Galileo E1 OS signals are authenticated; signals on the E5b or E6 bands remain subject to manipulation. In the case of Chimera, the mechanism remains in prolonged development and a timeframe for operational service is not yet in sight. BeiDou and GLONASS offer no known NMA solution for civilian use. For multi-GNSS receivers, these native NMA solutions are therefore somewhat limited in terms of their usefulness as the unprotected signals represent possible attack vectors.

AtomiChron® is a third-party NMA subscription service operated by Dutch geo-data specialists Fugro N.V. that addresses these shortcomings. It is based on authentication data generated by Fugro's numerous reference stations around the world, each of which collates and analyzes GNSS data from all four major satellite constellations (GPS, Galileo, BeiDou, GLONASS). The data from these reference stations is then collated and compared at Fugro's network centers, which in turn transmit their findings (and other operational data) to the Inmarsat satellite constellation to be relayed to a AtomiChron®-capable receiver with a valid subscription.

This makes AtomiChron® the ideal NMA solution for multi-GNSS products such as the LANTIME, as it authenticates GNSS traffic from every signal type on every GNSS band supported by the clock.

The global distribution of these reference stations makes it almost entirely impossible for an adversary to compromise the reference data at its source, as spoofed data from one or two reference stations is easily detected as an outlier.

Naturally, the transmissions to and from the Inmarsat satellites are encrypted and cryptographically signed, such that they can only be decrypted and authenticated by a receiver with a valid AtomiChron® license. This ensures that incoming AtomiChron® data can be uniquely authenticated, and eliminates any risk of the AtomiChron® signal itself being spoofed.

Access to the AtomiChron® service requires a paid-up subscription. If subscribed via an IMS-GXL183 module, this subscription is concluded directly with Meinberg.

13.9 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.

13.9.1 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

and on the website of GNU/Linux
www.linux.org

13.9.2 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

13.9.3 Network Time Protocol Version 4 (NTP)

The NTP project, lead by David L. Mills, can be reached in the internet at www.ntp.org. 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.                                                         *
*                                                                   *
*********************************************************************
```

13.9.4 lighttpd

For our web based configuration tool (HTTP and HTTPS) we use Lighttttpd. 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.

13.9.5 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

13.10 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