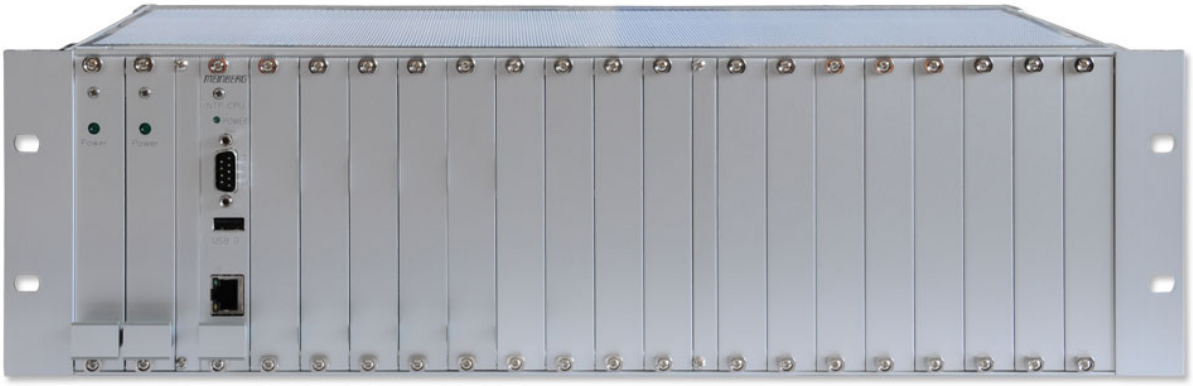
The Synchronization Experts.



HANDBUCH

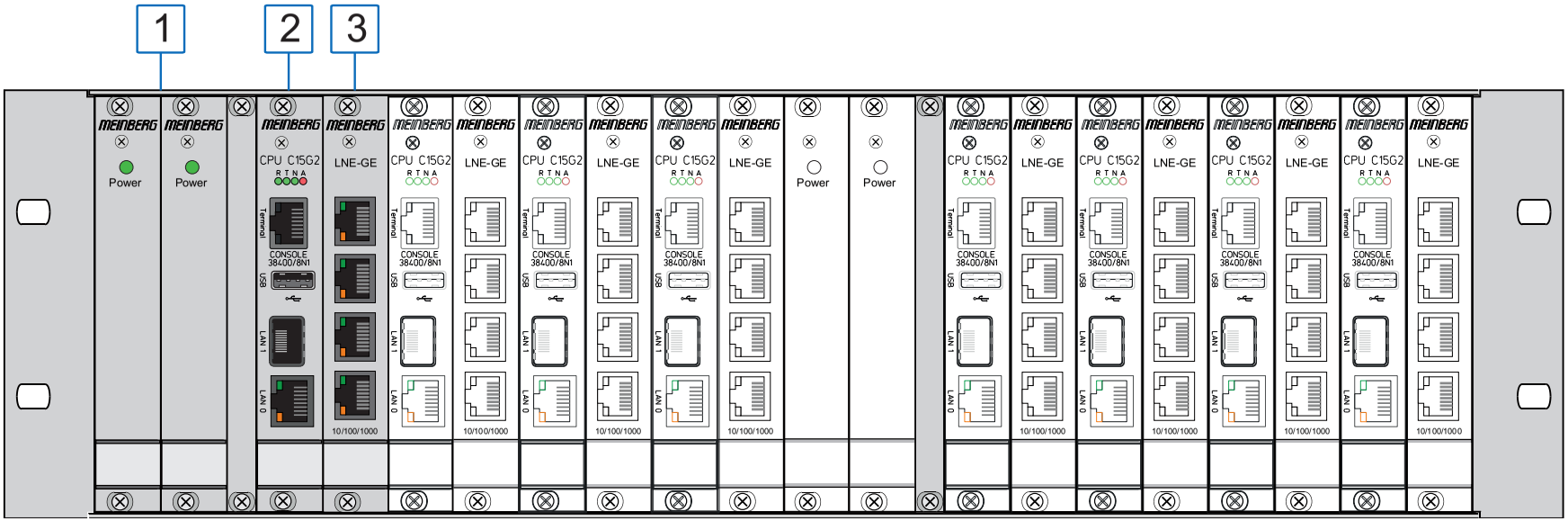
LANTIME CPU Expansion Shelf

LCES/NTP/LNE/RPS/BGT

4. Februar 2022

Meinberg Funkuhren GmbH & Co. KG

Front view (Frontansicht) LANTIME CPU Expansion Shelf



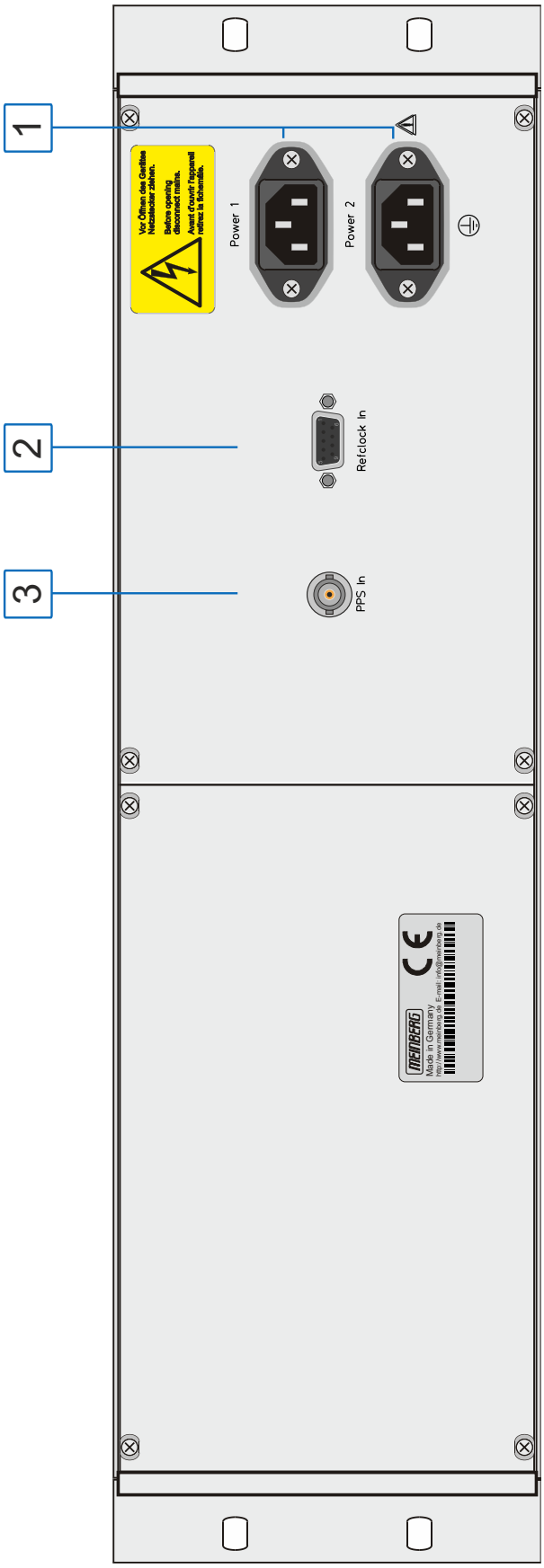
ENGLISH

1. Power supply
2. ***LANCPU***
   - Terminal connector, RJ45 interface (VT100, 38400Baud, 8N1)
   - USB connector
   - Network connectors: LAN 0 - 10/100 Mbit/s, RJ45
     LAN 1 - 1000Base-T, SFP
3. LNE-GE, 4 x network expansion ports 10/100/1000 Mbit/s

DEUTSCH

1. Netzteil
2. ***LANCPU***
   - Terminalanschluss, RS232 Schnittstelle (VT100, 38400 Baud, 8N1)
   - USB Anschluss
   - Netzwerk Anschlüsse: LAN 0 - 10/100 Mbit/s, RJ45
     LAN 1 - 1000Base-T, SFP
3. LNE-GE, 4 x Netzwerk Erweiterung 10/100/1000 Mbit/s

Rear view (Rückansicht) LANTIME CPU Expansion Shelf



ENGLISH

1. Power supply connector
2. Refclock Input, DSUB-9 conncetor
3. PPS Input, BNC female

DEUTSCH

1. Spannungsversorgung
2. Refclock Eingang, DSUB-9 Anschluss
3. PPS Eingang, BNC Buchse

Inhaltsverzeichnis

1 Impressum

Meinberg Funkuhren GmbH & Co. KG
Lange Wand 9, 31812 Bad Pyrmont

Telefon: 0 52 81 / 93 09 - 0
Telefax: 0 52 81 / 93 09 - 230

Internet: https://www.meinberg.de
Email: info@meinberg.de

Datum: 04.02.2022

2 Wichtige Sicherheitshinweise

2.1 Wichtige Sicherheitshinweise und Sicherheitsvorkehrungen

Die folgenden Sicherheitshinweise müssen in allen Betriebs- und Installationsphasen des Gerätes beachtet werden. Die Nichtbeachtung dieser Sicherheitshinweise bzw. besonderer Warnungen oder Betriebsanweisungen in den Handbüchern zum Produkt, verstößt gegen die Sicherheitsstandards, Herstellervorschriften und sachgemäße Benutzung des Gerätes. Meinberg Funkuhren übernimmt keine Verantwortung für Schäden, die durch Nichtbeachtung dieser Richtlinien entstehen.

In Abhängigkeit von Ihrem Gerät oder den installierten Optionen können einige Informationen für Ihr Gerät ungültig sein.

Das Gerät erfüllt die aktuellen Anforderungen der folgenden EU-Richtlinien: EMV-Richtlinie, Niederspannungsrichtlinie, RoHS-Richtlinie und, falls zutreffend, der RED-Richtlinie.

Wenn eine Vorgehensweise mit den folgenden Signalwörtern gekennzeichnet ist, dürfen Sie erst fortfahren, wenn Sie alle Bedingungen verstanden haben und diese erfüllt sind. In der vorliegenden Dokumentation werden die Gefahren und Hinweise wie folgt eingestuft und dargestellt:

GEFAHR!
Das Signalwort bezeichnet eine Gefährdung mit einem hohen Risikograd . Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung zu schweren Verletzungen, unter Umständen mit Todesfolge , führt.

WARNUNG!
Das Signalwort bezeichnet eine Gefährdung mit einem mittleren Risikograd . Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung zu schweren Verletzungen, unter Umständen mit Todesfolge , führen kann.

VORSICHT!
Das Signalwort bezeichnet eine Gefährdung mit einem niedrigen Risikograd . Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung zu leichten Verletzungen führen kann.

ACHTUNG!
Dieser Hinweis macht auf einen Bedienungsablauf, eine Vorgehensweise oder Ähnliches aufmerksam, deren Nichtbefolgung bzw. Nichtausführung möglicherweise einen Schaden am Produkt oder den Verlust wichtiger Daten verursachen kann.

2.2 Verwendete Symbole

In diesem Handbuch werden folgende Symbole und Piktogramme verwendet. Zur Verdeutlichung der Gefahrenquelle werden Piktogramme verwendet, die in allen Gefahrenstufen auftreten können.

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.*

2.3 Produktdokumentation

Umfangreiche Dokumentation zum Produkt wird auf einem USB-Stick bereitgestellt, welcher im Lieferumfang des Systems enthalten ist. Darüber hinaus stehen die Handbücher auf der Meinberg-Webseite https://www.meinberg.de zum Download zu Verfügung: geben Sie dort oben im Suchfeld die entsprechende Systembezeichnung ein. Unser Support-Team hilft Ihnen in dieser Hinsicht auch gerne.

Im Reiter „Doku u. Support“ des Web-Interface werden ebenfalls Bedienungshandbücher für Zeitserver-Administratoren bereitgestellt.

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

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

Nichtbeachtung dieser Anleitung kann zu einer Minderung der Sicherheit dieses Gerätes führen!

Bitte bewahren Sie dieses Handbuch sorgfältig auf.

Dieses Handbuch richtet sich ausschließlich an Elektrofachkräfte oder von einer Elektrofachkraft unterwiesene Personen, welche mit den jeweils gültigen nationalen Normen und Sicherheitsregeln vertraut sind. Einbau, Inbetriebnahme und Bedienung dieses Gerätes dürfen nur von qualifiziertem Fachpersonal durchgeführt werden.

2.4 Sicherheit bei der Installation

WARNUNG!

Inbetriebnahme vorbereiten
Dieses Einbaugerät wurde entsprechend den Anforderungen des Standards IEC 62368-1 (Geräte der Audio-/Video-, Informations- und Kommunikationstechnik - Teil 1: Sicherheitsanforderungen) entwickelt und geprüft.

Bei Verwendung des Einbaugerätes in einem Endgerät (z.B. Gehäuseschrank) sind zusätzliche Anforderungen gem. Standard IEC 62368-1 zu beachten und einzuhalten. Insbesondere sind die allgemeinen Anforderungen und die Sicherheit von elektrischen Einrichtungen (z.B. IEC, VDE, DIN, ANSI) sowie die jeweils gültigen nationalen Normen einzuhalten.

Das Gerät wurde für den Einsatz im Industriebereich sowie im Wohnbereich entwickelt und darf auch nur in solchen Umgebungen betrieben werden. Für Umgebungen mit höherem Verschmutzungsgrad gem. Standard IEC 60664-1 sind zusätzliche Maßnahmen erforderlich, wie z.B. Einbau in einem klimatisierten Schaltschrank.

Transportieren, Auspacken und Aufstellen
Wenn das Gerät aus einer kalten Umgebung in den Betriebsraum gebracht wird, kann Betauung auftreten. Warten Sie, bis das Gerät temperaturangeglichen und absolut trocken ist, bevor Sie es in Betrieb nehmen.

Beachten Sie bei dem Auspacken, Aufstellen und vor Betrieb des Geräts unbedingt die Information zur Hardware-Installation und zu den technischen Daten des Geräts. Dazu gehören z.B. Abmessungen, elektrische Kennwerte, notwendige Umgebungs- und Klimabedingungen usw.

Der Brandschutz muss im eingebauten Zustand sichergestellt sein.

Zur Montage darf das Gehäuse nicht beschädigt werden. Es dürfen keine Löcher in das Gehäuse gebohrt werden.

Aus Sicherheitsgründen sollte das Gerät mit der höchsten Masse in der niedrigsten Position des Racks eingebaut werden. Weitere Geräte sind von unten nach oben zu platzieren.

Das Gerät muss vor mechanischen Beanspruchungen wie Vibrationen oder Schlag geschützt angebracht werden.

Anschließen der Datenkabel

Während eines Gewitters dürfen Datenübertragungsleitungen weder angeschlossen noch gelöst werden (Gefahr durch Blitzschlag).

Bei dem Verkabeln der Geräte müssen die Kabel in der Reihenfolge der Anordnung angeschlossen bzw. gelöst werden, die in der zum Gerät gehörenden Benutzerdokumentation beschrieben ist. Fassen Sie alle Leitungen bei dem Anschließen und Abziehen immer am Stecker an. Ziehen Sie niemals am Kabel selbst. Durch das Ziehen am Kabel kann sich das Kabel vom Stecker lösen oder der Stecker selbst beschädigt werden.

Verlegen Sie die Leitungen so, dass sie keine Gefahrenquelle (Stolpergefahr) bilden und nicht beschädigt (z. B. geknickt) werden.

Anschließen der Stromversorgung

Dieses Gerät wird an einer gefährlichen Spannung betrieben. Nichtbeachtung der Sicherheitshinweise dieses Handbuchs kann zu ernsthaften Personen- und Sachschäden führen.

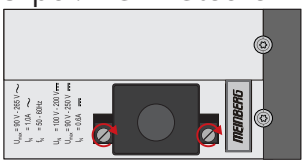
Vor dem Anschluss an die Spannungsversorgung muss ein Erdungskabel an den Erdungsanschluss des Gerätes angeschlossen werden.

Die Stromversorgung sollte mit einer kurzen, induktivitätsarmen Leitung angeschlossen werden.

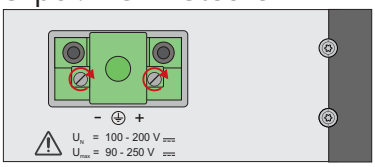
Überprüfen Sie vor dem Betrieb, ob alle Kabel und Leitungen einwandfrei und unbeschädigt sind. Achten Sie insbesondere darauf, dass die Kabel keine Knickstellen aufweisen, um Ecken herum nicht zu kurz gelegt worden sind und dass keine Gegenstände auf den Kabeln stehen.

Achten Sie ebenfalls darauf, dass alle Steckverbindungen fest sitzen und stellen Sie bei Einsatz der Steckverbinder 3- pol. MSTB und 5-pol. MSTB sicher, dass die Sicherungsschrauben (Schlitzschrauben) fest angezogen sind (siehe Abbildung, Bsp. LANTIME M300 Netzteil).

5-pol. MSTB-Stecker



3-pol. MSTB-Stecker



Eine fehlerhafte Schirmung oder Verkabelung bzw. nicht fachgerecht hergestellte Steckverbindungen gefährden Ihre Gesundheit und Sicherheit (schwere Verletzungen durch elektrischer Schlag, unter Umständen mit Todesfolge) und können Ihr Meinberg-Gerät bzw. andere Geräte zerstören und stellen möglicherweise eine Brandgefahr dar.

Stellen Sie sicher, dass alle erforderlichen Sicherheitsvorkehrungen getroffen werden. Stellen Sie alle Kabelverbindungen zum Gerät im stromlosen Zustand her, ehe Sie den Strom einschalten. Beachten Sie die am Gerät angebrachten Sicherheitshinweise (siehe Sicherheitssymbole).

Das Metallgehäuse des Gerätes ist geerdet. Es muss sichergestellt werden, dass bei der Montage im Schaltschrank keine Luft- und Kriechstrecken zu benachbarten Spannung führenden Teilen unterschritten werden oder Kurzschlüsse verursacht werden.

Im Störfall oder bei Servicebedarf (z.B. bei beschädigten Gehäuse oder Netzkabel oder bei dem Eindringen von Flüssigkeiten oder Fremdkörpern), kann der Stromfluss unterbrochen werden.

Fragen zur Hausinstallation klären Sie bitte mit Ihrer Hausverwaltung.

AC Stromversorgung	DC Stromversorgung
• Das Gerät ist ein Gerät der Schutzklasse 1 und darf nur an eine geerdete Steckdose angeschlossen werden (TN-System). • Zum sicheren Betrieb muss das Gerät durch eine Installationssicherung von max. 16 A abgesichert und mit einem Fehlerstromschutzschalter, gemäß den jeweils gültigen nationalen Normen, ausgestattet sein. • Die Trennung des Gerätes vom Netz muss immer an der Steckdose und nicht am Gerät erfolgen. • Geräte mit Netzstecker werden mit einer sicherheitsgeprüften Netzleitung des Einsatzlandes ausgerüstet und dürfen nur an eine vorschriftsmäßig geerdete Schutzkontakt-Steckdose angeschlossen werden, andernfalls droht elektrischer Schlag. • Stellen Sie sicher, dass die Steckdose am Gerät oder die Schutzkontakt-Steckdose der Hausinstallation dem Benutzer frei zugänglich ist, damit in Notfall das Netzkabel aus der Steckdose gezogen werden kann.	• Das Gerät muss nach den Bestimmungen der IEC 62368-1 außerhalb der Baugruppe spannungslos schaltbar sein (z.B. durch den primärseitigen Leitungsschutz). • Montage und Demontage des Steckers zur Spannungsversorgung ist nur bei spannungslos geschalteter Baugruppe erlaubt (z.B. durch den primärseitigen Leitungsschutz). • Die Zuleitungen sind ausreichend abzusichern und zu dimensionieren. *Anschlussquerschnitt:* *1 mm² – 2,5 mm²* *17 AWG – 13 AWG* • Versorgung des Gerätes muss über eine geeignete Trennvorrichtung (Schalter) erfolgen. Die Trennvorrichtung muss gut zugänglich in der Nähe des Gerätes angebracht werden und als Trennvorrichtung für das Gerät gekennzeichnet sein.

2.5 Schutzleiter-/ Erdungsanschluss

ACHTUNG!

Um einen sicheren Betrieb zu gewährleisten und um die Anforderungen der IEC 62368-1 zu erfüllen, muss das Gerät über die Schutzleiteranschlussklemme korrekt mit dem Schutzerdungsleiter verbunden werden.

Ist ein externer Erdungsanschluss am Gehäuse vorgesehen, muss dieser mit der Potentialausgleichsschiene (Erdungsschiene) verbunden werden. Die Montageteile sind nicht im Lieferumfang enthalten.

Hinweis:
Bitte verwenden Sie ein Erdungskabel mit Querschnitt $\geq$ 1.5 mm^2
Achten Sie immer auf eine korrekte Crimpverbindung!

2.6 Sicherheit im laufenden Betrieb

WARNUNG!

Vermeidung von Kurzschlüssen
Achten Sie darauf, dass keine Gegenstände oder Flüssigkeiten in das Innere des Geräts gelangen. Elektrischer Schlag oder Kurzschluss könnte die Folge sein.

Lüftungsschlitze
Achten Sie darauf, dass die Lüftungsschlitze nicht zugestellt werden bzw. verstauben, da sonst Überhitzungsgefahr aufgrund eines Wärmestaus im Gerät während des Betriebes bestehen könnte. Störungen im Betrieb und Produktschäden können die Folge sein.

Bestimmungsgemäßer Betrieb
Der Bestimmungsgemäße Betrieb und die Einhaltung der EMV-Grenzwerte (Elektromagnetische Verträglichkeit) sind nur bei ordnungsgemäß montiertem Gehäusedeckel gewährleistet (Kühlung, Brandschutz, Abschirmung gegenüber elektrischen, magnetischen und elektromagnetischen Feldern).

Ausschalten im Stör-/Service-Fall
Durch Ausschalten allein werden Geräte nicht von der Stromversorgung getrennt. Im Stör- oder Servicefall müssen die Geräte jedoch sofort von allen Stromversorgungen getrennt werden.

Gehen Sie dabei folgendermaßen vor:
- Schalten Sie das Gerät aus.
- Ziehen Sie alle Stromversorgungsstecker.
- Verständigen Sie den Service.
- Geräte, die über eine oder mehrere Unterbrechungsfreie Stromversorgungen (USVen) angeschlossen sind, bleiben auch dann in Betrieb, wenn der Netzstecker der USV/USVen gezogen ist. Deshalb müssen Sie die USVen nach Vorgabe der zugehörigen Benutzerdokumentation außer Betrieb setzen.

2.7 Sicherheit bei der Wartung

WARNUNG!

Das Gerät darf nicht geöffnet werden. Reparaturen am Gerät dürfen nur durch den Hersteller oder durch autorisiertes Personal durchgeführt werden. Durch unsachgemäße Reparaturen können erhebliche Gefahren für den Benutzer entstehen (elektrischer Schlag, Brandgefahr).

Durch unerlaubtes Öffnen des Gerätes oder einzelner Geräteteile können ebenfalls erhebliche Gefahren für den Benutzer entstehen. Außerdem hat dies den Garantieverlust sowie den Haftungsausschluss zur Folge.

Gefahr durch bewegliche Teile: halten Sie sich von beweglichen Teilen fern.

Geräteteile können während des Betriebs sehr warm werden. Berühren Sie nicht diese Oberflächen! Schalten Sie, wenn erforderlich, vor dem Ein- oder Ausbau von Geräteteilen das Gerät aus und lassen Sie es abkühlen.

2.8 Umgang mit Batterien

WARNUNG!

Die Lithiumbatterie auf den Empfängermodulen hat eine Lebensdauer von mindestens 10 Jahren. Sollte ein Austausch erforderlich werden, sind folgende Hinweise zu beachten:

Unsachgemäße Handhabung der Batterie kann zu einer Explosion oder zu einem Austritt von entflammbaren Flüssigkeiten oder Gasen führen.

- Die Batterie darf nicht kurzgeschlossen oder wiederaufgeladen werden.
- Die Batterie nicht ins Feuer werfen.
- Die Batterie darf nur dem vom Batteriehersteller angegebenen Luftdruck ausgesetzt werden.
- Die Batterie darf nur mit demselben oder einem vom Hersteller empfohlenen gleichwertigen Typ ersetzt werden. Ein Austausch der Lithiumbatterie darf nur vom Hersteller oder autorisiertem Fachpersonal vorgenommen werden.
- Die Batterie darf nicht mechanisch zerkleinert oder in einem offenen Feuer oder im Ofen entsorgt werden.
- Bei der Entsorgung gebrauchter Batterien sind die örtlichen Bestimmungen über die Beseitigung von Sondermüll zu beachten.

ACHTUNG!

Die Batterie versorgt u.a. den RAM sowie die Real-Time-Clock (RTC) der Referenzuhr.

Unterschreitet die Batteriespannung den Wert von 3 V DC, empfiehlt Meinberg den Austausch der Batterie. Bei einer Unterschreitung der Batteriespannung könnte möglicherweise folgendes Verhalten der Referenzuhr auftreten:

- Die Referenzuhr hat nach dem Einschalten ein falsches Datum bzw. eine falsche Zeit
- Die Referenzuhr startet immer wieder im Cold-Boot-Modus
- Teilverlust der auf der Referenzuhr getätigten Konfigurationen

2.9 Reinigen und Pflegen

ACHTUNG!

Auf keinen Fall das Gerät nass reinigen! Durch eindringendes Wasser können erheblichen Gefahren für den Anwender entstehen (z.B. Stromschlag).

Flüssigkeit kann die Elektronik des Gerätes zerstören! Flüssigkeit dringt in das Gehäuse des Gerätes ein und kann einen Kurzschluss der Elektronik verursachen.

Reinigen Sie das Gerät ausschließlich mit einem weichen, trockenen Tuch. Verwenden Sie auf keinen Fall Löse- oder Reinigungsmittel.

2.10 Vorbeugung von ESD-Schäden

ACHTUNG!

Die Bezeichnung EGB (Elektrostatisch gefährdete Bauteile) entspricht der englischsprachigen Bezeichnung „ESDS Device“ (Electrostatic Discharge-Sensitive Device) und bezieht sich auf Maßnahmen, die dazu dienen, elektrostatisch gefährdete Bauelemente vor elektrostatischer Entladung zu schützen und somit vor einer Schädigung oder gar Zerstörung zu bewahren. Systeme und Baugruppen mit elektrostatisch gefährdeten Bauelementen tragen in der Regel folgendes Kennzeichen:

Kennzeichen für Baugruppen mit elektrostatisch gefährdeten Bauelementen

Folgende Maßnahmen schützen elektrostatisch gefährdete Bauelemente vor der Schädigung:

Aus- und Einbau von Baugruppen vorbereiten
Entladen Sie sich (z.B. durch Berühren eines geerdeten Gegenstandes), bevor Sie Baugruppen anfassen.

Für sicheren Schutz sorgen Sie, wenn Sie bei der Arbeit mit solchen Baugruppen ein Erdungsband am Handgelenk tragen, welches Sie an einem unlackierten, nicht stromführenden Metallteil des Systems befestigen.

Verwenden Sie nur Werkzeug und Geräte, die frei von statischer Aufladung sind.

Baugruppen transportieren
Fassen Sie Baugruppen nur am Rand an. Berühren Sie keine Anschlussstifte oder Leiterbahnen auf Baugruppen.

Baugruppen aus- und einbauen
Berühren Sie während des Aus- und Einbauens von Baugruppen keine Personen, die nicht ebenfalls geerdet sind. Hierdurch ginge Ihre eigene, vor elektrostatischer Entladung schützende Erdung verloren und damit auch der Schutz des Gerätes vor solchen Entladungen.

Baugruppen lagern
Bewahren Sie Baugruppen stets in EGB-Schutzhüllen auf. Diese EGB-Schutzhüllen müssen unbeschädigt sein. EGB-Schutzhüllen, die extrem faltig sind oder sogar Löcher aufweisen, schützen nicht mehr vor elektrostatischer Entladung.

EGB-Schutzhüllen dürfen nicht niederohmig und metallisch leitend sein, wenn auf der Baugruppe eine Lithium-Batterie verbaut ist.

2.11 Rückgabe von Elektro- und Elektronik-Altgeräten

ACHTUNG!

WEEE-Richtlinie über Elektro und Elektronik-Altgeräte 2012/19/EU
(WEEE: Waste Electrical and Electronic Equipment)

Getrennte Sammlung
Produktkategorie: Gemäß den in der WEEE-Richtlinie, Anhang I, aufgeführten Gerätetypen ist dieses Produkt als „IT- und Kommunikationsgeräte“ klassifiziert.

Dieses Produkt genügt den Kennzeichnungsanforderungen der WEEE-Richtlinie. Das Produkt-symbol links weist darauf hin, dass Sie dieses Elektronikprodukt, nicht im Hausmüll entsorgen dürfen.

Rückgabe- und Sammelsysteme
Für die Rückgabe Ihres Altgerätes nutzen Sie bitte die Ihnen zur Verfügung stehenden länderspezifischen Rückgabe- und Sammelsysteme oder setzen Sie sich mit Meinberg Funkuhren in Verbindung.

Bei Altgeräten, die aufgrund einer Verunreinigung während des Gebrauchs ein Risiko für die menschliche Gesundheit oder Sicherheit darstellen, kann die Rücknahme abgelehnt werden.

Rückgabe von Batterien
Batterien, die mit dem obengezeigten WEEE-Mülltonnen-Symbol gekennzeichnet sind, dürfen gemäß EU-Batterien-Richtlinie nicht zusammen mit dem Hausmüll entsorgt werden:

3 Vor dem Start

3.1 Text- und Syntaxkonventionen

In diesem Kapitel werden kurz die Text und Syntaxkonventionen beschrieben, die in diesem Handbuch Anwendung finden.

Web Interface: Beispiel Menü „Netzwerk“
Untermenü „Network → Network Interfaces“
Register im Submenü „Network → Network Interfaces → IPv4“

Die Menüführung wird logisch getrennt durch den Pfeil nach Rechts ()→.

Verzeichnisnamen / Pfade Beispiel Lantime Konfigurationsdatei
Die Verzeichnisnamen und Pfade werden kursiv dargestellt.

Code und Kommandozeilenbefehle

```
- cmd/www-upload.htm

#Programmcode und Kommandozeilenbefehle werden in einer grauen Box mit
Monospace-Schrift angezeigt.
```

Benutzer-Passwörter:
Für Benutzerpasswörter und das Shared Secret sind derzeit folgende Zeichen erlaubt:

Erlaubter Zeichensatz für beide:

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

3.2 Empfohlene Werkzeuge

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

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

Abbildung: benötigte Werkzeuge (von rechts nach links): INBUS 2,5mm, Kreuzschraubendreher PH1 x 80, Schlitzschraubendreher, TORX T20, TORX T8

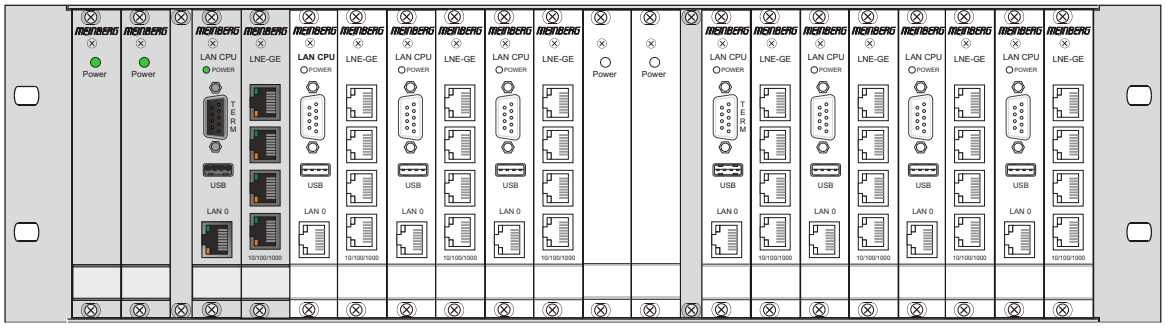
3.3 Liste der verwendeten Abkürzungen

AFNOR	Association Francaise de Normalisation time codes
AC	Wechselstrom
ASCII	American Standard Code for Information Interchange
BMC	Best Master Clock
BMCA	Best Master Clock Algorithmus
BNC	Bayonet Neil Councilman Connector
Bps	Bytes per second
bps	Bits per second
CAT5	Standard Netzwek-Kabel
CET	Central European Time
CLI	Command Line Interface
DB9	Steckverbinder vom Typ D-Subminiatur
DARS	Digital Audio Reference Signal
DC	Gleichstrom
DCF77	Ist ein langwelliges Zeitsignal. DCF77 steht für D=Deutschland (Deutschland), C=Langwellensignal, F=Frankfurt, 77=Frequenz: 77,5 kHz.
DCFMARK	Einzelimpuls mit programmierbarem Datum und Uhrzeit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSCP	Differentiated Services Code Points
DST	Daylight Saving Time
E1	Europäisches digitales Übertragungssignal bei 2,048 MHz, das in Telekommunikationsnetzen verwendet wird.
E2E	End-to-end
ETH	Ethernet
FTP	File Transfer Protocol
FW	Firmware
GE / GbE	Gigabit Ethernet
GLONASS	GLObal NAvigation Satellite System von den russischen Luftfahrt-Verteidigungskräften
GM	Grandmaster
GND	Ground (Connector)
GNSS	Global Navigation Satellite System (GPS, GLONASS, Galileo, Beidou)
GOAL	GPS Optical Antenna Link
GPS	Global Positioning System (USA)
GPIO	General Purpose Input Output
GSM	Global System for Mobile Communications
HMI	Human-Machine Interface
HP	Horizontale Pitch - ist eine Einheit, die die horizontale Breite von elektronischen Geräten im Rack misst.
HPS	High Performance Synchronization PTP/NTP/SyncE GBit Modul
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	Protokoll zur hochpräzisen Synchronisation im Nanosekundenbereich (PTP)
IP	Internet Protocol
IP 20	Schutzklasse 20
IRIG	Inter-range instrumentation group time codes
LCD	Liquid Crystal Display
LDAP(S)	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
LINUX	Unix-ähnliches Mehrbenutzer-Computer-Betriebssystem
LIU	Line Interface Unit- ein Modul zur Erzeugung von E1/T1-Signalen MBit/s (framed) und Clock (unframed)
LNE	Local Network Extention, zusätzliche Ethernet-Ports
MAC	Media Access Control
MD5	Message-Digest kryptographische Hash-Funktion
MESZ	Mitteleuropäische Sommerzeit
MEZ	Mitteleuropäische Zeit
MIB	Management Information Base
MRS	Multi Reference Source
MSF	Zeitzeichensender in Anthorn, UK
NIST	National Institute of Standards and Technology
NMEA	Communication standard from National Marine Electronics Association
NTP	Network Time Protocol
NTPD	NTP Deamon
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 3 kHz to 300 GHz
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
RS-232	Serial port level
RS-485	Serial port level

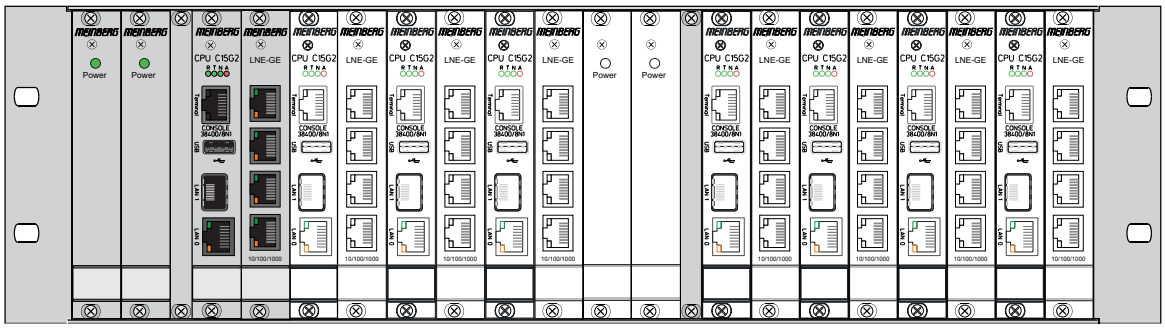
RSC	Redundant Switch Control unit
RX	Receiving Data
SBC	Single Board Computer
SDU	Signal Distribution Unit
SHA-1	Secure Hash Algorithm 1
SMB	Subminiature coaxial connector
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SMTP	Simple Mail Transfer Protocol
SPS	Standard Positioning 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
T1	North American telecommunication signal at 1.544 MHz frequency
TACACS	Terminal Access Controller Access Control System
TAI	Temps Atomique International
TC	Time Code
TCA	Time Code Amplified
TCG	Time Code Generator
TCR	Time Code Receiver for IRIG A/B, AFNOR or IEEE1344 codes
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)

4 Komplettsystem LCES-NTP

Das System LCES-NTP besteht aus bis zu acht physikalisch getrennten LAN-CPUs, LNE-Netzwerkerweiterungsmodule und, je nach Konfiguration, zwei oder vier Netzteilen (siehe technische Daten). Das Komplettsystem ist betriebsbereit in einem Baugruppenträger montiert. Die Schnittstellen sowie die Ein-/Ausgangssignale der Baugruppe sind an der Front- und Rückwand des Systems herausgeführt.



LCES im Baugruppenträger mit LAN-CPU C05F1 - Geode™ LX800



LCES im Baugruppenträger mit LAN-CPU C15G2 - Intel® Atom™ Processor E Series

5 Technische Daten 3HE-Gehäuse

Gehäusetyp BGT - Baugruppenträger, 19"/3HE

Gehäusematerial Aluminium

Temperaturbereich

Betrieb 0 ... 50 °C (32 ... 122 °F)

Lagerung -20 ... 70 °C (-4 ... 158 °F)

Relative Luftfeuchtigkeit

Betrieb 85 % max. (nicht kondensierend)

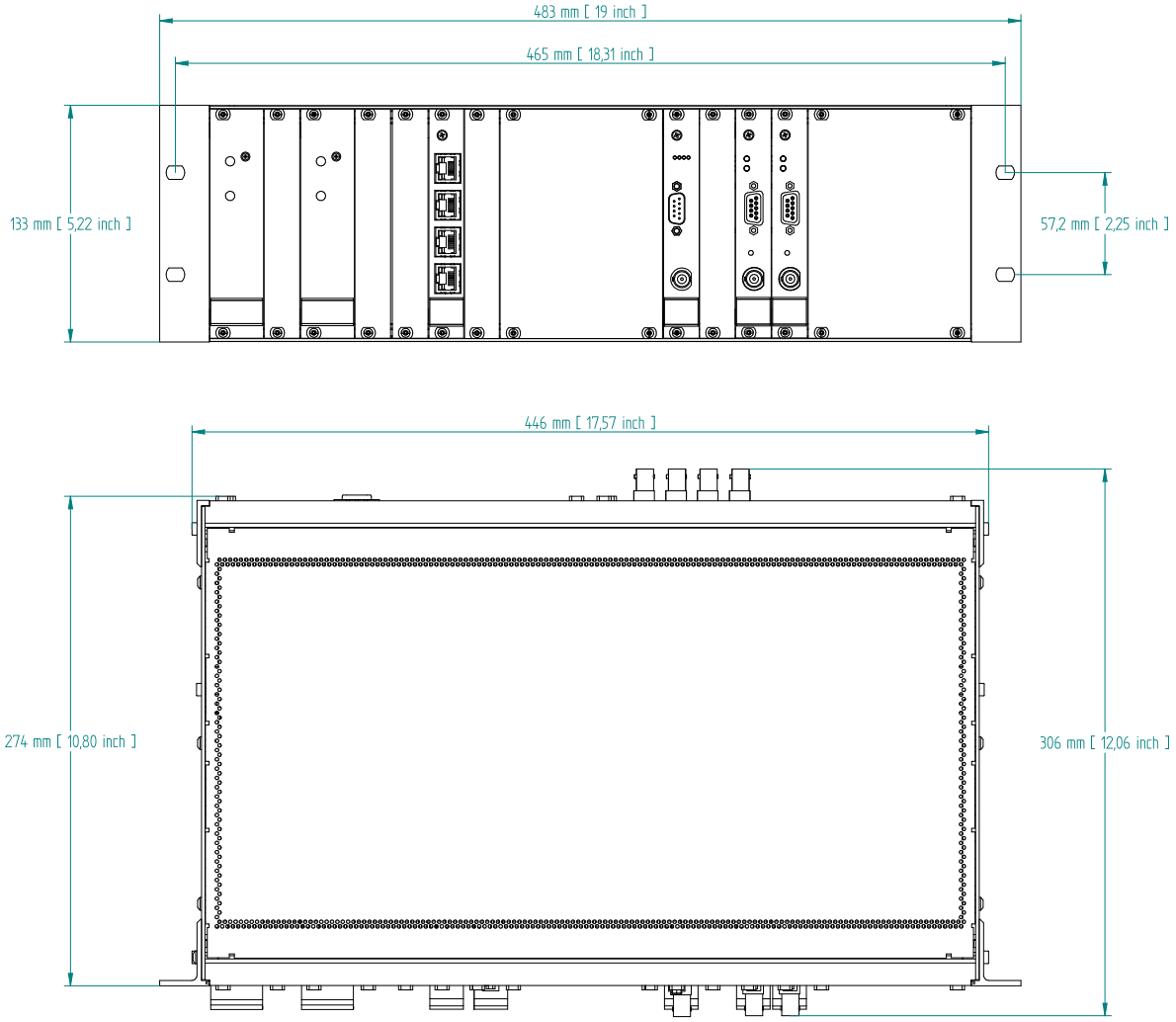
Betriebshöhe

Betrieb 2000 m / 6562 ft (Über Seehöhe)

Akustik 0 dB (A)

IP Schutzklasse IP20

Gehäuseabmessungen



6 Network Time Protocol (NTP)

NTP ist ein Verfahren zur Synchronisation von Rechneruhren in lokalen und globalen Netzwerken. Das Grundprinzip, Version 1 [Mills88], wurde bereits 1988 als RFC (Request For Comments) veröffentlicht. Erfahrungen aus der praktischen Anwendung im Internet wurden in Version 2 [Mills89] eingebracht. Das Programmpaket NTP ist eine Implementierung der aktuellen Version 4 [Mills90], basierend auf der Spezifikation RFC-1305 von 1990 (im Verzeichnis doc/NOTES). Das Paket ist frei kopierbar und unterliegt den Copyright Bedingungen.

Die Arbeitsweise von NTP unterscheidet sich grundsätzlich von den meisten anderen Protokollen. NTP synchronisiert nicht einfach alle beliebigen Uhren untereinander, sondern bildet eine Hierarchie von Zeitservern und Clients. Eine Hierarchieebene wird als stratum bezeichnet, wobei Stratum-1 die höchste Ebene darstellt (das LANTIME ist ein Stratum-1-Server). Zeitserver dieser Ebene synchronisieren sich auf eine Referenzzeitquelle, das können z.B. Funkuhren, Satelliten-Empfänger oder Modem-Zeitdienste sein. Stratum-1-Server stellen ihre Zeit mehreren Clients im Netz zur Verfügung, die als Stratum-2 bezeichnet werden.

Ausgehend von einer oder mehreren Referenzzeiten kann durch NTP eine hohe Synchronisationsgenauigkeit realisiert werden. Jeder Rechner synchronisiert sich mit bis zu 3 gewichteten Zeitquellen, wobei ausgefeilte Mechanismen den Abgleich der Systemzeit mit anderen Rechnern im Netz sowie ein Nachregeln der eigenen Systemuhr ermöglichen. Abhängig von der Jitter-Charakteristik der Zeitquellen und der Lokalisierung des einzelnen Rechners im Netzwerk wird eine Zeitgenauigkeit von 128 ms, häufig besser als 1 ms, erreicht.

6.1 NTP Clients

Das Programmpaket NTP wurde auf verschiedenen UNIX Systemen getestet (siehe Liste). Bei vielen UNIX Installationen ist bereits ein NTP Client vorinstalliert. Es müssen nur die Konfigurationsdateien (/etc/ntp.conf - siehe NTP Client Installation) angepasst werden. Auch für die meisten anderen Betriebssysteme wie Windows 7/Vista/XP/NT/2000/98/95/3x, OS2 oder MAC existieren NTP Clients als Freeware oder Shareware.

Als Bezugsquelle für die neuesten Versionen wird die NTP Homepage empfohlen:
http://www.ntp.org

Auf unserer Homepage können aktuelle Informationen zur Installation und Funktion von NTP gefunden werden:
https://www.meinberg.de/german/sw/ntp.htm

7 Benutzerhandbuch Sicherheit

Dieses Kapitel beschreibt die Konfiguration eines Betriebssystems der LANTIME-Serie (LTOS) in Bezug auf die Sicherheitsfunktionen. Es gliedert sich in die folgenden Abschnitte: allgemeiner Überblick, Sicherung des Managements, Sicherung des Zeitservice und zusätzliche Informationen zur Ausgabe von Ereignisprotokollen. Abschließend werden einige Hinweise für den Aktualisierungsprozess eines LANTIME gegeben.

Es werden allgemeinen Kenntnisse über Public-Key-Infrastrukturen, RSA, symmetrische Schlüssel und die Protokolle SSL, SSH, NTP und SNMP vorausgesetzt.

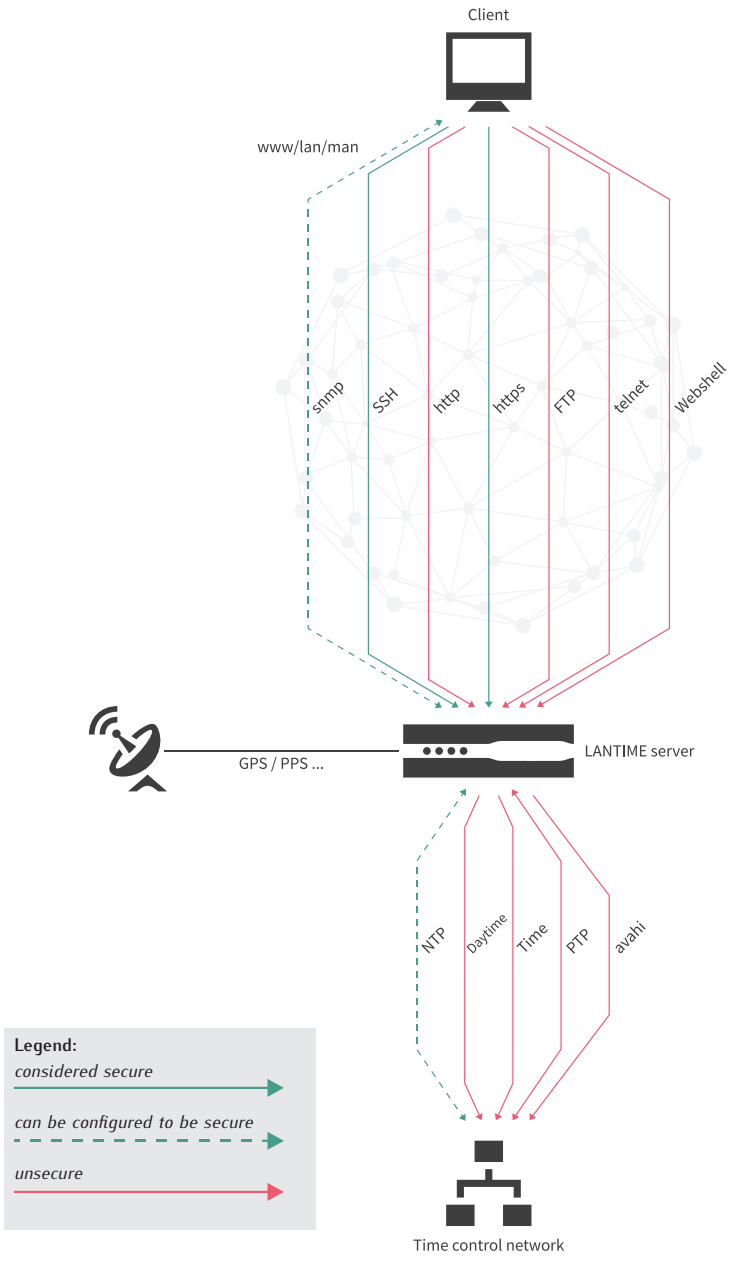


Abbildung 7.1: LANTIME Services

7.1 Allgemeine Informationen

Bevor Sie mit der Konfiguration beginnen, werfen Sie einen Blick auf Abbildung 7.1, um die Dienste zu identifizieren, die eine Absicherung zulassen.

Generell ist eine sichere Verwaltung des LANTIME mit SSH, HTTPS und SNMP möglich. Wenn die Konfiguration über SNMP gewünscht wird, ist die Verwendung der Version 3 die einzige Möglichkeit, eine sichere Verbindung zur Verwaltung des Systems herzustellen. Es ist eine gute Vorgehensweise, alle nicht genutzten Dienste zu deaktivieren, um die Angriffsfläche zu minimieren. Wenn möglich, aktivieren Sie also nur einen der Dienste (SNMP hat nicht die volle Konfigurationsunterstützung, aber Sie können die anderen Dienste über SNMP aktivieren)!

Die Bereitstellung von gesicherten Zeitinformationen ist nur für NTP verfügbar. Bitte beachten Sie, dass das NTP-Protokoll nur Integrität und Authentizität, aber keine Vertraulichkeit unterstützt. PTP unterstützt derzeit keine IT-Sicherheitsfunktionen. Diese sind erst für den nächsten Protokollstandard vorgesehen. Aus diesem Grund müssen Sie noch auf NTP zurückgreifen, um eine sichere Zeitsynchronisation zu gewährleisten.

Ein weiterer wichtiger Hinweis ist die Verwendung der neuesten Browser und Service-Clients, um die Auswahl der besten Sicherheitsalgorithmen für die Server- und Client-Kommunikation zu unterstützen. Durch die zeitnahe Installation von Updates können zudem bekannte Schwachstellen geschlossen und das Risiko eines erfolgreichen Angriffs minimiert werden.

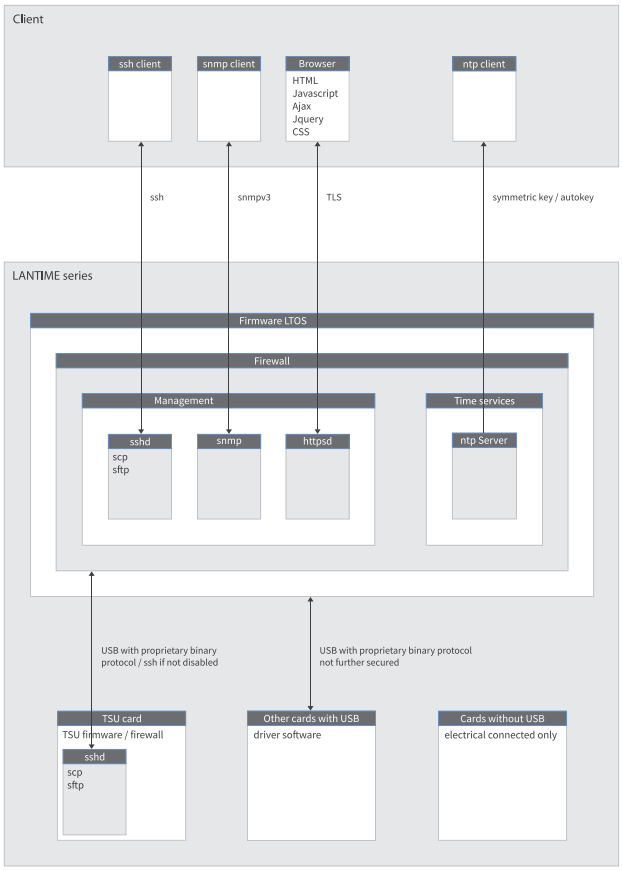


Abbildung 7.2: Die sicheren Protokolle im Detail

Die TSU-Karten von Meinberg bieten in der aktuellen Firmware-Version LTOS V7 nicht mehr die Möglichkeit, netzwerkseitig eine SSH-Verbindung aufzubauen. Der Zugriff ist nur über das CPU-Modul des LANTIME erlaubt. Es besteht weiterhin die Möglichkeit den SSH-Dienst einer TSU-Karte, wie in Figure 7.3 dargestellt, komplett zu deaktivieren.

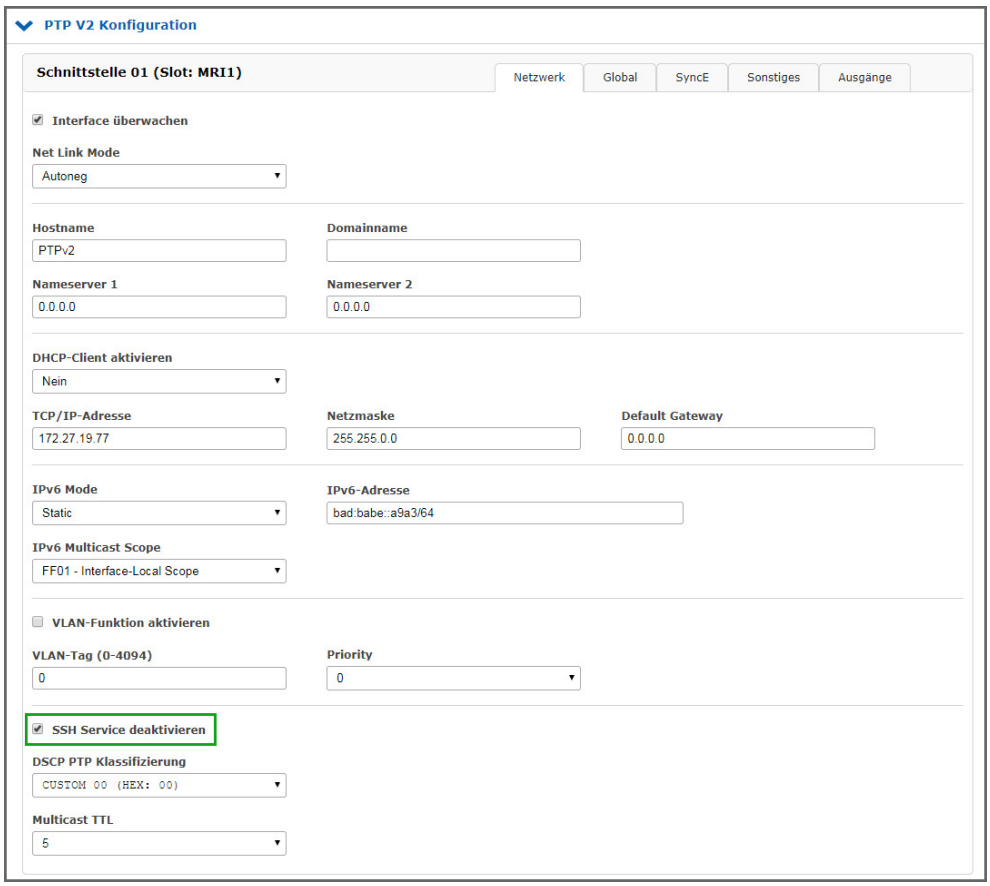


Abbildung 7.3: SSH auf TSU deaktivieren

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

Tabelle: Übersicht der Sicherheitsziele

Diese Tabelle zeigt die Sicherheitsziele der Protokolle in der Übersicht. Die Verantwortlichkeit wird durch ein detailliertes Syslog der von jedem Benutzer oder Prozess ausgeführten Aktionen gewährleistet. Die Log-Dateien können jedoch durch root- bzw. super-User nachträglich verändert werden. Aus diesem Grund kann die Nichtabstreitbarkeit durch das System nicht gewährleistet werden. Die größtmögliche Verfügbarkeit der Dienste wird durch aktuelle Updates und IP-Blocking erreicht. Für mehr Schutz implementieren Sie Web Application Firewalls und herkömmliche Firewalls im Netzwerk, die in der Lage sind, DOS/DDOS-Angriffe zu erkennen und zu verhindern.

Bei allen Änderungen an der Konfiguration ist zu beachten, dass sie nach einem Neustart verloren gehen oder von anderen Admins oder Superusern verworfen werden können, wenn sie nicht in der Startkonfiguration gespeichert sind.

7.2 Sicherstellung des Managements

Der sicherste Weg, einen LANTIME zu konfigurieren, besteht darin, den Client direkt mit dem LANTIME zu verbinden, bis nur noch sichere Kanäle eingerichtet sind. Dieses Handbuch verwendet als Beispiel das Web-Interface über ssl.

Nach dem Anschluss einer Referenzuhr und der folgenden Startprozedur eines LANTIME kann über das Frontpanel eine IP-Adresse konfiguriert werden (siehe Kapitel „LTOS Management und Überwachung → Konfiguration über das Webinterface → Netzwerk“). Jetzt ist es möglich, sich mit der konfigurierten IP-Adresse mit dem Webinterface zu verbinden. Verwenden Sie die Default-Anmeldeinformationen für die initiale Anmeldung:

Benutzer: *root*
Passwort: *timeserver*

Nach erfolgreicher Verbindung ist zunächst zu prüfen, ob eine neue Firmware-Version vorhanden ist (Update-Anweisungen siehe Kapitel Software-/Firmwareupdate). Nachdem das Update durchgeführt wurde, erzeugen oder injizieren Sie ein SSL-Zertifikat. In diesem Beispiel wird ein neues Zertifikat verwendet. Abbildung 7.4 zeigt die Schaltfläche zum Starten der Zertifikats-Generierung.

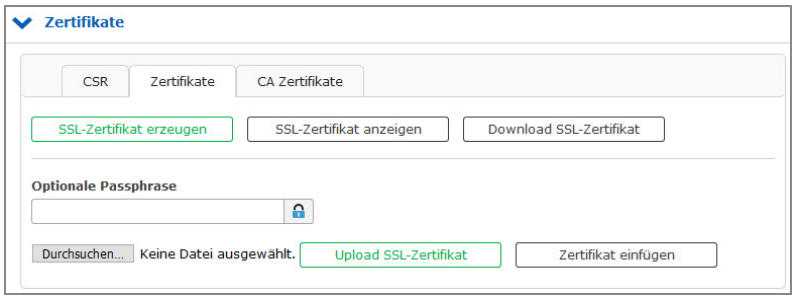


Abbildung 7.4: SSL-Zertifikat generieren - Schritt 1

Im nächsten Schritt müssen Sie die für das Zertifikat erforderlichen Informationen eingeben (siehe auch Kapitel „LTOS Management und Monitoring → Über das Webinterface → Sicherheit → Zertifikate“). Abbildung 7.5 zeigt das Formular. Verwenden Sie als Schlüssellänge 2048 oder höher. Kürzere Laufzeiten der Gültigkeitsdauer sind besser als längere. In diesem Beispiel wählen wir drei Jahre als einen guten Wert von kurzer Dauer und akzeptablen Managementkosten.

Abbildung 7.5: SSL-Zertifikat generieren Schritt 2

Abbildung 7.6: |Generiertes SSL-Zertifikat anzeigen

Sie können das generierte Zertifikat mit der Schaltfläche „SSL-Zertifikat anzeigen“ ausgeben. Benutzen Sie die Schaltfläche, um es mit dem Zertifikat zu vergleichen, das der Browser bei Ihrer nächsten HTTPS-Verbindung zum LANTIME bereitstellt. Beide sollten identisch sein! Der Importprozess ist in Bild 7.7 dargestellt. Die Zahlen in der Abbildung beschreiben die Reihenfolge der auszuführenden Aktionen. Die vierte Zahl stellt den Vergleich mit dem zuvor heruntergeladenen Zertifikat des LANTIME dar. Wenn beide Zertifikate identisch sind, können Sie mit Schritt 5 fortfahren, um die Vertrauennswürdigkeit des LANTIME-Zertifikats zu bestätigen. Moderne Browserkonfigurationen zeigen Ihnen, dass die Verbindung nicht sicher ist, wenn Sie ein selbstsigniertes Zertifikat verwenden. Aufgrund dieses Verhaltens empfehlen wir die Implementierung einer Public-Key-Infrastruktur, um die Warnung zu vermeiden. Achten Sie zudem auf die Nutzung eines Subject Alternative Name (SAN), da moderne Browser auch hierauf prüfen. Zu diesem Zweck können Sie eine Zertifikatsanforderung erzeugen, herunterladen, signieren und das signierte Zertifikat über das Web-Frontend in Bild 7.4 wieder hochladen.

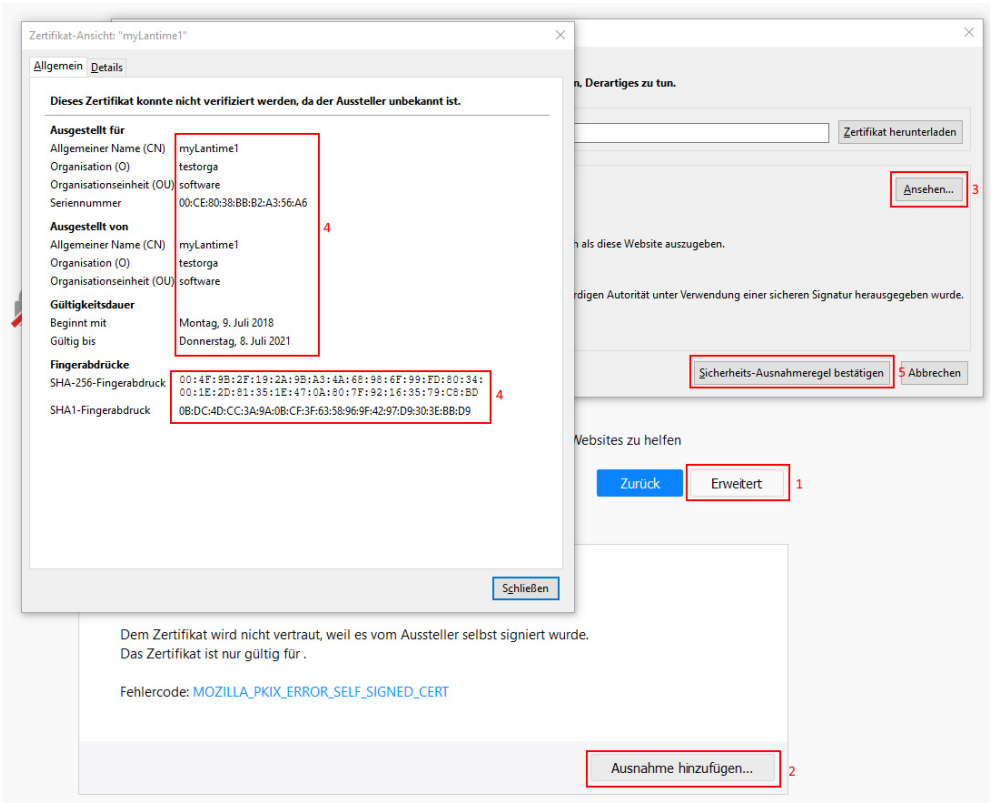


Abbildung 7.7: Importvorgang des neuen SSL-Zertifikats im Browser

Wenn die Verbindung über HTTPS möglich ist, können Sie alle anderen ungenutzten Dienste, wie in Bild 7.8 angezeigt wird, deaktivieren. Zusätzlich stellt in diesem Beispiel nur eine Netzwerkschnittstelle die HTTPS-Webschnittstelle zur Verfügung. Somit sind auch Szenarien wie ein dediziertes Konfigurationsnetzwerk möglich.

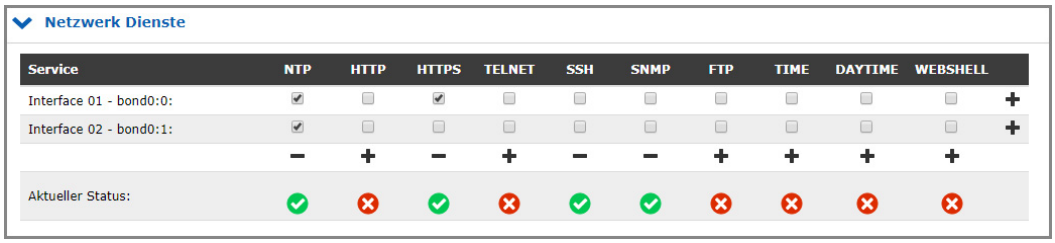


Abbildung 7.8: Dienste deaktivieren

Für den nächsten Schritt wird ein anderer Super-User als root benötigt. Gehen Sie zu Kapitel 10.1.6.4, um einen neuen Super-User zu erstellen. Nachdem Sie den neuen Super-User angelegt haben, melden Sie sich mit seinen Zugangsdaten an und deaktivieren Sie den Root-Login unter „Sicherheit → Anmeldung → Root-Zugang sperren“. Deaktivieren Sie bei Bedarf das Frontpanel unter „Sicherheit → Frontplatte → Frontplatte sperren“, sowie den USB-Anschluss und die lokale Konsole wie in Abbildung 7.9 gezeigt wird. Darüber hinaus können Sie die Fernzugriffssteuerung auf autorisierte IP-Adressen einschränken die in einer „Whitelist“ eingetragen sind. (Hinweis: Die Fernzugriffssteuerung wird für SSH-Verbindungen nicht wirksam).

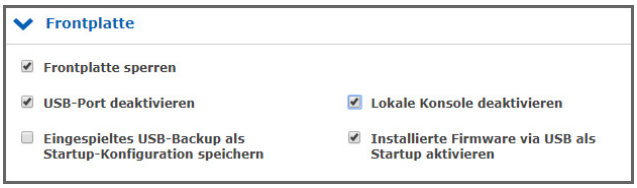


Abbildung 7.9: Sperren des Frontpanels und des USB-Ports

Der Timeout für Web-Sitzungen wird im Webinterface-Menü „Sicherheit“ unter „Anmeldung“ konfiguriert, wie in Bild 7.10 dargestellt ist. Kürzere Laufzeiten minimieren das Sicherheitsrisiko.

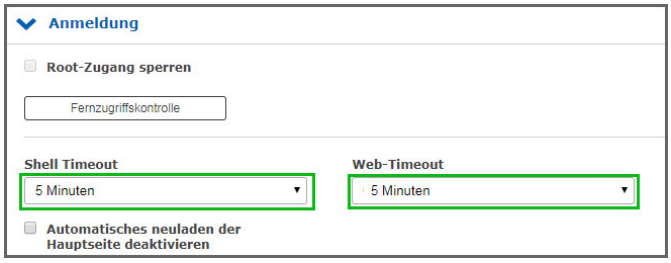


Abbildung 7.10: Timeout der Webschnittstelle einstellen

Werden alle Schritte befolgt, ist der LANTIME gut konfiguriert, um ihn sicher zu verwaltet und zu überwachen. Denken Sie daran, zu überprüfen, ob die IP-Konfiguration und die Fernzugriffskontrolle in der produktiven Netzwerkumgebung funktionieren.

Optional können Sie SNMP zur Verwaltung des LANTIME konfigurieren. Die Sicherheitsoptionen finden Sie unter „Sicherheit → SNMP“. Abbildung 7.11 zeigt das Menü.

Um eine sichere Verbindung über SNMP herzustellen, müssen Sie die Version 3 und den *authPriv-Modus* verwenden. Die zusätzlichen Parameter der Version 3 sind der Benutzername (Sicherheitsname), die Zugriffsrechte, das Authentifizierungs- und Datenschutzprotokoll/Algorithmen. Verwenden Sie SHA512 und AES256 als Algorithmen. Wie üblich werden längere Passwörter bevorzugt. Starten Sie anschließend den SNMP-Dienst auf der Registerkarte „Netzwerk → Netzwerkdienste“.

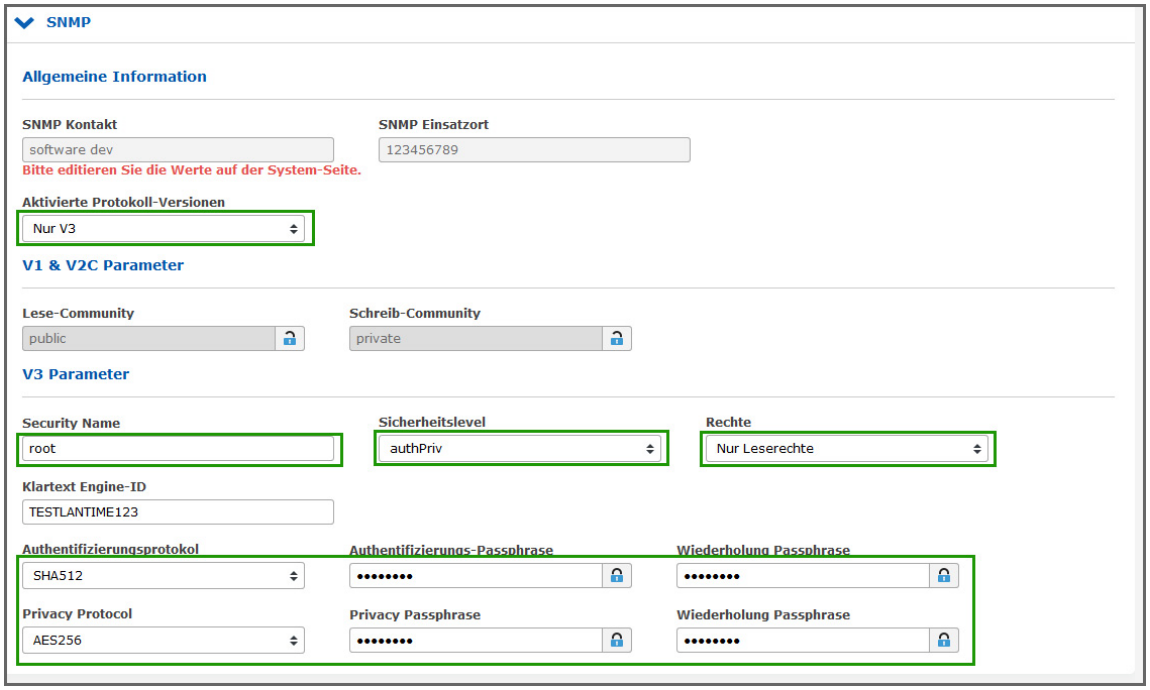


Abbildung 7.11: SNMP Konfiguration

7.3 Benutzer-Management und -Administration

Dieser Abschnitt beschreibt Benutzer- und Authentifizierungsverwaltung. Dieses Kapitel beschreibt die „normale“ Benutzerauthentifizierung und die externen Authentifizierungsserver Radius und TACACS+. Sie können auch im Kapitel „LTOS Management und Überwachung → Über das Webinterface → System → Externe Authentifizierung“ lesen, um weitere Informationen zu erhalten.

7.3.1 LANTIME Benutzerverwaltung

Der LANTIME liefert eine eingebaute Benutzerkonfiguration. Die Optionen finden Sie unter „System → Benutzerverwaltung“.

Es gibt drei verschiedene Benutzergruppen: Super-User, Admin-User und Info-User. Super-User dürfen alles tun, inklusive Bash-Zugang. Admin-User dürfen alles tun, was über die Weboberfläche einzustellen bzw. zu überwachen ist. Sie dürfen aber keine Operationen durchführen, die Superuserrechte vergeben würden. Info-User dürfen nur alle nicht sicherheitsrelevanten Informationen in der Weboberfläche sehen.

Die folgende Tabelle zeigt die Benutzerrechte der einzelnen Zugriffsebenen im Detail.

	Super User	Admin User	Info User
Vollständiger Zugriff auf die Befehlszeile	✓		
Ändern der Gerätekonfiguration durch das Webinterface	✓	✓	
Bearbeitung der zusätzlichen Konfigurationsdateien, die über das Webinterface* verfügbar sind.	✓		
Ausführen eines Firmware-Updates	✓		
Erstellen einer Diagnosedatei	✓		
Erstellen eines neuen Superuser-Accounts	✓		
Überprüfung aller Konfigurationswerte des Webinterfaces	✓	✓	✓

* Zusätzliche Netzwerkkonfiguration, zusätzliche NTP-Konfiguration, benutzerdefinierte Benachrichtigungen

Um einen Benutzer zu erstellen, verwenden Sie das Formular, das in Abbildung 7.12 dargestellt ist. Super-User können alle Benutzertypen anlegen. Der Admin-User kann weitere Admin-User und Info-User anlegen. Geben Sie einen Namen, ein Passwort und die Gruppe des Benutzers ein und drücken Sie dann die Schaltfläche „Benutzer anlegen“. Wenn erfolgreich, wird der neue Benutzer in der Benutzerliste direkt unter dem Formular create user angezeigt. Wählen Sie die Benutzernamen und Passwörter so, dass sie nicht vorhersehbar sind.

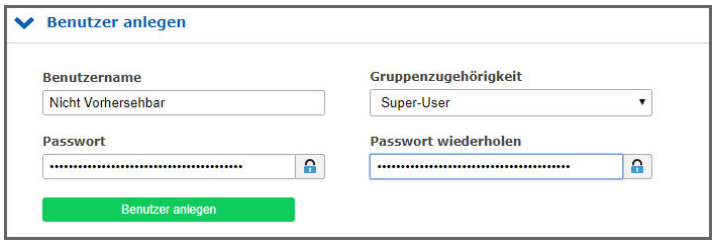


Abbildung 7.12: Einen neuen Super-User erstellen

Abbildung 7.13: Benutzer-Liste

Für Passwörter gibt es einige zusätzliche Optionen, die in Bild 7.14 zu sehen sind. Wählen Sie eine lange Passwortlänge und ein periodisches Änderungsintervall. Zusätzlich können Sie mit der Einstellung „nur sichere Passwörter zulassen“ ein Passwort erzwingen, das viele verschiedene Zeichensätze enthält.

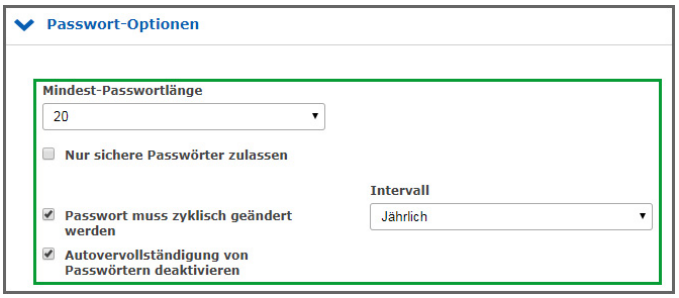


Abbildung 7.14: Passwort-Optionen

7.3.2 Externe Benutzerauthentifizierung: LDAP(S), Radius und TACACS+

Das Kapitel beschreibt die möglichen externen Authentifizierungsmethoden, die von der LANTIME Firmware zur Verfügung gestellt werden.

LDAP (Lightweight Directory Access Protocol)
LDAP basiert auf dem Client-Server-Modell und wird für sogenannte Verzeichnisdienste verwendet. LDAP beschreibt die Kommunikation zwischen dem LDAP-Client und dem Verzeichnisserver. Aus einem solchen Verzeichnis können objektbezogene Daten, wie z.B. Personendaten oder Rechnerkonfigurationen, ausgelesen werden.

RADIUS (Remote Authentication Dial-In User Service)
Ein RADIUS-Server ist ein zentraler Authentifizierungsserver, der von Diensten zur Authentifizierung von Clients in einem physischen oder virtuellen Netzwerk (VPN) verwendet wird. Der RADIUS-Server übernimmt die Authentifizierung für den Dienst, d.h. die Überprüfung von Benutzername und Passwort.

TACACS (Terminal Access Controller Access-Control-System)
TACACS ist ein Kommunikationsprotokoll zur Authentifizierung, das von der IETF standardisiert und weit verbreitet ist. TACACS-Server bieten eine zentrale Authentifizierungsinstanz für Benutzer. In typischen Cisco-Netzwerkumgebungen (z.B. Router und Switches) wird TACACS+ für die zentrale Benutzerverwaltung verwendet.

7.3.2.1 Reihenfolge der Authentifizierungsverfahren

Die Reihenfolge der Authentifizierung stellt sich wie folgt dar, wenn alle Authentifizierungsverfahren (LDAP, RADIUS, TACACS+ und LOKAL) aktiviert und konfiguriert wurden:

1. LDAP
2. RADIUS
3. TACACS+
4. Lokale Anmeldung

Bei gleichen Benutzernamen/Passwortphrasen in unterschiedlichen Systemen ist es also möglich, dass sich die Zugriffsrechte nicht wie gewünscht ergeben. Außerdem kann es so schnell zu intransparenten Log-Nachrichten kommen. Es ist also immer auf die Reihenfolge und konsistente Benutzerdaten/Rechte in den Diensten zu achten.

7.3.2.2 LDAP und LDAPS

Der LANTIME unterstützt die Verbindung zu einem LDAP-Server über LDAP und LDAPS. Meinberg empfiehlt die sichere Kommunikation über LDAPS einzurichten. Dazu muss eine zentrale Vertrauensstelle (RootCA) dem LANTIME bekannt gemacht werden.

Ein Zertifikat einer Zertifizierungsstelle kann über das Webinterface „Sicherheit → Zertifikate → CA Zertifikate“ hochgeladen werden. Der Abschnitt CA Zertifikate beschreibt die Optionen für den Upload von Root-CA-Zertifikaten. Wenn der LDAP-Server ein Zertifikat nutzt, welches von einer globalen Zertifizierungsstelle signiert/ausgestellt wurde, entfällt dieser Schritt. Die Liste von vertrauenswürdigen globalen Zertifizierungsstellen wird mit jedem LANTIME-Update aktualisiert.

Die Konfiguration einer LDAP(S) Anbindung wird im Kapitel „Webinterface → Benutzerverwaltung → Externe Authentifizierung → 10.1.6.7 (LDAP Setup)“ beschrieben.

7.3.2.3 Externe Authentifizierung über LDAP

Die externe Authentifizierung über LDAP kann in dem Webinterface unter „System → Benutzerverwaltung → Benutzer-Administration → Externe Authentifizierung → LDAP / LDAPS“ konfiguriert werden. Die LANTIME-Firmware unterstützt eine anonyme sowie benutzerbezogene Anmeldung. Für eine Microsoft-Active-Directory-Anmeldung muss ein Benutzername (LDAP Benutzer bzw. binddn) und eine Passwortphrase (LDAP Passwort bzw. bindpw) angegeben werden. Die Suchstrategie (Search Scope) für AD-Einträge kann über base (baseObject), one (singleLevel) und sub (wholeSubtree) verändert werden. Der dazugehörige Suchpfad im AD kann über das Feld „Search Base“ angegeben werden.

Ein Beispiel für einen Pfad wäre *„CN=Users,DC=test,DC=mbg,DC=de“*.

Damit die AD-Informationen auf die lokalen Einstellungen abgebildet werden können, müssen „Filter“ und „Mappings“ angelegt werden. Im AD können die Attribute frei gewählt werden, die die Information beinhalten sollen. Ein Filter wird angegeben, um die Ergebnismenge der LDAP-Antwort auf die erforderlichen Attribute zu beschränken. Das Mapping wird benötigt, um von RFC2307 abweichende Attribute des LDAP-Verzeichnisdienstes auf die korrekten im RFC angegeben Attribute, die von dem LDAP-Dienst auf dem LANTIME genutzt werden, abzubilden. Die User-ID für die passwd-Abbildung wird zum Beispiel durch folgendes Mapping von dem frei gewählten Attribut „sAMAccountName“ auf das im RFC2307 dafür vorgesehene Attribut „uid“ abgebildet: *„passwd uid sAMAccountName“*.

Die mindestens anzugebenden Informationen sind:

- Die User-ID (der Anmeldename)
- Die User-ID-Nummer (eine Nummer, die nicht durch einen lokalen Benutzer vergeben ist oder vergeben werden könnte)
- Die User-Gruppen-Nummer (Gruppenzugehörigkeit siehe unten)
- Das User-Home-Verzeichnis (neuer Ordner unter /home/)

Der einzige Wert, der im Verzeichnisserver nicht frei vergeben werden kann, ist die Gruppenzugehörigkeit im LTOS. Folgende Werte können z.B. im „gidNumber“ Attribut hinterlegt werden:

- Die Gruppe Super-User hat die Gruppen-ID = 0
- Die Gruppe Admin-User hat die Gruppen-ID = 4
- Die Gruppe Info-User hat die Gruppen-ID = 100

Die Verbindung zum LDAP-Server kann unter dem Menüpunkt „Global“ angegeben werden, so bald ein neuer LDAP-Server über den Button „LDAP Server hinzufügen“ hinzugefügt wurde. Es kann zwischen „ldap“ und „ldaps“ gewählt werden und es muss die URI des LDAP-Servers angegeben werden.

Hinweis:
Die URI muss bei einer ldaps-Verbindung mit der URI (im Common-Name oder den Subject-Alternative-Names) des LDAP-Server-Zertifikats übereinstimmen, da sonst die Verifizierung fehlschlägt.

Der Modus steuert, ob ein konfigurierter LDAP-Server angefragt wird. Sollte der Port vom Standard (389, 636) abweichen, kann über das Feld „Alternativer Port“ ein anderer ausgewählt werden. Über den Reiter „Misc“ können LDAP-Server wieder entfernt werden. Wenn alles eingestellt ist müssen die Einstellungen über den Button **„Speichern“** in die laufende Konfiguration übernommen werden. Nach dem Funktionstest kann die laufende Konfiguration als Startkonfiguration gespeichert werden.

Zum derzeitigen Firmware-Stand 7.02.003 können Fehlermeldungen des ldap-Dienstes über die System-Messages (CLI oder WEB) eingesehen werden. Authentifizierungsgfehler werden in die Datei */var/log/auth.log* geschrieben.

7.3.2.4 Radius- und TACACACS-Verbindung

Zusätzlich zu den von LANTIME selbst verwalteten Benutzern kann eine Radius- oder TACACACS-Verbindung zur Authentifizierung von Benutzern verwendet werden. Diese Verbindung muss in der Benutzerverwaltung unter „Externen Authentifizierungsserver erlauben“ freigegeben werden. Siehe Abbildung 7.15 für die Eingabemöglichkeiten. Sie müssen zuerst die externe Authentifizierung aktivieren. Wählen Sie anschließend Radius oder TACACS+ aus dem Dropdown-Menü und geben Sie den Hostnamen, den vorab ausgetauschten Schlüssel und den korrekten Port ein. Von nun an ist es möglich, sich mit dem externen Authentifizierungsmechanismus anzumelden. Zunächst prüft das System den externen Server auf den Benutzer. Wenn kein Benutzer mit diesen Zugangsdaten existiert, prüft das System die lokalen Benutzer. Wie man einen externen Authentifizierungsserver konfiguriert wird im Kapitel „LTOS Management und Monitoring → Webinterface → Externe Authentifizierung“ beschrieben.

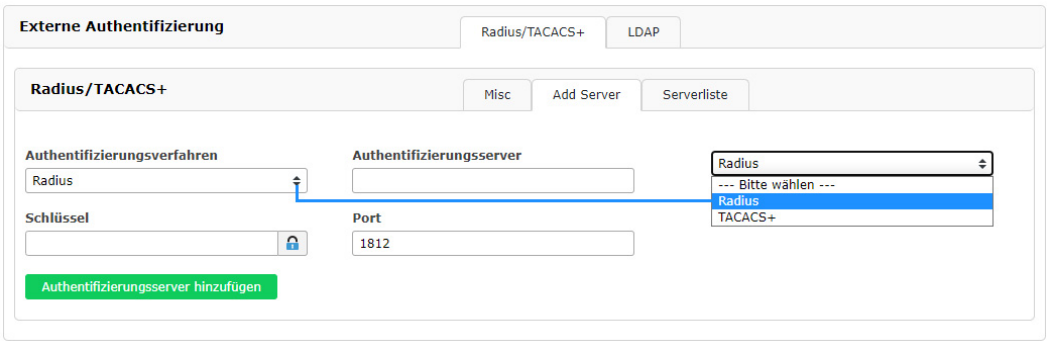


Abbildung 7.15: Webinterface Menü „System → Benutzerverwaltung → Externe Authentifizierung“

7.4 Sicherung des NTP-Zeitdienstes

Der NTP-Zeitdienst bietet eine authentifizierte und integritätsgesicherte Paketübertragung. Derzeit gilt der NTP-Autokey als nicht so sicher wie das symmetrische Schlüsselverfahren. Daher wird in diesem Leitfaden die symmetrische Schlüsselkonfiguration verwendet. Das Kapitel „LTOS Management und Überwachung → Über das Webinterface → NTP Symmetrische Schlüssel“ beschreibt alle Konfigurationsmöglichkeiten im Detail.

Um eine Verbindung zu konfigurieren, benötigt das System einen Schlüssel. Verwenden Sie entweder neu generierte oder fügen Sie vorhandene Schlüssel in der Schlüsseldatei über die Schaltfläche **NTP-Schlüssel bearbeiten** im Menü „NTP → NTP Symmetrische Schlüssel“ hinzu. Wenn Sie die Schlüssel vom System automatisch generieren lassen, sind MD5 und SHA1 Schlüssel in der Schlüsseldatei vorhanden. Für die derzeit höchste Sicherheit sind jedoch AES128-CMAC Schlüssel zu verwenden. Diese können noch nicht automatisch generiert werden.

Wie Sie AES128-CMAC-Schlüssel erzeugen können, wird im Kapitel „Konfiguration → Webinterface → NTP → NTP Symmetrische Schlüssel“ beschrieben.

Die Abbildung 7.16 zeigt Beispiele für generierte und modifizierte (AES128CMAC) NTP-Schlüssel. Die Schlüssel-IDs müssen den vertrauenswürdigen Schlüsseln im Menüpunkt „Allgemeine Einstellungen“ in der Registerkarte NTP hinzugefügt werden (siehe Bild 7.17). Im Menü „NTP Zugriffsbeschränkung“ können Sie auch die Paketunterstützung für Modus 6 und 7 deaktivieren. Optional können Sie hier die Zugriffsbeschränkung aktivieren, um den Zugriff nur auf bekannte IP-Adressen zu ermöglichen. Die symmetrischen Schlüssel werden für jeden Verbindungstyp verwendet, d.h. Server zu Client, externer NTP-Server, Broadcast, Multicasting und Manycasting.

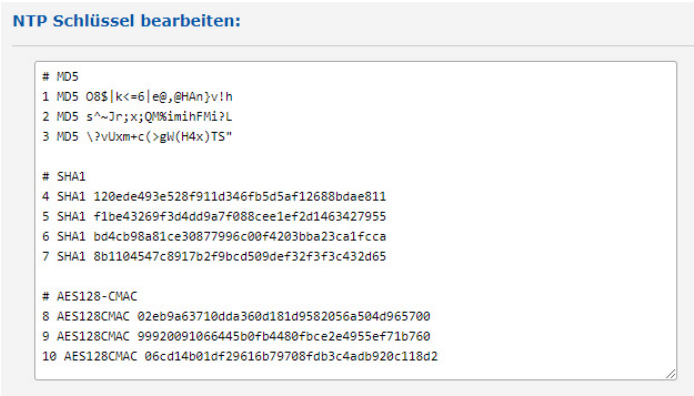


Abbildung 7.16: Symmetrische NTP-Schlüssel

Abbildung 7.17: Vertrauenswürdige Schlüssel-IDs

Die Einfügepunkte für die richtigen Schlüssel-IDs sind in Abbildung 7.18, 7.19 und 7.20 markiert. Die Konfigurationsdatei eines Clients ist in Bild 7.21 dargestellt. Sie enthält den Pfad zur Schlüsseldatei, die vertrauenswürdigen Schlüssel-IDs und die Server-IP, die in diesem Beispiel den Schlüssel mit der ID 1 verwendet.

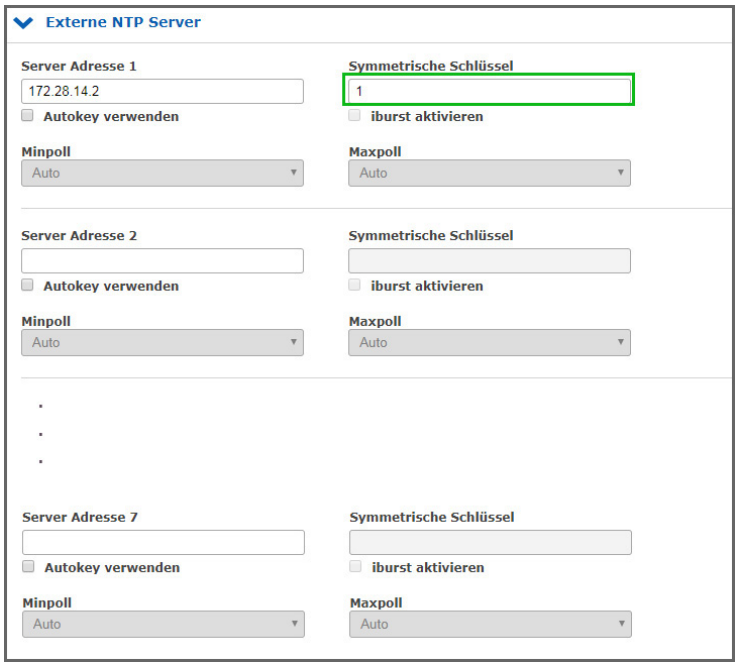


Abbildung 7.18: Externe Severkonfiguration

Abbildung 7.19: Broadcast-Konfiguration

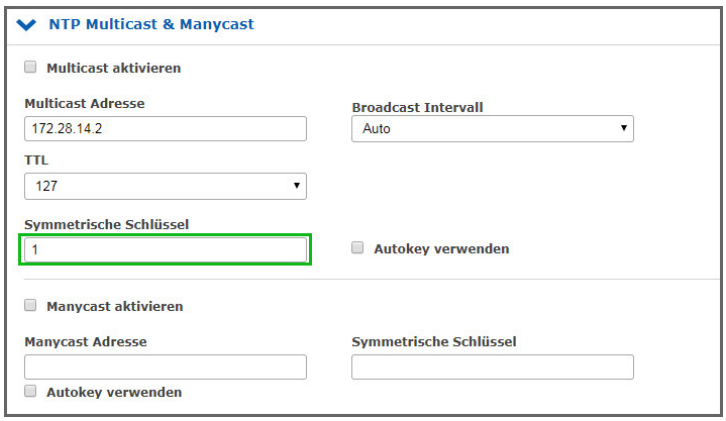


Abbildung 7.20: Multi- und Manycast-Konfiguration

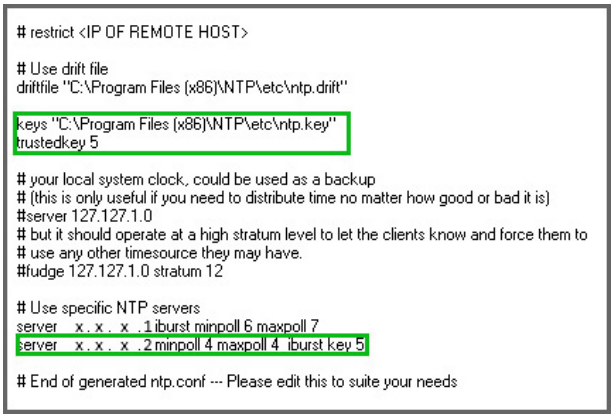


Abbildung 7.21: NTP Client-Konfiguration

7.5 Ausgabe von Ereignisprotokollen

Der LANTIME bietet viele Transportkanäle für Ereignisprotokollinformationen und eine fein abgestufte Benachrichtigungsauswahl für jeden dieser Kanäle. Derzeit kann, mit Ausnahme von SNMPv3, kein Ereignistransportkanal abgesichert werden. Es ist eine gute Praxis, Ereignisprotokollinformationen auf einem zentralen Server zu sammeln, um sie zu korrelieren und auf Anomalien zu überprüfen. Beachten Sie dabei mögliche sicherheitsrelevante Informationslecks aufgrund der fehlenden Verschlüsselung bei anderen Diensten als SNMPv3.

Das Kapitel „LTOS Management und Monitoring → Über das Webinterface → Benachrichtigung“ beschreibt die Konfigurationsmöglichkeiten für die Transportkanäle. Wenn Sie SNMP v3 mit der gewählten **authPriv**-Sicherheitsstufe verwenden, werden auch SNMP-Traps sicher versendet. Konfigurieren Sie die SNMP authPriv-Einstellung wie unter „Sicherheit → SNMP“ in Kapitel 7.2 beschrieben.

7.6 Aktualisieren und Sichern der LANTIME-Firmware

Laden Sie die neueste LTOS-Version unter https://www.meinberg.de/german/sw/firmware.htm herunter. Die heruntergeladene LTOS-Datei muss über die LANTIME-Weboberfläche unter „System → Firmware/Software Update“, wie in Abbildung 7.22 dargestellt, hochgeladen werden. Die LTOS V7 Firmware ist mit einer digitalen Signatur ausgestattet, die beim Test „Preflight Checks“ direkt nach dem Upload überprüft wird. Sollte dieser Test eine fehlerhafte Signatur feststellen, wird eine Warnung ausgegeben. Wenn dies geschieht, laden Sie die neue Firmware erneut von der Meinberg Web-Seite und wiederholen Sie den Vorgang. Bei wiederholten Warnungen kontaktieren Sie bitte den Meinberg-Support.

Im nächsten Schritt müssen Sie das Update bestätigen und die neue Firmware, wie in Bild 7.23 gezeigt, aktivieren. Das Update war erfolgreich, wenn Abbildung 7.24 angezeigt wird.

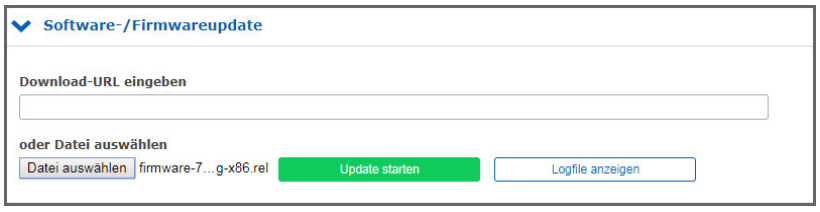


Abbildung 7.22: Firmware auswählen und hochladen

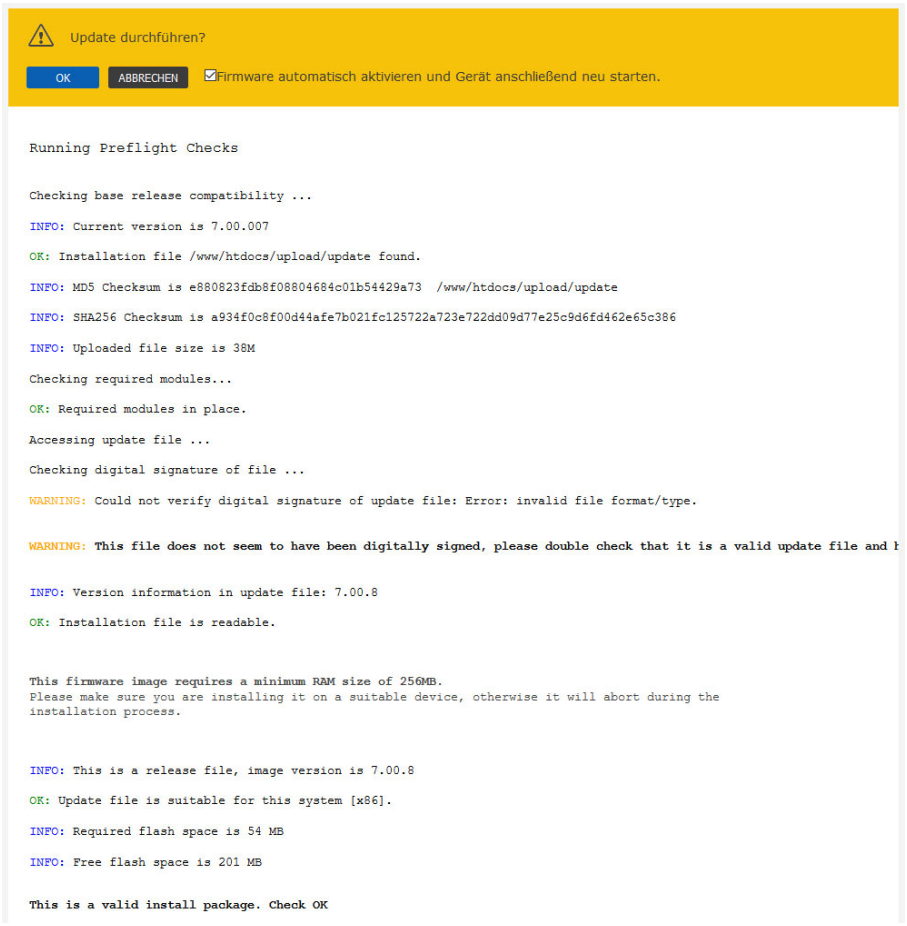


Abbildung 7.23: Firmware-Update-Prozedur bestätigen

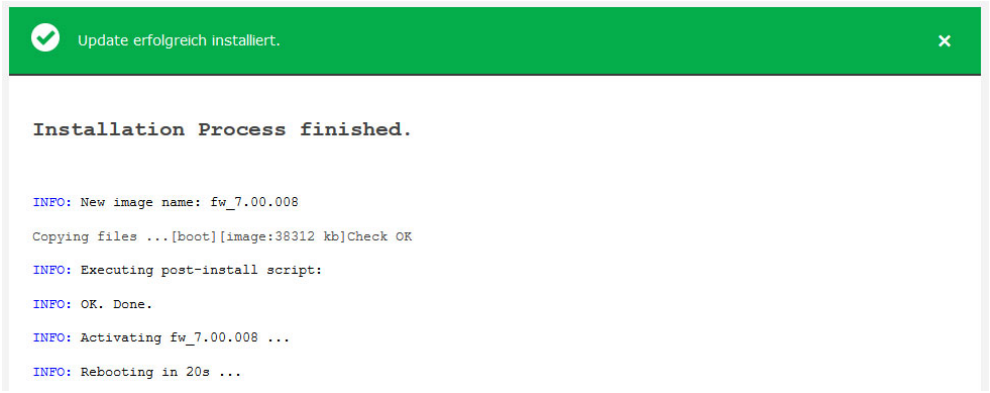


Abbildung 7.24: Firmware wurde aktualisiert

Die Konfigurationseinstellungen des LANTIME bleiben bei einem Firmware Update erhalten, mit Ausnahme der Konfigurationsdateien des Webservers und des SSH-Dienstes. Diese werden bei einem Update überschrieben, um aktuelle kryptografische Verfahren mit einem Update ausliefern zu können. Sollte die automatische Aktualisierung entgegen unserer Empfehlung nicht gewünscht sein, kann eine eigene kundenspezifische Konfigurationsdatei für diese Dienste hinterlegt werden.

SSH Konfiguration:
In der Konfigurationsdatei */etc/ssh/ssh.cfg* wird definiert, welche Konfigurationsdatei der SSH-Dienst verwenden soll. In der Werkskonfiguration enthält die Datei folgenden Eintrag:

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

Sofern die Datei */etc/standard/sshd_config* als SSH-Konfigurationsdatei definiert ist, wird diese Datei bei einem Firmware-Update aktualisiert. Ist die Datei */etc/ssh/sshd_config* eingetragen, kann in dieser eine eigene Konfiguration angelegt werden, die bei einem Update nicht ersetzt wird.

Webserver Konfiguration:
In der Konfigurationsdatei */etc/webUI/webUI_custom.cfg* wird definiert, welche Konfigurationsdatei der Webserver verwenden soll. In der Werkskonfiguration enthält die Datei folgenden Eintrag:

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

Sofern keine Datei als Webserver-Konfigurationsdatei definiert ist wird die Werkskonfigurationsdatei, die bei einem Firmware-Update aktualisiert wird, verwendet. Ist eine beliebige Datei unter */mnt/flash/data/* eingetragen, kann in dieser eine eigene Konfiguration angelegt werden, die bei einem Update nicht ersetzt wird. Dateien, die unter */mnt/flash/data* abgelegt werden sind nicht Teil einer Konfiguration, sie sind jedoch rebootsicher (persistent) gespeichert.

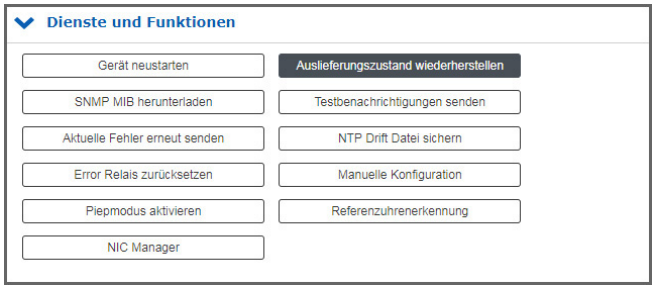


Abbildung 7.25: LANTIME auf Werkseinstellungen zurücksetzen

Damit der SSH-Dienst und der Webserver wieder automatische Konfigurationsupdates erhalten, können Sie die werksseitigen Pfade in diesen beiden Dateien wiederherstellen.

Das Wiederherstellen der werksseitigen Standardeinstellungen über das Webinterface, wie in 7.25 gezeigt, bewirkt, dass alle benutzerdefinierten Konfigurationseinstellungen bis auf die Netzwerkeinstellungen in der aktuellen Startup-Konfiguration zurückgesetzt werden. Im Detail bedeutet dies, dass u.a. Ihre Zertifikate, Zugangsdaten, SNMP, NTP und SSH-Schlüssel verloren gehen. Zuvor unter einem anderen Namen gespeicherte Konfigurationen bleiben auch bei einem Factory-Reset erhalten. Diese müssen, wenn gewünscht, zusätzlich über das Webinterface gelöscht werden.

Nach einem „Reset“ der Firmware über die Webschnittstelle werden alle Zertifikate auf die werkseitigen Voreinstellungen umgestellt. Der SSH-Schlüssel wird beim Hochfahren nach dem Reset zufällig neu generiert.

Ein Backup der LANTIME-Firmware, ob heruntergeladen oder auf der Flash-Speicherkarte des LANTIME gespeichert, erfolgt in Klartextform. Achten Sie daher darauf, dass kein Unbefugter Zugriff darauf hat. Das Gleiche gilt für eine Diagnosedatei.

8 LANTIME Basic Configuration Wizard

Nach dem Einschalten des Gerätes kann nach ca. einer Minute ein Terminalprogramm (z.B. Putty) über die serielle Schnittstelle (TERM/CONSOLE), verbunden mit einem Nullmodemkabel oder einem CAB-CONSOLE-RJ45 Kabel, gestartet werden. Die Einstellungen für die Schnittstelle müssen auf 38400 Baud, 8 Datenbits, keine Parität und ein Stopbit (8N1) eingestellt werden. Die Terminal Emulation muss auf VT100 gesetzt werden. Computer ohne serielle Schnittstelle können mit einem „Serial-to USB“ Konverter angeschlossen werden.

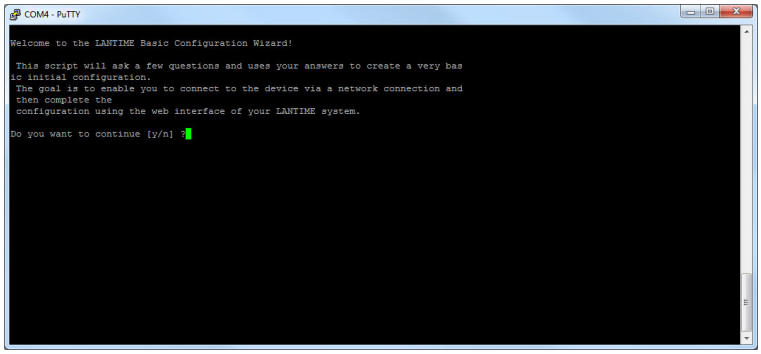
Nach dem Herstellen der Verbindung sollte die Eingabeaufforderung für die Benutzerkennung angezeigt werden:

Welcome to Meinberg LANTIME
login: _

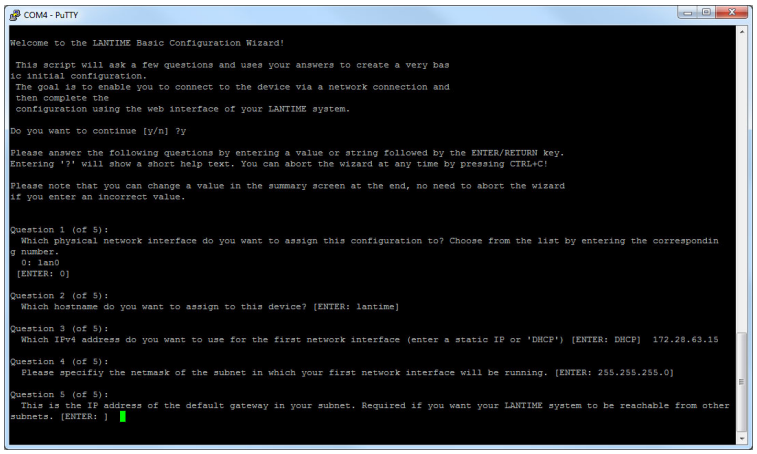
Default Benutzer: **root**
Default Passwort: **timeserver**
(evtl. noch einmal RETURN drücken)

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

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



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



Bestätigen Sie ihre anschließend ihre Konfigurationen.

9 Einleitung Konfiguration LANTIME

Das LANTIME bietet mehrere Möglichkeiten zur Konfiguration der Parameter:

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

Zur ersten Inbetriebnahme des LANTIME muss das Frontpanel LCD/VFD Interface benutzt werden, um dem Gerät eine IP Adresse zu vergeben (siehe auch DHCP IPv4 oder AUTOCONF IPv6). Wurde einmal das Netzwerkinterface mit entweder einer IPv4 Adresse, Netzmaske und IPv4 GATEWAY oder über die IPv6 SCOPE-LINK Adresse initialisiert, kann von einem anderen Rechner im Netzwerk (remote) auf den LANTIME zugegriffen werden.

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

Um eine TELNET Verbindung zu dem LANTIME aufzubauen, geben Sie die folgenden Befehle von Ihrer Kommandozeile ein:
telnet 198.168.10.10 // IP Adresse vom LANTIME
Default Benutzer: root
Default Passwort: timeserver

Um eine SSH Verbindung zu dem LANTIME aufzubauen, geben Sie den folgenden Befehl von Ihrer Kommandozeile ein:
ssh root@198.168.10.10 // Default User @ IP Adresse vom LANTIME
Default Passwort: timeserver

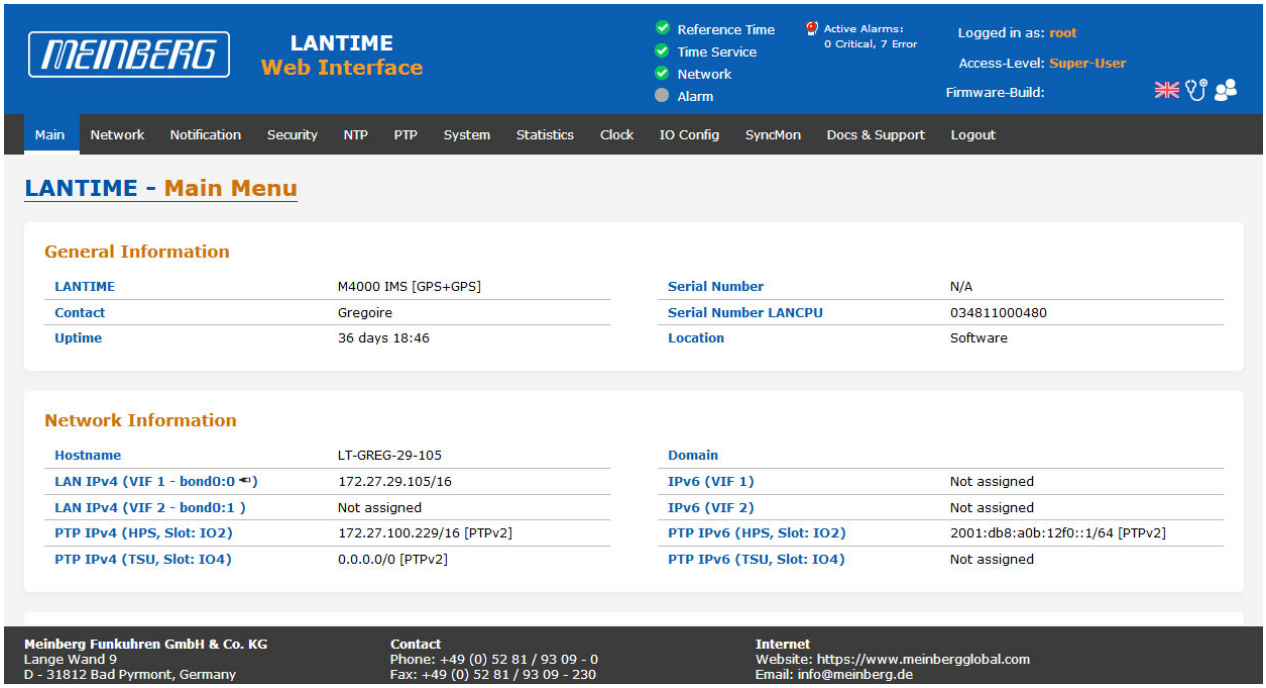
Um eine HTTP Verbindung zu dem LANTIME aufzubauen, geben Sie die folgende Adresse in Ihrem WEB-Browser ein:
http://198.168.10.10 // IP Adresse vom LANTIME
Default Benutzer: root
Default Passwort: timeserver

Um eine Secure HTTP (HTTPS) Verbindung zu dem LANTIME aufzubauen, geben Sie die folgende Zeile in Ihrem WEB-Browser ein:
https://198.168.10.10 // IP Adresse vom LANTIME
Default Benutzer: root
Default Passwort: timeserver

10 LTOS7 Management und Überwachung

10.1 Das Webinterface

10.1.1 Startmenü



In diesem Kapitel finden Sie Konfigurations- und Statusinformationen Ihres LANTIME-Systems, auf die Sie über die Web-GUI zugreifen können. Die Startseite gibt einen Überblick über die wichtigsten Konfigurations- und Statusparameter des Systems.

- Informationen über das LANTIME-Modell und die verwendete Firmware
- Netzwerkinformationen
- Status des Empfängers
- NTP-Status
- PTP-Status (Option)
- Letzte Nachrichten
- Statistiken (NTP/MRS Leistung, NTP Zugriff....)
- Erweiterte Statistik (MRS - externe Referenzeingangssignale)
- Dokumentation (Handbücher), Supportinformationen

Das Feld im unteren Bereich zeigt die letzten Nachrichten des Systems mit einem Zeitstempel an. Die neuesten Nachrichten stehen ganz oben in der Liste. Dieses ist der Inhalt der Datei /var/log/lantime_messages, die nach jedem Systemstart erstellt wird (und nach einem Ausschalten oder Neustart verloren geht).

Über die Navigation oben auf der Seite erreichen Sie eine Reihe von Konfigurationsmenüs, die in den folgenden Kapiteln beschrieben werden.

10.1.1.1 Einleitung

Um eine http- oder eine gesicherte https-Sitzung mit dem Web Interface auf der CPU Ihres LANTIME-Systems zu starten, müssen Sie Ihren Internetbrowser öffnen und die IP-Adresse der Netzwerk-Schnittstelle eingeben, die Sie für diese Verbindung verwenden. Per Standardkonfiguration ist das https-Protokoll an jeder Netzwerkschnittstelle aktiviert. Http-Anfragen werden automatisch an https umgeleitet.

Wenn Sie nur eine dedizierte Netzwerkschnittstelle für Management und Monitoring und den Rest für andere Dienste nutzen möchten, finden Sie die entsprechenden Konfigurationsoptionen im Kapitel „LTOS-Konfiguration → Webinterface → Netzwerk“ im Untermenü Netzwerkdienste.

Wenn die Verbindung mit dem LANTIME korrekt hergestellt wurde, werden Sie aufgefordert, Login-Daten einzugeben, um die Web-Sitzung zu starten. Standardmäßig lautet die Eingabe von Benutzername/Passwort: root/timeserver. Aus Sicherheitsgründen wird empfohlen, die Standard-Anmeldeinformationen nach der ersten Anmeldung zu ändern. Die entsprechenden Einstellungen zur Benutzerverwaltung finden Sie im Kapitel „LTOS6 Konfiguration → Webinterface → System“ im Untermenü Benutzerverwaltung.

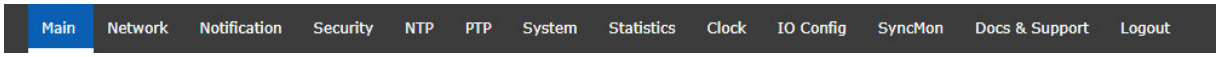
Nach Eingabe des korrekten Passworts erscheint die Hauptmenü-Seite des Webinterfaces eines LANTIME-Systems.

Die Hauptseite enthält einen Überblick über die wichtigsten Konfigurations- und Statusparameter des Systems, einschließlich:

- allgemeine Informationen (Modellname, Seriennummer, Betriebszeit seit dem letzten Neustart)
- zugeordnete Netzwerk- und PTP-Schnittstellen (beide in IPv4- oder IPv6-Konfiguration)
- Empfänger-Statusinformationen (synchronisieren oder nicht, bei GNSS-Empfängern einige zusätzliche Satellitendaten)
- SHS (Secure Hybrid System) Status in redundanter Empfängerkonfiguration, der einen Plausibilitätsmodus bietet, bei dem die Eingangszeiten beider Zeitsignale kontinuierlich miteinander verglichen werden. Weitere Informationen zum SHS-Modus und den entsprechenden Einstellungen finden Sie im Kapitel „LTOS6 Konfiguration → Webinterface → Sicherheit → SHS-Konfiguration“.

10.1.1.2 Das Hauptmenü - Navigation im Webinterface

Über die Navigation oben auf der Seite erreichen Sie eine Reihe von Konfigurationsmenüs, die in den folgenden Kapiteln beschrieben werden.



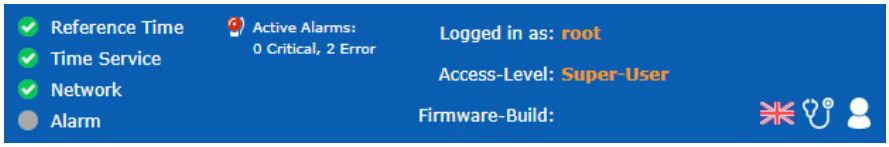
Wenn Sie auf der Hauptseite nach unten scrollen, finden Sie einen Abschnitt mit den letzten Protokollmeldungen, die während des LANTIME-Betriebes erzeugt wurden. Die Nachrichten in diesem Feld sind auf die letzten 50 begrenzt und chronologisch geordnet. Die Meldungen werden in der Datei */var/log/lantime_messages* gespeichert, die nach jedem Systemstart erstellt wird (und nach einem Ausschalten oder Neustart verloren geht). Um alle Protokollmeldungen in der Protokolldatei anzuzeigen, müssen Sie das CLI (Command Line Interface) verwenden. Zu Ihrer Information finden Sie eine Liste der verfügbaren CLI-Befehle für die LANTIME-Verwaltung und -Überwachung in der Kommandozeilen-Referenz.

10.1.1.3 Webinterface - Benachrichtigungen und Alarme

Oben auf der Hauptseite in der rechten Ecke finden Sie ein Bild der Status-LED-Lampen, die sich auch physisch an der Vorderseite eines LANTIME-Systems befinden (Modelle mit integrierter Frontplatteneinheit). Wenn das System in Betrieb ist und alles wie erwartet läuft, leuchten die oberen drei Status-LEDs grün und die Alarmanzeige erlischt. Wenn Sie nach dem Einschalten des Systems und nach Abschluss des Startvorgangs feststellen, dass eine oder mehrere LEDs rot leuchten, lesen Sie bitte das Kapitel über Troubleshooting und Alarmierungen.

Bitte beachten Sie: Der Start des Systems kann je nach Hardwarekonfiguration Ihres Systems einige Minuten dauern.

Neben den Status-LEDs werden alle aktiven Alarme angezeigt, die derzeit in einem LANTIME als kritisch und schwerwiegend eingestuft sind. Mit einem Mausklick auf die Alarme gelangen Sie zu einer Tabelle der Benachrichtigungsereignisse die die Alarme ausgelöst haben. Diese sind mit roten Indikatoren gekennzeichnet.



Weitere Informationen zur Beseitigung einer Ursache für jeden einzelnen Alarm finden Sie im Kapitel Troubleshooting und Alarmierungen.

Neben dem Alarmbereich auf der Hauptseite befindet sich ein Feld mit Informationen über Ihren Login-Status und Informationen darüber, zu welcher Access-Level-Gruppe Sie als aktueller Benutzer gehören. Es gibt drei Arten von Benutzern: Super-User, Admin-User und Info-User. Die genauen Definitionen der drei verschiedenen Benutzertypen und deren Zugriffsrechte finden Sie im Kapitel „LTOS6 → Webinterface → System → Benutzerverwaltung“.

In der oberen rechten Ecke der Hauptseite sehen Sie weitere Symbole. Die angezeigte Flagge zeigt das Sprachpaket an, das gerade für die Anzeige der Weboberfläche aktiviert ist. Im Moment können Sie zwischen englischen und deutschen Sprachpaketen wählen.

Neben dem Sprachkennung befindet sich ein „Arzt-Stethoskop-Symbol“. Dieses Icon ist mit einer Diagnose-Datei des Systems verknüpft. Alle notwendigen Daten für die Diagnose und Fehlersuche des Gerätes sind in dieser Datei enthalten. Durch Anklicken dieses Symbols wird sofort eine aktuelle Diagnosedatei zum Herunterladen erzeugt, die Sie auf Ihrem lokalen Computer speichern und weiterverwenden können. Der Download kann je nach Dateigröße, die mehrere MB betragen kann, bis zu 60 Sekunden dauern. In der Diagnose-Datei werden alle Daten über die Systemkonfiguration und Protokollmeldungen gesammelt. Die Diagnose-Datei kann auch ein wichtiges Werkzeug für das Meinberg-Support-Team sein, wenn Sie Hilfe bei der Konfiguration benötigen oder Probleme haben, die Sie nicht alleine lösen können. Mehr Informationen zur Diagnosedatei finden Sie im Kapitel „LTOS6 Konfiguration → Webinterface → System → Download Diagnosedatei“.

Die Weboberfläche ist in mehrere Dialogmenüs unterteilt, wobei einige der Menüpunkte (z.B. PTP, IO-Konfiguration, SyncMon) von den im LANTIME-System integrierten Hardwarekomponenten abhängen und nur in Systemen mit entsprechender Konfiguration erscheinen. Die restlichen Dialoge sind für alle LANTIME- und IMS-Systeme gleich.

Sie können zwischen den Dialogen wechseln, indem Sie auf einen Menüpunkt oben in der Menüzeile klicken. Haben Sie in einem Dialog etwas an den Einstellungen geändert, müssen Sie den „Speichern-Button“ betätigen, bevor Sie in einen anderen Topmenü-Eintrag wechseln. Wenn Sie auf „Logout“ klicken, wird Ihre laufende Web-Session mit dem LANTIME-Gerät sofort beendet.

Die beiden Dialoge „Main“ und „SyncMon“ liefern Ihnen nach dem letzten Neustart die Statusinformationen über das LANTIME-System. Der Rest der Dialoge bietet Konfigurationen von Funktionen für den LANTIME-Betrieb und die verwendeten Dienste. Die Dialoge mit Eigenschaft-Konfigurationen werden in einer Baumstruktur dargestellt, in der jedes Untermenü durch Anklicken des Zeichens „→“ am Anfang der Untermenüzeile zu einem Submenü erweitert werden kann. Wenn Sie den Dialog öffnen, wird der „→“ zu „↓“ und wenn Sie auf das „↓“-Symbol klicken, wird der aktuell geöffnete Dialog geschlossen. Sie können im aktuell ausgewählten Menü einige Dialoge gleichzeitig öffnen (siehe Abbildung auf der nächsten Seite).

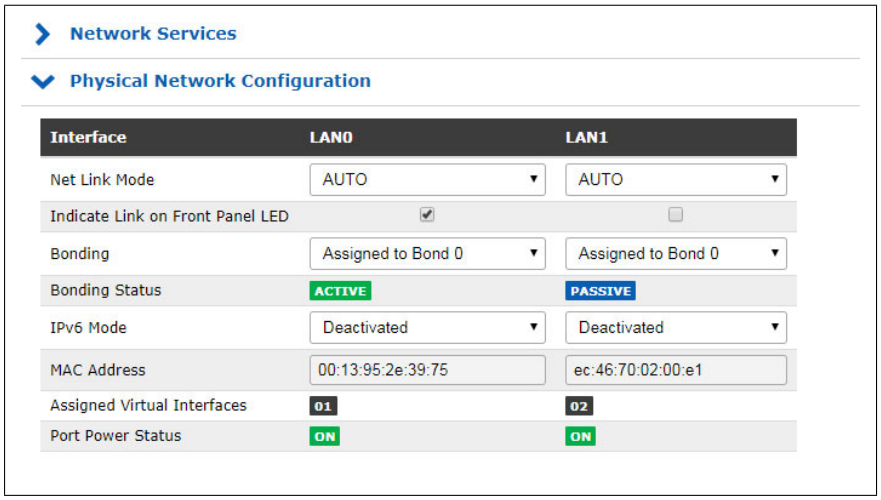


Abbildung: Eine Baumstruktur der einzelnen Menüs. Öffnen einer Verzweigung durch Anklicken eines „→-Symbols“ und Schließen durch „↓“ vor dem Menünamen.

Im Allgemeinen müssen Sie in jedem Konfigurationsmenü, in dem Sie sich befinden, beim Ausfüllen oder Bearbeiten eines oder mehrerer Funktionsfelder am Ende der Seite die Einstellung durch Anklicken der Schaltfläche „Einstellungen speichern“ am unteren Rand der Seite bestätigen. Wenn Sie diesen Schritt ausführen und die Einstellung erfolgreich übernommen wurde, erhalten Sie im Hauptmenü einen Dialog mit einer Bestätigungsnachricht auf einem grünen Feld. Gleichzeitig mit der Anwendung einer neuen Konfiguration erscheint eine Logmeldung in der Liste der letzten Meldungen im Hauptmenü: „Gerätekonfiguration geändert“.

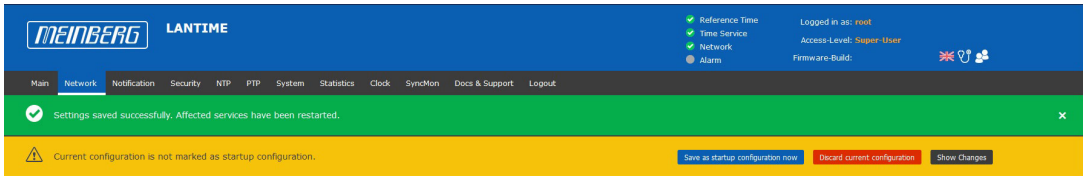


Abbildung: Einstellungen wurden erfolgreich gespeichert. Betroffene Dienste wurden neu gestartet.

Ein Dialog zum Speichern der Startkonfiguration. Optionen zum Speichern, Verwerfen der aktuellen Konfiguration und Anzeigen von Änderungen zwischen der Startkonfiguration und der aktuellen Konfiguration.

Neben der Konfigurationsmeldung erhalten Sie auch einen Aufmerksamkeitshinweis, der auf einer gelben Leiste angezeigt wird: „Die aktuelle Konfiguration ist noch nicht als Startkonfiguration gekennzeichnet“. Das bedeutet, dass Sie die neue Konfiguration zunächst durch Anklicken einer Schaltfläche „Jetzt sichern als Startkonfiguration“ bestätigen müssen, wenn Sie diese beim nächsten Systemstart als Startkonfiguration ausführen möchten. Wenn Sie auf diese Schaltfläche klicken, erhalten Sie eine weitere Bestätigungsnachricht: „Aktuelle Konfiguration wirklich als Startkonfiguration aktivieren?“, die Sie durch Anklicken der Schaltfläche „OK“ bestätigen. Die neue Konfiguration ist nun die aktive Startkonfiguration auf Ihrem LANTIME-System.

Wenn Sie hingegen zur zuletzt gespeicherten Startkonfiguration zurückkehren möchten, wählen Sie die Schaltfläche „Aktuelle Konfiguration verwerfen“, wenn die Meldung auf einer gelben Leiste erscheint.

Jeder Eintrag, den Sie in den angebotenen Dialogen eingeben, wird auf Plausibilität für dieses Feld geprüft. Wenn Sie z.B. falsche Zeichen verwendet haben (z.B. Buchstaben in der IP-Adresse oder Sonderzeichen, die nicht erlaubt sind) oder Sie eine ungültige Netzwerkkonfiguration angegeben haben, erhalten Sie eine Meldung auf einem roten Balken, die eine Fehlermeldung und den Zeitpunkt des Eigenschaften-Eintrags angibt. Der falsche Eintrag wird vom System nicht akzeptiert, auch nicht der Rest der neuen Einstellungen, die Sie zu diesem Zeitpunkt vorgenommen haben, daher müssen Sie die Konfigurationsschritte erneut durchführen. Siehe nachfolgend ein Beispiel für eine Warnmeldung, wenn ein Fehler bei der Eingabe eines Parameterwertes auftritt.

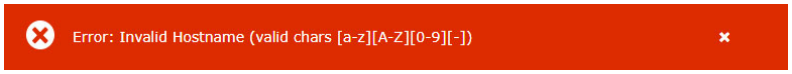
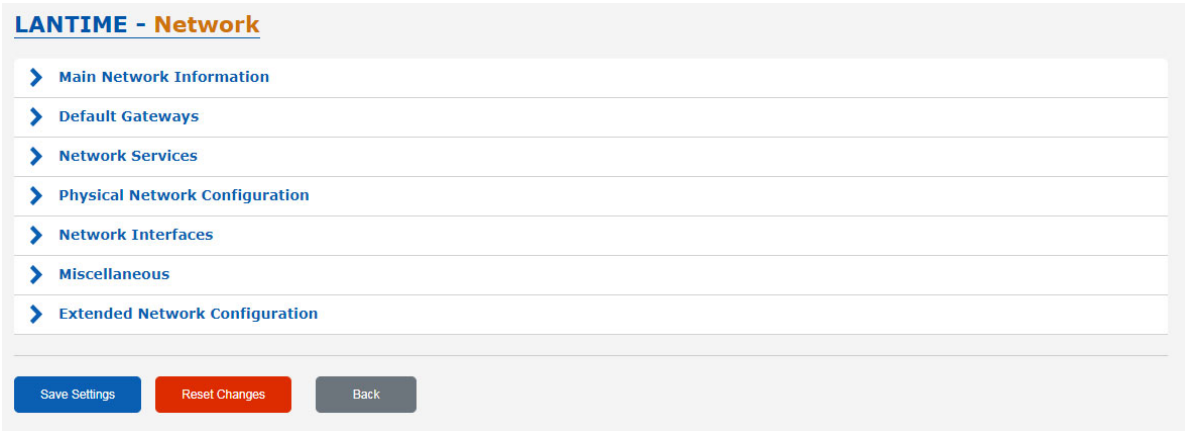


Abbildung: Anzeige einer Warnmeldung mit einer Fehlermeldung und Angabe, zu welchem Parameter die Meldung gehört.

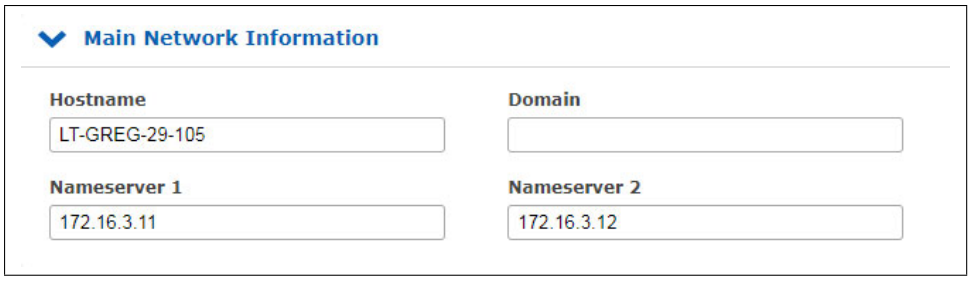
Erlaubte Zeichen und Sonderzeichen, mit denen Sie Dialogfelder ausfüllen können, finden Sie im Kapitel „Vor dem Start → Text- und Syntaxkonventionen“.

Zur Konfiguration der Systemfunktionen gehen Sie nun in das entsprechende Menü, das in einem der folgenden Kapiteln beschrieben wird.

10.1.2 Netzwerk



10.1.2.1 Netzwerk Informationen



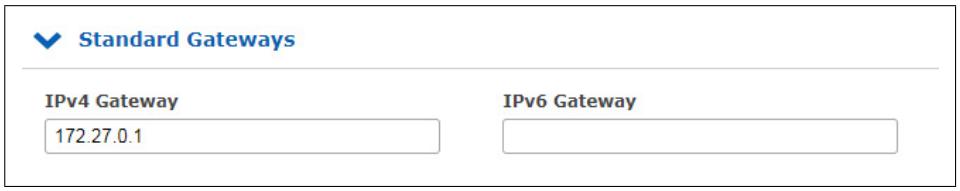
Hostname
Der Hostname des LANTIME ist ein eindeutiger Name eines Computers in einem Netzwerk. Jede im LANTIME konfigurierte IP-Adresse ist diesem Hostnamen zugeordnet.

Domain
Dieses Feld wird verwendet, um den Netzwerkdomain-Namen zu konfigurieren. Ein Netzwerkdomänenname ist ein textbasiertes Label, das leichter zu merken ist als die im Internetprotokoll verwendeten numerischen Adressen (z.B. meinberg.de).

Nameserver1
IP-Adresse des primären DNS-Servers im Netzwerk.
Der DNS-Server wird verwendet, um sowohl IP-Adressen als auch Hostnamen in einem Netzwerk aufzulösen.

Nameserver2
Hier kann ein alternativer Nameserver eingetragen werden.

10.1.2.2 Standard Gateways

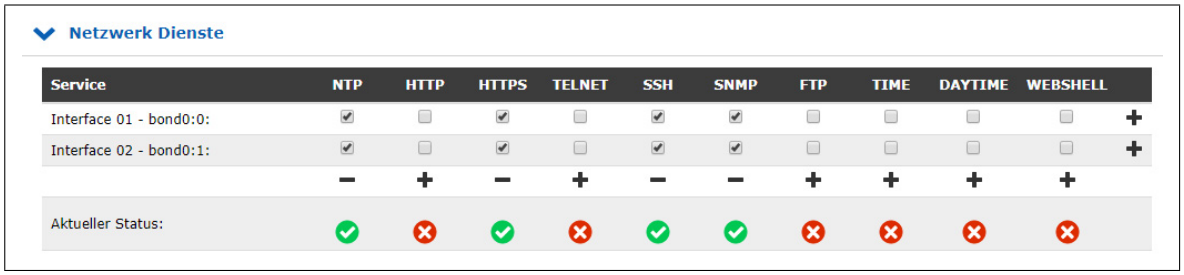


In diesem Menü können Sie Standardgateways konfigurieren, die für IPv4 und IPv6 verwendet werden. Für ein Standard-Gateway wird in der Hauptroutinentabelle eines LANTIME ein „default"-Eintrag angelegt. Wenn der LANTIME keine direkte Route oder Routingregel zu einer Ziel-IP hat, wird er immer versuchen, das Ziel über das Standard-Gateway zu erreichen.

IPv4 Gateway Konfiguration des standardmäßigen IPv4-Gateways.

IPv6 Gateway Konfiguration des standardmäßigen IPv6-Gateways.

10.1.2.3 Netzwerkdienste



In diesem Untermenü können Sie verschiedene Dienste für die vorhandenen virtuellen Netzwerkschnittstellen aktivieren oder deaktivieren. Mit den +/- Tasten können Sie ganze Zeilen oder Spalten in der Matrix markieren oder abwählen.

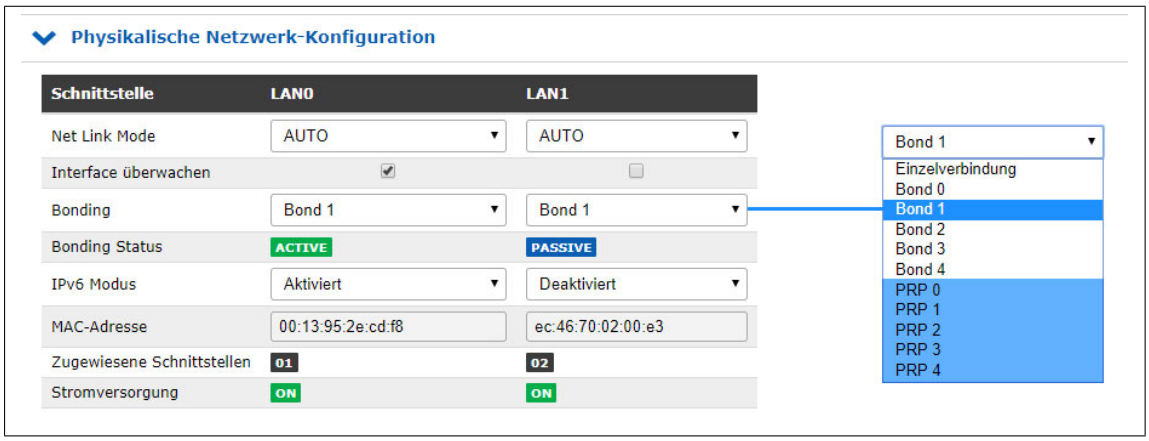
Die folgenden Service-Status sind möglich:

- Für mindestens eine virtuelle Schnittstelle wurde ein Dienst aktiviert und ist aktiv.
- Der Dienst wurde für keine virtuelle Schnittstelle aktiviert und wird daher gestoppt.

Die folgenden Dienste werden vom LANTIME unterstützt:

NTP: Network Time Protocol, UDP Port 123
HTTP: Hyper Transfer Protocol, TCP Port 80
HTTPS: Hyper Transfer Protocol Secure, TCP Port 443
TELNET: Teletype Network, TCP Port 23
SSH: Secure Shell, TCP Port 22
SNMP: Simple Network Management Protocol, UDP Port 161 / 162 (Traps)
FTP: File Transfer Protocol, TCP Port 20
TIME: Time Protocol, TCP/UDP Port 37
DAYTIME: UDP Port 13
FPC: Emuliert das Frontpanel-Display eines LANTIME und bildet ihn in einem Browser ab.
WEBSHELL: Melden Sie sich über einen Webbrowser an einer Befehlszeilenschnittstelle eines LANTIME an. WEBSHELL arbeitet auf Port 4200. Eingabe im Webbrowser: [IP/HOSTNAME]: 4200

10.1.2.4 Physikalische Netzwerkkonfiguration



Net Link Mode
Ermöglicht die Konfiguration des Netzwerkverbindungsmodus der Schnittstelle. Sie können zwischen den unterstützten Verbindungsmodi der jeweiligen physikalischen Schnittstelle wählen.

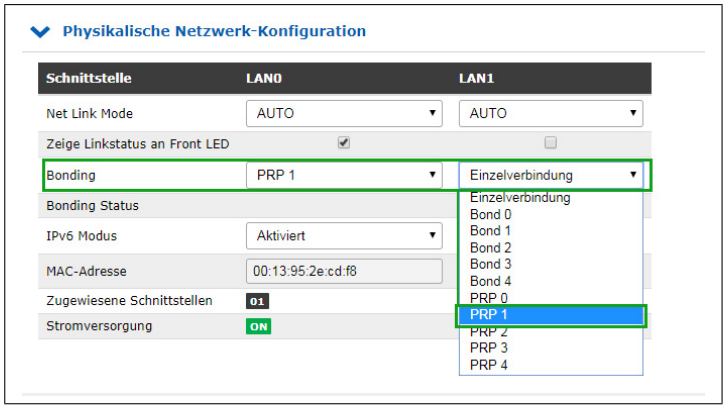
Der Standardwert AUTO (Autonegotiation) kann unter normalen Umständen unverändert bleiben. Autonegotiation bezieht sich auf ein Verfahren, das es zwei miteinander verbundenen Ethernet-Geräten ermöglicht, unabhängig voneinander die maximal mögliche Übertragungsgeschwindigkeit und das Duplexverfahren auszuhandeln und entsprechend zu konfigurieren.

Interface überwachen
Sobald einer der ausgewählten Netzwerkports keine Verbindung hat, wird dieser Status durch eine rote LED „Network“ auf der Frontplatte angezeigt und das Ereignis „Network Link Down“ gemeldet. Wenn an allen ausgewählten Ports eine Netzwerkverbindung verfügbar ist, leuchtet die LED „Network“ auf der Vorderseite grün.

Bonding
Hier können 2 oder mehr physikalische Netzwerkports zu einer Bonding-Gruppe zusammengefasst werden. Der LANTIME unterstützt die Bonding-Modi „Active - Backup“ und „LACP“. Der zu verwendende Modus kann im Submenü „Netzwerk → Sonstiges → Bonding-Modus“ ausgewählt werden. Weitere Informationen zur Funktionsweise der beiden Modi finden Sie im Submenü „Verschiedenes“.

PRP

PRP steht für Parallel Redundancy Protocol und ist seit 2010 in der Norm IEC 62439-3 definiert. PRP ist Layer-2-basiert und wurde für Computernetzwerke entwickelt, die eine zuverlässige Lösung in Bezug auf Hochverfügbarkeit und Betriebsfunktionalität benötigen. Ein LANTIME mit zwei oder mehr Schnittstellen und der Firmware 6.22.001 oder höher hat die Möglichkeit, als DAN zu fungieren („Dual Attached Node“ - ein Gerät, das an beide redundanten Netzwerke angeschlossen ist).



Ab der LANTIME-Firmware-Version 7.0 ist PRP auch bequem über das Webinterface-Menü „Netzwerk → Physikalische Netzwerk-Konfiguration“ einzustellen. Wählen Sie im Drop-Down-Menü „Bonding“ für mindestens zwei Schnittstellen die gleiche PRP-Gruppe aus.

IPv6 Modus

Aktivierung oder Deaktivierung des IPv6-Protokolls.

MAC Adresse

Media Access Control, zeigt die MAC-Adresse der angegebenen physikalischen Schnittstelle an.

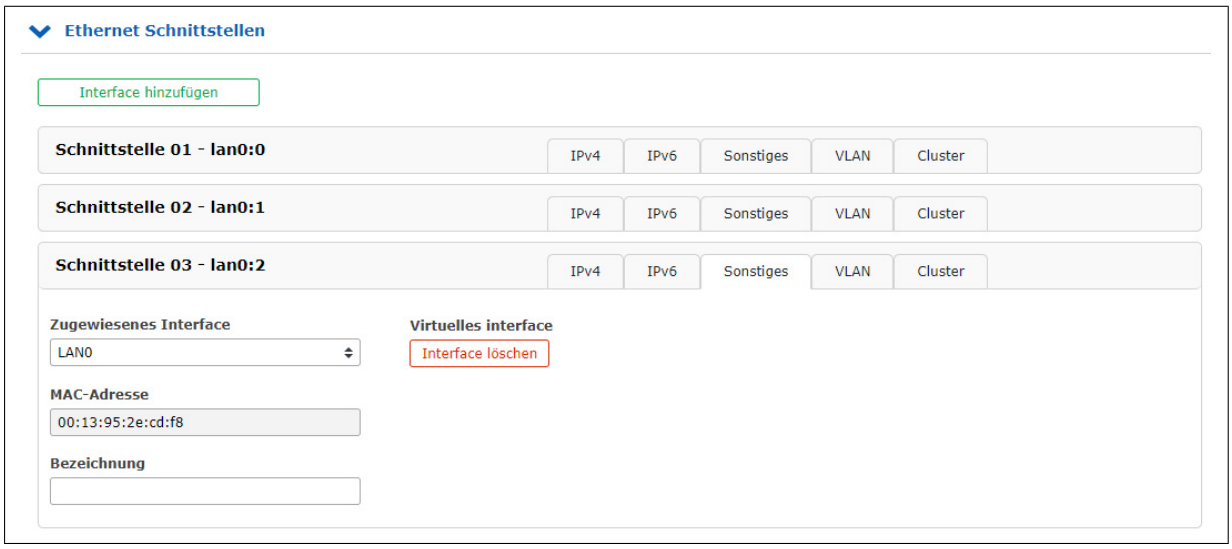
Zugewiesene Schnittstellen

Gibt an, welche virtuellen Schnittstellen der angegebenen physikalischen Schnittstelle zugeordnet sind.

Stromversorgung

Diese Funktion ist in IMS-Systemen verfügbar, in denen mehrere physikalische Schnittstellen verfügbar sein können. Der Port Power Status zeigt an, ob eine bestimmte physikalische Schnittstelle ein- oder ausgeschaltet ist.

10.1.2.5 Netzwerk-Schnittstellen



In diesem Menü werden die virtuellen Schnittstellen des LANTIME verwaltet. Jedem verfügbaren physikalischen Port können bis zu 99 virtuelle Schnittstellen zugeordnet werden. Der Name der virtuellen Schnittstelle besteht aus einer fortlaufenden Nummer der zugeordneten physikalischen Schnittstelle und der Nummer einer virtuellen Schnittstelle (beginnend mit Null).

Das obige Beispiel zeigt eine Konfiguration, in der der physikalischen Schnittstelle **LAN0** insgesamt drei virtuelle Schnittstellen zugeordnet sind, nämlich **lan0:0**, **lan0:1** und **lan0:2**.

Im Falle eines aktiven „Bonding“ wird die physikalische Schnittstelle durch den Namen der Bonding-Gruppe ersetzt, z.B. **bond0:0**.

Schnittstelle hinzufügen
Mit dieser Schaltfläche kann eine neue virtuelle Schnittstelle erstellt werden. Die neue virtuelle Schnittstelle ist standardmäßig dem physikalischen Port lan0 zugeordnet und wird am Ende der Eingabe dem gewünschten physikalischen Port zugewiesen. Die Zuordnung kann mit der Registerkarte „Sonstiges“ geändert werden.

Submenü IPv4:
In diesem Untermenü können die IPv4-Parameter konfiguriert oder die aktuelle Konfiguration des DHCP-Servers angezeigt werden.

TCP/IP Adresse: IPv4-Adresse der angegebenen Schnittstelle.

Netzmaske: Konfiguration der Subnetzmaske für die angegebene Schnittstelle.

Gateway: Konfiguration eines schnittstellenspezifischen Gateways. Diese Einstellung darf nur vorgenommen werden, wenn die IP der Schnittstelle NICHT im gleichen Subnetz wie das Standard-Gateway liegt und der netzwerkübergreifende Verkehr im Subnetz über das Gateway aktiviert werden soll.

DHCP-Client aktivieren: Mit dieser Einstellung kann ein DHCP-Client für die automatische Zuordnung der Netzwerkkonfiguration durch einen DHCP-Server aktiviert werden.

Submenü IPv6:
In diesem Menü können die IPv6-Parameter konfiguriert oder die von einem DHCP-Server vorgegebene Konfiguration angezeigt werden.

TCP/IP-Adresse: Ipv6-Adresse der angegebenen Schnittstelle

DHCP-Client aktivieren: Mit dieser Einstellung kann ein DHCPv6-Client für die automatische Zuordnung der Netzwerkkonfiguration durch einen DHCPv6-Server aktiviert werden.

Submenü Sonstiges:

Zugeordnete Schnittstelle: Legt fest, welches physikalische Netzwerk der aktuell ausgewählten virtuellen Schnittstelle zugeordnet ist.

„Virtuelles Interface“ Löschen-Button: Löscht die aktuell ausgewählte virtuelle Schnittstelle.

MAC-Adresse: Zeigt die MAC-Adresse des zugewiesenen physikalischen Netzwerkports an.

Label: Individuelle Textbeschreibung der Schnittstelle (Alias).

Submenü VLAN:
VLAN Option aktivieren: Aktivierung der getaggten VLAN-Funktion für die ausgewählte virtuelle Schnittstelle.

VLAN-Tag (0-4094): Hier können VLAN-Tags von 0-4094 eingegeben werden. Das ausgewählte Tag wird in den Datenbereich eines Ethernet-Pakets eingefügt.

Priorität: PCP (Priority Code Point). Legt die Priorität eines Ethernet-Frames fest. Die Prioritäten können zwischen einer niedrigen Priorität, Wert 1 und einer hohen Priorität, Wert 7, eingestellt werden.

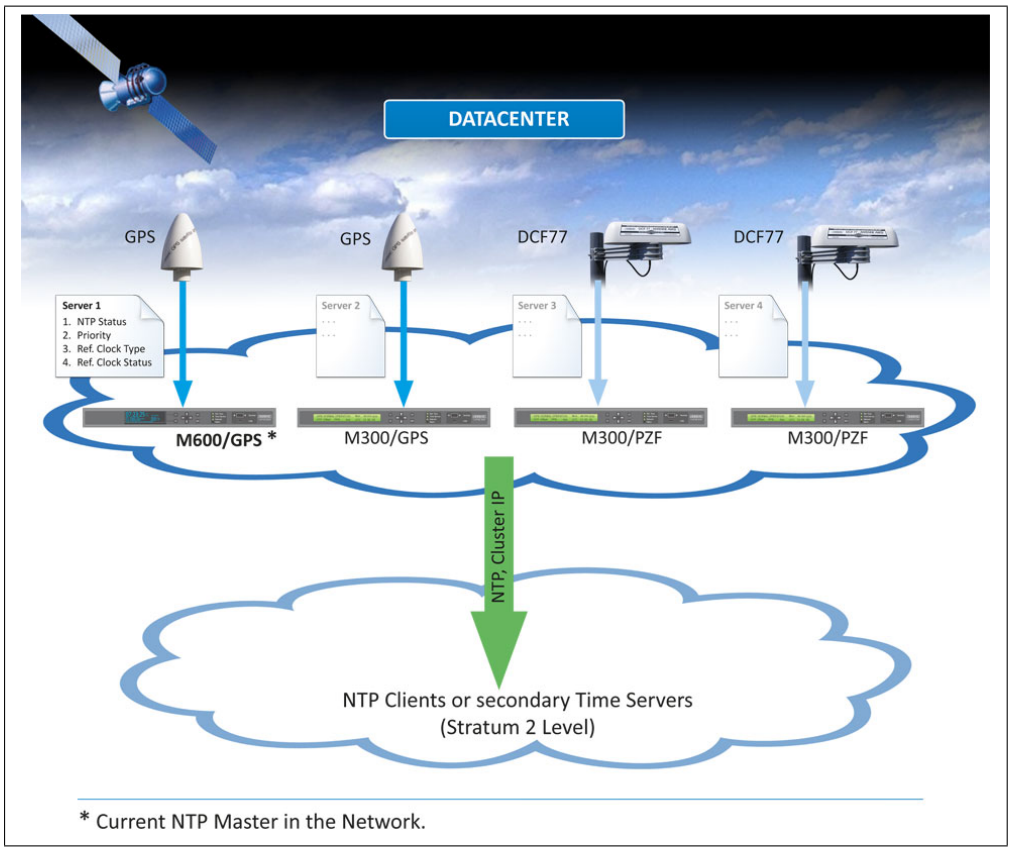
Der Prioritätswert 0 entspricht dem Best Effort.

Submenü Cluster:
Der Cluster-Modus ist ein Verfahren zur redundanten Zeitsynchronisation durch Gruppieren (Clustering) mehrerer LANTIME NTP-Server. Innerhalb dieser Gruppe tauschen die teilnehmenden NTP-Server kontinuierlich Status- und Qualitätsinformationen untereinander aus. Die Statusinformationen werden miteinander verglichen und durch einen speziellen Algorithmus wird entschieden, welcher der NTP-Server als aktueller MASTER im Netzwerk fungieren soll. Der Rest der Gruppe fungiert als SLAVE und bleibt als Backup passiv. Verliert der aktuelle Master seine Synchronisationsquelle oder tritt ein anderer Fehler auf, übernimmt ein anderer NTP-Server aus dem Cluster die Masterrolle. Der aktuelle Master antwortet auf Anfragen von NTP-Clients über eine gemeinsame Cluster-IP. Auch wenn der Master durch einen anderen NTP-Server ersetzt wird, ändert sich diese IP nicht.

Die Konfiguration eines NTP-Clusters ist sinnvoll, wenn seitens der NTP-Clients nur eine IP-Adresse für einen externen NTP-Server konfiguriert werden kann und auch noch Redundanz erforderlich ist.

Der aktuelle Master wird nach den folgenden Parametern in dieser Reihenfolge ausgewählt:

1. NTP-Status (sync, not sync);
2. Priorität (vom Benutzer konfigurierbar, der niedrigste Wert hat die höchste Priorität, Standard = 0);
3. Ref-Clock-Typ - GNSS-Empfänger wie GPS haben die höchste Bewertung;
4. Ref-Clock-Status (sync, not sync).



10.1.2.6 Cluster Konfiguration

Cluster-Option aktivieren: Über dieses Auswahlfeld kann die Clusterfunktion aktiviert werden.

Modus: Die Clustermitglieder können ihre Statusinformationen entweder über Multicast- oder Unicast-Meldungen austauschen. Für Multicast wird standardmäßig eine Cluster-Multicast-Adresse 239.192.0.1 verwendet. Diese Einstellung kann im Menü „Netzwerk → Sonstiges“ geändert werden. Zusätzlich kann dort der Netzwerkport, der für die Clusterkommunikation verwendet wird, geändert werden. Standardmäßig wird der Port 7000 für die Clusternachrichten verwendet.

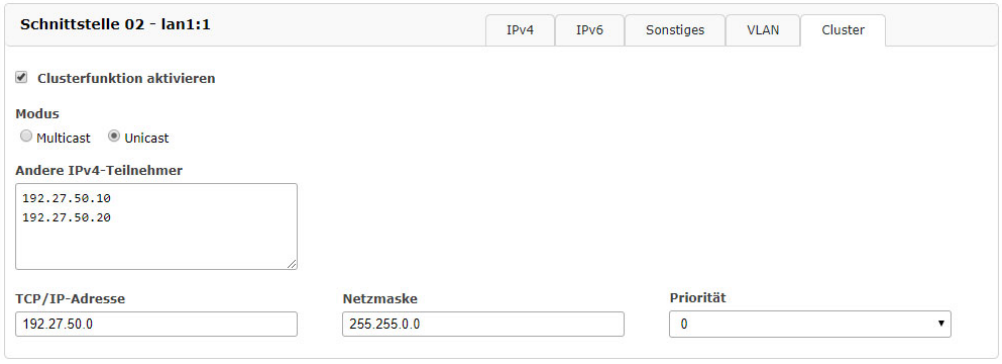
TCP/IP Adresse: IP-Adresse der NTP-Cluster-Schnittstelle. Für alle Clustermitglieder muss die gleiche Cluster-IP konfiguriert werden. Es wird empfohlen, eine Cluster-IP im gleichen Subnetz wie die entsprechende virtuelle Schnittstelle zu konfigurieren.

Netzmaske: Netzmaskenkonfiguration für die Cluster-Schnittstelle.

Priorität: Die hier eingestellte Priorität wird bei der Bestimmung des MASTERs durch den Clusteralgorithmus berücksichtigt. Der niedrigste Wert hat die höchste Priorität.

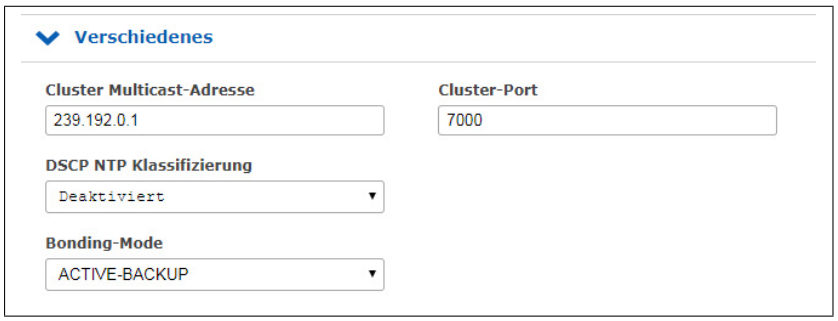
Beispielkonfiguration für einen Multicast Cluster:

Beispielkonfiguration für einen Unicast-Cluster:



Im Unicast-Cluster müssen die IP-Adressen der Clustermitglieder im Feld „Andere IPv4-Teilehmer“ eingetragen werden.

10.1.2.7 Verschiedenes



Cluster Multicast Adresse:
Konfiguration der Cluster-Multicast-Adresse. Über diese Adresse tauschen die LANTIME-Clustermitglieder ihre Statusmeldungen aus, wenn der Multicast-Modus aktiviert ist.

Cluster Port:
Konfiguration eines freien Netzwerkports für die Cluster-Kommunikation. Standardmäßig ist dieser Port auf 7000 eingestellt.

DSCP-NTP-Klassifikation:
DSCP = Differential Service Code Point. DSCP ist im Allgemeinen ein Verfahren zur Priorisierung des Datenverkehrs über IP. Im LANTIME ermöglicht diese Einstellung die Zuordnung der NTP-Pakete zu einer bestimmten Traffic-Klasse. Die Informationen über die Traffic-Klasse werden in einen Header eines IPv4-Pakets eingefügt. Router können diese Informationen auswerten und die NTP-Pakete wie priorisiert behandeln.

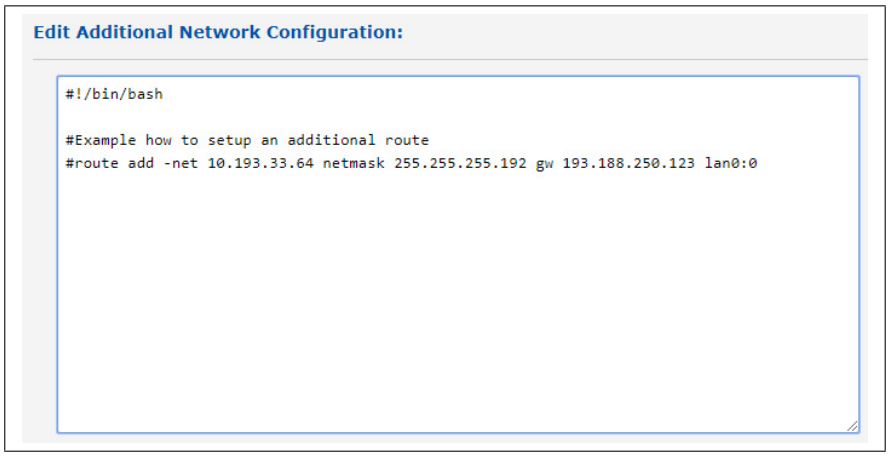
Bonding-Modus:
Im Menü „Netzwerk → Physikalische Netzwerkkonfiguration“ können zwei oder mehr physikalische Netzwerkports zu einer Bonding-Gruppe zusammengefasst werden. Der Bonding-Modus wird verwendet, um entweder den „ACTIVE BACKUP“ oder den „LACP“ Modus (Link Aggregation Control Protocol) zu konfigurieren, die vom LANTIME unterstützt werden.

ACTIVE-BACKUP:
Eine physikalische Schnittstelle in der Bonding-Gruppe wirkt wie ein „aktiver Slave“. Der gesamte Netzwerkverkehr eines LANTIME-Bond läuft über diese Schnittstelle. Die anderen physikalischen Schnittstellen in der Bonding-Gruppe sind passiv. Verliert die aktuell aktive Schnittstelle die Netzwerkverbindung, übernimmt die passive Schnittstelle nahtlos deren Funktion. Auch die MAC-Adresse des Netzwerkports bleibt unverändert.

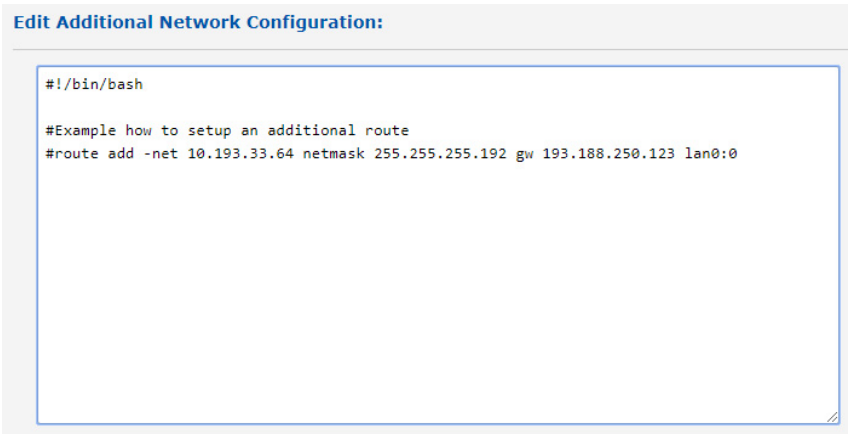
LACP:
LACP (802.3ad) ermöglicht eine Kombination mehrerer physikalischer Verbindungen zu einer logischen. Dies führt zu einer Lastverteilung und erhöht zusätzlich die Sicherheit im Fehlerfall im Vergleich zu „Active Backup“. Es ist wichtig, dass auch andere angeschlossene Netzwerkgeräte LACP unterstützen und die Netzwerkanschlüsse entsprechend konfiguriert sind.

10.1.2.8 Erweiterte Netzwerkeinstellungen

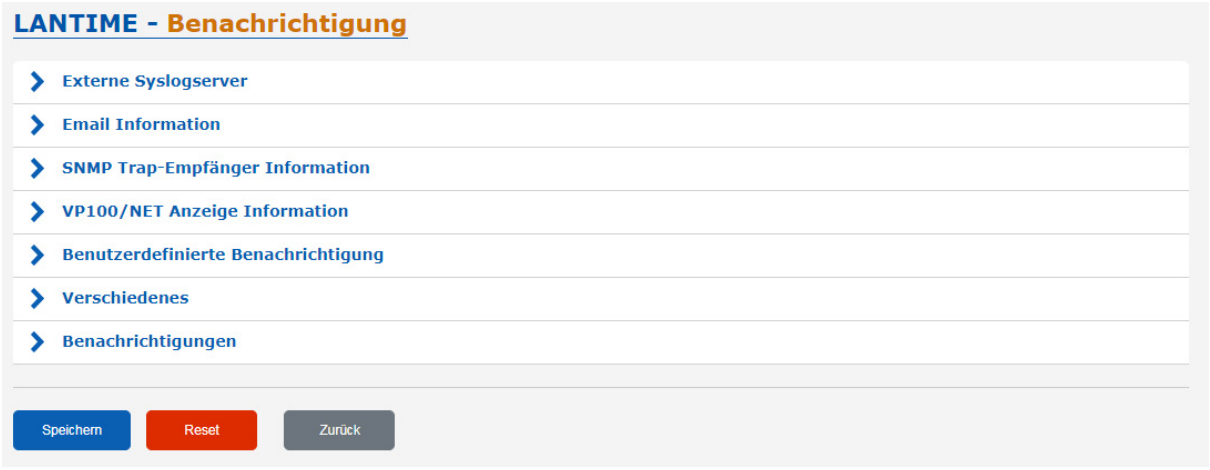
Die erweiterten Netzwerkeinstellungen sind aus Sicherheitsgründen nicht eingeschaltet. Die Funktion kann über eine SSH-Verbindung in der */etc/mbg/msc.cfg* mit dem Parameter „DISABLE SCRIPT“ nachträglich aktiviert / gesteuert werden.



In der erweiterten Netzwerkkonfiguration kann ein Bash-Skript bearbeitet werden, das bei jedem Neustart des LANTIME oder bei Änderungen der netzwerkbezogenen Konfiguration automatisch ausgeführt wird.

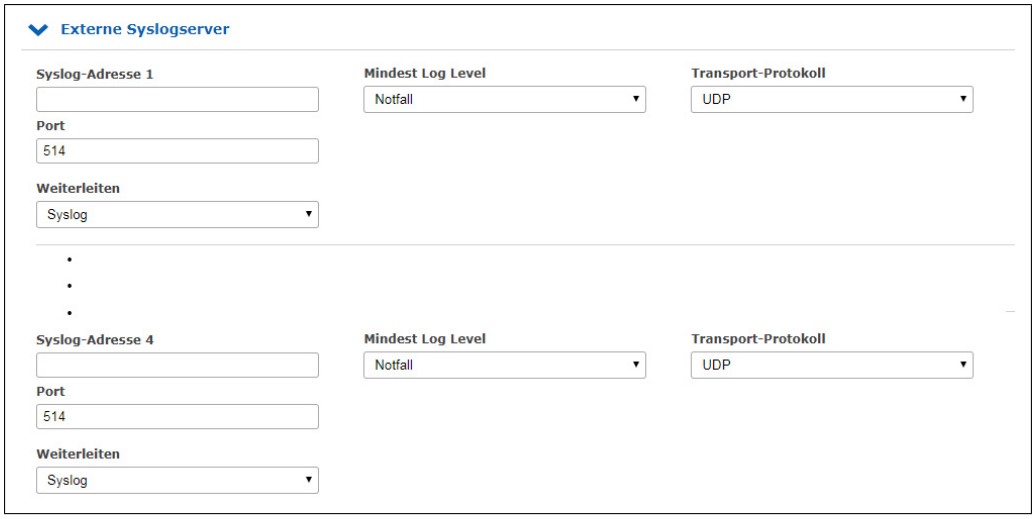


10.1.3 Benachrichtigung

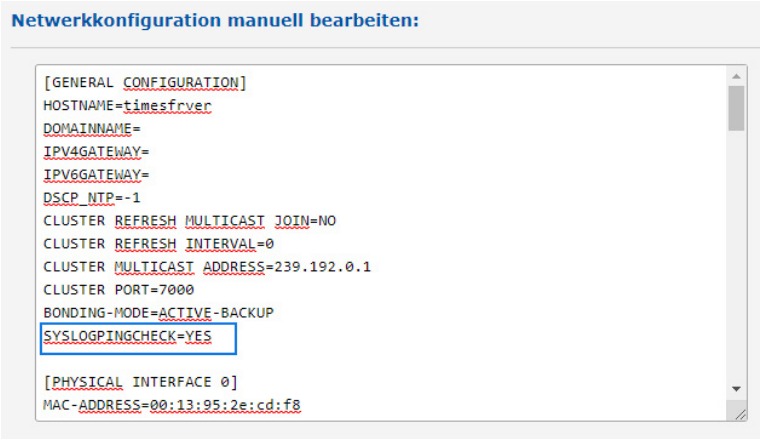


10.1.3.1 Externe Syslog-Server

Alle Informationen, die im LANTIME in SYSLOG (/var/log/messages) geschrieben werden, können auch an einen Remote-Server weitergeleitet werden.



Syslog-Adresse(n):
Sie können bis zu 4 externe Syslog-Server über das Webinterface eingeben. Standardmäßig wird die Erreichbarkeit des Syslog Servers über Ping/ICMP überprüft. Wenn der registrierte Syslog-Server nicht erreichbar ist, wird er nicht in die Syslog-Konfigurationsdatei */etc/syslog-ng/syslog-ng/syslog-ng.conf* eingetragen. Falls IMCP aufgrund von Firewall-Einschränkungen im Netzwerk nicht erlaubt ist, können Sie den Pingcheck über die manuelle Netzwerkkonfiguration ausschalten. Um fortzufahren, navigieren Sie wie unten beschrieben:



„System → Dienste und Funktionen → Manuelle Konfiguration → Netzwerk-Konfiguration“: Geben Sie für den Parameter „SYSLOGPINGCHECK“ den Wert „NO“ ein und speichern Sie die neuen Einstellungen.

Minimaler Log-Level:
Log-Level-Konfiguration

Transportprotokoll:
Transportprotokoll-Konfiguration:
UDP - verbindungslose Übertragung
TCP - verbindungsorientiert

Port:
Konfiguration des zu verwendenden Netzwerkanschlusses. Standardmäßig hat IANA den Port 514 für Syslog-Meldungen registriert.

Weiterleiten:

Syslog
Alles, was intern in der Datei /var/log/messages protokolliert wird, wird auch an den konfigurierten Syslog-Server gesendet (natürlich unter Berücksichtigung des konfigurierten Log-Levels).

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

Notification/Text
Nur die Ereignisse, die in der Ereignisliste unter „Benachrichtigungen → Benachrichtigungen“ aufgeführt sind, werden an den Syslog-Server gesendet.

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

Notification/Splunk
Wie bei „Notification/Text“, nur in einem anderen Format:

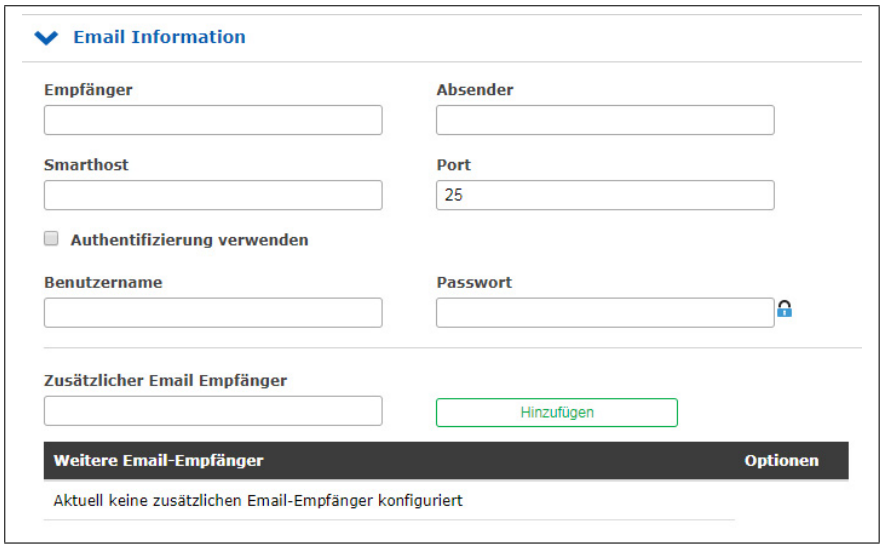
Format:
```
Mar 22 14:41:46 su-rims1-1 ext_syslog_cfg_splunk: msg_nr=20,
msg_name=Device Configuration Changed, msg_txt=, add_txt=
```

Notification/JSON
Wie bei „Notification/Text“, nur in einem anderen Format:

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„: “"}
```

10.1.3.2 E-Mail-Information

Der LANTIME ist in der Lage, über bestimmte Systemereignisse per E-Mail zu informieren. Im Menü „E-Mail-Informationen“ können Sie die notwendigen Einstellungen vornehmen. Im Untermenü „Benachrichtigungen“ können Sie die Systemereignisse auswählen, für die der LANTIME eine Benachrichtigungs-E-Mail versenden soll.



Empfänger: E-Mail des gewünschten Empfängers.

Absender: Adresse des Absenders.

Smarthost: Für den Versand der E-Mails benötigen Sie einen Smarthost (Relay-Server). Bitte geben Sie hier die Serveradresse ein.

Port: Konfiguration des Netzwerkports. Die Standardeinstellung ist 25, da das SMTP (Simple Mail Transfer Protocol) standardmäßig den TCP-Port 25 verwendet.

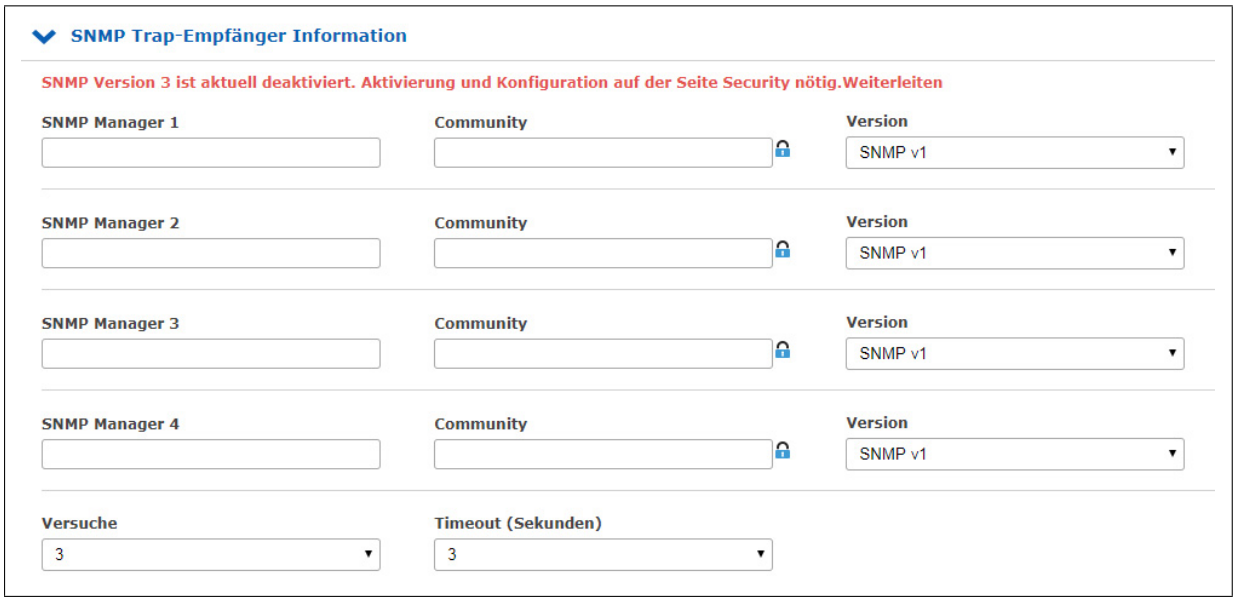
Authentifizierung verwenden (Checkbox): Viele Mailserver benötigen eine gültige Authentifizierung. Bitte markieren Sie das Kontrollkästchen, um sie zu aktivieren.

Benutzername/ Passwort: Bitte geben Sie einen gültigen Zugang für den E-Mail-Server ein.

Zusätzlicher Email Empfänger: Konfiguration zusätzlicher E-Mail-Empfänger.

10.1.3.3 SNMP-Trap-Empfänger

Der LANTIME ist in der Lage, mit Hilfe von SNMP-Traps über bestimmte Systemereignisse zu informieren. Im Menü „SNMP Trap Receiver“ können Sie bis zu 4 Trap-Empfänger konfigurieren. Im Untermenü „Benachrichtigungen“ können Sie die Systemereignisse auswählen, für die der LANTIME einen SNMP-Trap senden soll.



SNMP-Trap-Empfänger: IP-Adresse oder Hostname des SNMP-Trap-Empfängers.

Community: SNMP-Read-Community des Trap-Empfängers.

Version: SNMP-Version, die verwendet werden soll.

Anzahl der Wiederholungen: Gibt die Anzahl der Wiederholungen an, die ein LANTIME versucht einen Trap zu senden.

Timeout: Timeout-Wert für die Verbindungsdauer.

10.1.3.4 VP100/NET Display-Informationen

Das Meinberg VP100/20NET Netzwerkdisplay dient zur Anzeige von Uhrzeit und Datum. Dieses Display verfügt über eine integrierte Netzwerkkarte und einen SNTP-Client. Die Zeit wird von jedem NTP-Zeitserver über das NTP-Protokoll empfangen und damit die interne Uhr eingestellt. Diese Anzeige kann auch beliebige Zeichen als Lauftext anzeigen. Alle LANTIME-Alarmmeldungen können als Textnachrichten auf dem Display angezeigt werden. Im Untermenü „Benachrichtigungen“ können Sie die Systemereignisse auswählen, die vom LANTIME an die Anzeige gesendet werden sollen. Eine Meldung erscheint dreimal hintereinander als Lauftext auf dem Display.

Display: IP-Adresse der Netzwerkanzeige.

Serial number: Hier müssen Sie die korrekte Seriennummer des Displays eingeben.
Die Seriennummer wird angezeigt, wenn Sie die rote SET-Taste viermal drücken.

10.1.3.5 Alle Events in der Übersicht

Ereignis	Schweregrade (nach X.733)	Beschreibung
Normal Operation	Info	Zeigt den normalen Betrieb des LANTIME an
NTP Not Sync	Fehler	NTP-Dienst ist nicht synchron -> NTP-Nachrichten
NTP Sync	Info	Der NTP-Dienst wurde erfolgreich synchronisiert
NTP Stopped	Kritisch	NTP-Dienst gestoppt -> NTP-Nachrichten
NTP Offset Limit exceeded	Fehler	Maximaler NTP-Offsetwert wurde überschritten -> Sync Monitoring
NTP Offset Limit OK	Info	Maximaler NTP-Offset nicht überschritten -> Sync Monitoring
System Reboot	Aktion	Das System ist neu gestartet
CLK[NR] Not Responding	Kritisch	Empfängermodul reagiert nicht -> Referenzuhr-Nachrichten
CLK[NR] Not Sync	Fehler	Empfängermodul ist nicht synchron -> Referenzuhr-Nachrichten
CLK[NR] Sync	Info	Das Empfängermodul ist synchron zu seiner Zeitquelle
Antenna Faulty	Fehler	Keine Antenne oder kein ausreichendes Signal erkannt -> Referenzuhr-Nachrichten
Antenna Reconnect	Info	Antenne / Signal wurde vom LANTIME erkannt
Antenna Short Circuit	Fehler	Kurzschluss am Antennenanschluss -> Referenzuhr-Nachrichten

Tabelle: Alle Benachrichtigungs-Ereignisse

Ereignis	Schweregrade (nach X.733)	Beschreibung
Device Configuration Changed	Aktion	Die Softwarekonfiguration des LANTIME wurde geändert
Leap Second Announced	Info	Eine Schaltsekunde wurde angekündigt
SHS Time Limit OK	Info	Der eingestellte SHS-Zeitgrenzwert wurde nicht überschritten
SHS Time Limit Warnung	Warnung	Der eingestellte Schwellenwert für eine SHS Warnung wurde überschritten
SHS Time Limit Error	Kritisch	Der eingestellte Schwellenwert für einen SHS-Fehler wurde überschritten -> SHS-Konfiguration
Power Supply Failure	Kritisch	Fehler an einem Netzteil erkannt -> Sicherheit im laufenden Betrieb
Power Supply OK	Info	Betriebsbereites Netzteil
Power Consumption Overload	Kritisch	Überlastung des Netzteils/der Netzteile. Es sind nicht genügend Netzteile im Einsatz -> Redundante Stromversorgung
Power Consumption OK	Info	Die eingesetzten Netzteile liefern ausreichend Leistung für das System
Power Redundancy not guaranteed	Warnung	Bei Ausfall eines Netzteiles ist der weitere Betrieb nicht gewährleistet -> Redundante Stromversorgung
Power Redundancy activated	Info	Der Normalbetrieb ist auch nach dem Ausfall eines Netzteils gesichert
Sync Monitor	Aktion	Die Limits des Sync-Monitors wurden überschritten

Tabelle: Alle Benachrichtigungs-Ereignisse

Ereignis	Schweregrade (nach X.733)	Beschreibung
Sync Monitor Alert	Fehler	Fehlfunktion des SyncMon - überwachter Netzwerkknoten ist nicht erreichbar -> Error Logs
Sync Monitor OK	Info	Keine Störungen erkannt im Sync Monitor
MRS Source: Limit Exceed	Fehler	Eingestellte MRS-Grenzwerte wurden überschritten -> Referenzuhr-Nachrichten
MRS Source: No Signal	Warnung	Eine konfigurierte MRS-Zeitquelle ist nicht mehr verfügbar -> Referenzuhr-Nachrichten
MRS Source: Signal Detected	Info	Eine konfigurierte MRS-Zeitquelle ist verfügbar
MRS Source: Selected Signal Changed	Aktion	Die aktive MRS-Quelle hat sich geändert
MRS Source: Invalid Signal	Warnung	Eine konfigurierte MRS-Quelle liefert ein ungültiges Signal
MRS Source: Signal OK	Info	Die konfigurierte MRS-Quelle liefert ein korrektes Signal
FDM Error	Fehler	Die Abweichung der Zeit oder Frequenz der überwachten Netzleitung ist außerhalb der eingestellten Toleranz
FDM OK	Info	Die überwachte Netzfrequenz- und Zeitabweichung befindet sich im eingestellten Toleranzbereich
Network Link Down	Fehler	Keine Netzwerkverbindung an einem der LAN-Ports -> Netzwerk-Meldungen
Network Link Up	Info	Netzwerkverbindung am LAN-Anschluss erkannt
PTP Link Down	Fehler	Keine Netzwerkverbindung am PTP-Netzwerkanschluss

Tabelle: Alle Benachrichtigungs-Ereignisse

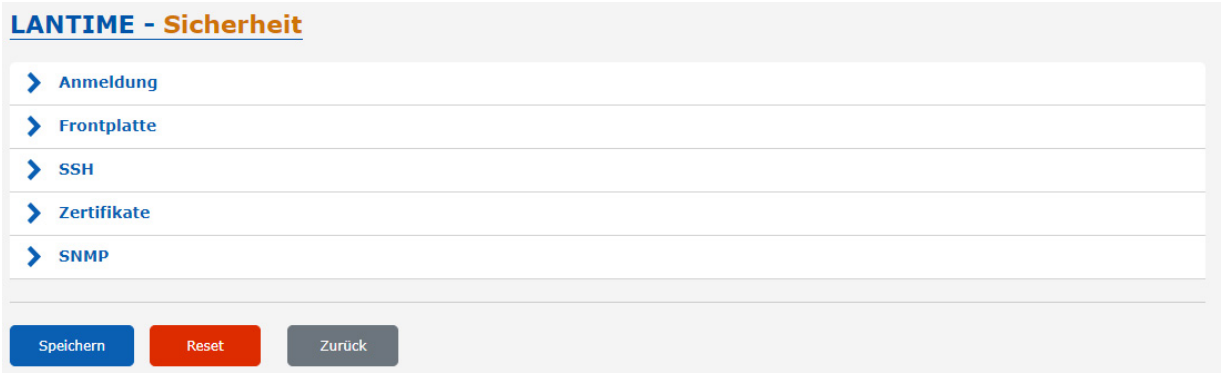
Ereignis	Schweregrade (nach X.733)	Beschreibung
PTP Link Up	Info	Netzwerkverbindung am PTP-Netzwerkanschluss erkannt
PTP State Changed	Info	Der aktuelle PTP-Status hat sich geändert
PTP Error	Fehler	Ein PTP-Fehler wurde erkannt -> ??
Low System Resources	Warnung	Geringe Systemressourcen erkannt
Sufficient System Resources	Info	Wiederhergestellte Systemressourcen
Fan Failure	Kritisch	Ein Fehler wurde bei einem Lüfter festgestellt -> Sonstige Meldungen
Fan OK	Info	Keine Fehler bei installierten Lüftern
Certificate Expired	Fehler	HTTPS-Zertifikat ist abgelaufen -> Zertifikate
HTTPS Certificate Expiration Warning (expiration in 90, 60 or 30 days)	Warnung	HTTPS-Zertifikat endet in 90, 60 oder 30 Tagen ab -> Zertifikate
Self-Signed Certificate In Use	Warnung	Das eingesetzte Zertifikat ist selbst signiert und kommt nicht von einer offiziellen Zertifizierungsstelle -> Zertifikate
Oscillator Adjusted	Info	Der interne Oszillator arbeitet stabil und ist justiert
Oscillator Not Adjusted	Warnung	Interner Oszillator ist nicht justiert -> Referenzuhr-Nachrichten
Cluster Master Changed	Info	Der Master eines LANTIME NTP-Clusters hat sich geändert -> Netzwerk

Tabelle: Alle Benachrichtigungs-Ereignisse

Ereignis	Schweregrade (nach X.733)	Beschreibung
Cluster Falseticker detected	Warnung	Ein NTP-Falseticker wurde in der Clusterverbindung erkannt
Cluster Falseticker cleared	Info	Zuvor erkannter Cluster-Falseticker ist wieder in Ordnung
IMS Error	Fehler	Es wurde ein Fehler in einem IMS-Modul festgestellt -> Sonstige Meldungen
IMS OK	Info	IMS-Modul ist fehlerfrei
Trusted Source OK	Info	Die als vertrauenswürdig ausgewählte Quelle befindet sich im eingestellten Offset-Bereich -> ??
Trusted Source Error	Fehler	Offset-Grenzwertverletzung der verwendeten vertrauenswürdigen Quelle -> ??
Sync-E Input Quality Level Changed	Info	Der Qualitätsfaktor der SyncE-Referenz hat sich geändert -> ??
ESI: ITU limits violated	Fehler	Überschreitung bzw. Unterschreitung der durch ITU-T festgelegten Empfehlungen -> ??
ESI: ITU limits adhered	Info	ITU-Grenzwerte werden eingehalten
Port Error	Error	z.B. Kurzschluss auf dem Eingang einer IMS-VSI-Referenzkarte
Port OK	Info	Signal am Port ist in Ordnung (die Karte muss das Port-Ereignis unterstützen - z.B. IMS-VSI)
Faillock: user banned	Aktion	Fehlgeschlagener Login - User wird temporär gesperrt

Tabelle: Alle Benachrichtigungs-Ereignisse

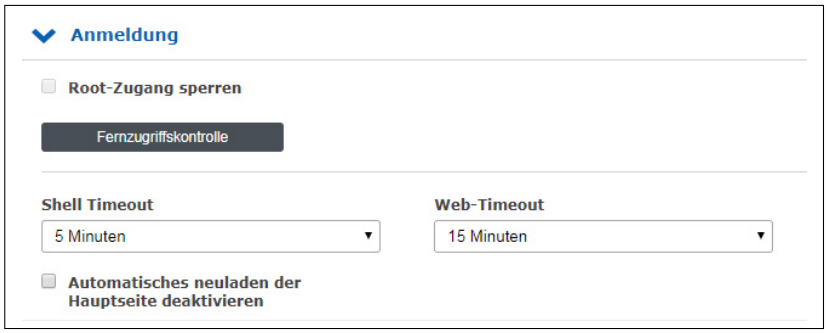
10.1.4 Sicherheit



Diese Seite ermöglicht die Konfiguration von Zugriffsbeschränkungen und **snmp**. Es bietet auch die Möglichkeit, SSH-Schlüssel und das HTTPS-Zertifikat zu erstellen.

Wenn Sie sich nicht sicher sind, welche Werte erforderlich sind, wenden Sie sich bitte an Ihren Netzwerk-Administrator.

Anmeldung
Im Menü „Anmeldung“ können Sie allgemeine Sicherheitseinstellungen für das Anmeldeverhalten des LANTIME vornehmen.



Root-Zugang sperren:
Diese Funktion kann nur von einem Admin-Benutzer oder einem Superuser aktiviert werden. Wenn diese Funktion aktiv ist, kann sich der „root“-Benutzer nicht mehr am LANTIME anmelden.

Fernzugriffskontrolle:
In dieser Konfigurationsdatei können Sie eine Zugriffskontrolle für die LANTIME-Webschnittstelle konfigurieren, die auf dem IP-Protokoll basiert. In dieser Datei können Sie die IP-Adressen eingeben, die für den Zugriff auf die Weboberfläche zugelassen werden sollen. Nach dem ersten Eintrag ist der Zugriff auf alle anderen Clients automatisch gesperrt. Es können einzelne Client-IPs oder ganze Subnetze konfiguriert werden.

Shell Timeout:
Definiert ein Timeout in Sekunden. Nach Ablauf dieser Frist ohne Benutzerinteraktion wird die aktuelle Sitzung auf der Kommandozeile für den angemeldeten Benutzer beendet.

Web-Timeout:
Der Parameter Web-Timeout definiert, wie viele Minuten Inaktivität vergehen können, bis ein Benutzer automatisch von der Weboberfläche abgemeldet wird.

Automatisches Neuladen der Hauptseite deaktivieren:
Verhindert das automatische Neuladen des Webinterfaces innerhalb 60 Sekunden, solange sich ein Benutzer im Hauptmenü vom LANTIME befindet.

Frontplatte:
Enthält allgemeine Sicherheitseinstellungen für das Frontpanel des LANTIME.

Frontplatte sperren:
Wenn die Funktion aktiviert ist, ist die Frontplatte eines LANTIME deaktiviert.

USB-Port deaktivieren:
Nach der Aktivierung dieser Funktion wird der USB-Anschluss eines LANTIME auf der Frontplatte deaktiviert und angeschlossene USB-Sticks können nicht erkannt werden.

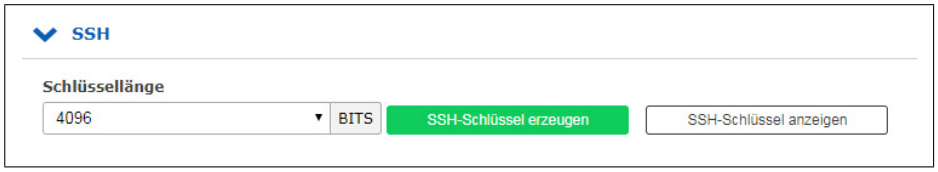
Checkbox „Eingespieltes USB-Backup als Startup-Konfiguration speichern“
Sie können eine vorher gesicherte Konfiguration über das USB-Stick-Menü auf Ihrem LANTIME aufspielen, wenn Sie dieses Kontrollkästchen aktiviert haben, wird die hochgeladenen Konfiguration direkt als Startkonfiguration übernommen.

Checkbox „Installierte Firmware via USB als Startup aktivieren“
Durch die Aktivierung dieser Checkbox wird eine Firmware-Version, die über das USB-Menü auf dem LANTIME geladen wurde, direkt als aktive Firmware übernommen.

Siehe auch ??.

10.1.4.1 SSH - Secure Shell

Über „Secure Shell Login“ (SSH) ist es möglich, eine gesicherte Verbindung zum LANTIME herzustellen. Alle Daten werden bei der Übertragung über Ethernet verschlüsselt. Um diesen Dienst nutzen zu können, muss SSH auf jeder Schnittstelle in den Netzwerkeinstellungen aktiviert sein (siehe auch das Konfigurationskapitel Netzwerkdienste). „Web GUI [rightarrow]] Netzwerk → Netzwerkdienste“).

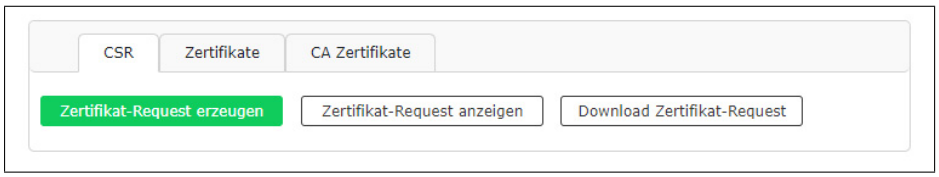


Länge des Keys (Bits):
Legt die Schlüssellänge für einen neuen zu generierenden Schlüssel fest.

Generierung eines SSH-Keys:
Erzeugt ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, in konfigurierbarer Länge.

Zeige SSH-Key:
Mit dieser Schaltfläche können Sie die öffentlichen SSH-Schlüssel eines LANTIME anzeigen.

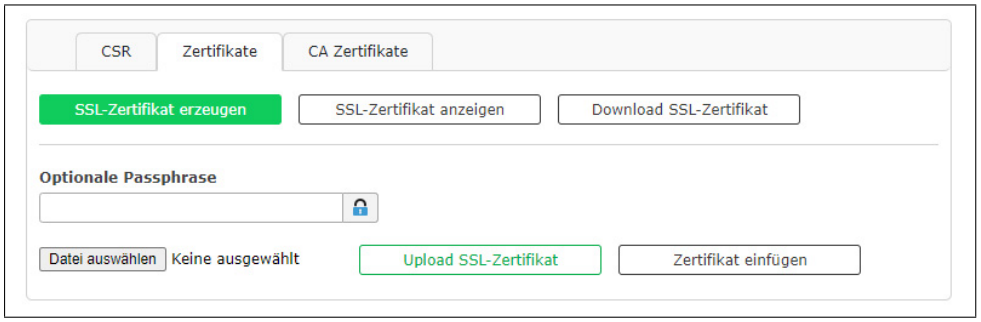
10.1.4.2 Zertifikate



HTTPS ist ein Standard für die verschlüsselte Übertragung von Daten zwischen Webbrowser und Webserver. Sie basiert auf X.509-Zertifikaten und asymmetrischen Krypto-Verfahren. Der Zeitserver verwendet diese Zertifikate um sich bei einem Client (Webbrowser) zu authentifizieren. Wenn sich ein Webbrowser zum ersten Mal mit dem HTTPS-Webserver Ihres LANTIME verbindet, werden Sie aufgefordert, das Zertifikat des Webservers zu akzeptieren.

Um sicherzustellen, dass Sie mit Ihrem bekannten Zeitserver kommunizieren, überprüfen Sie das Zertifikat und akzeptieren Sie es, wenn es mit dem im LANTIME gespeicherten übereinstimmt. Alle weiteren Verbindungen vergleichen das Zertifikat mit dem, welches in Ihrer Webbrowser-Konfiguration gespeichert ist. Anschließend werden Sie aufgefordert, das Zertifikat nur dann zu überprüfen, wenn es geändert wird.

Hinweis: Standardmäßig ist im LANTIME ein selbstsigniertes Zertifikat installiert, das nicht von einer Certificate-Authority (CA) signiert ist. Daher geben einige Webbrowser an, dass die Verbindung nicht sicher ist. Wenn Sie ein Zertifikat installieren möchten, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, können Sie die Schaltfläche „SSL-Zertifikat hochladen“ verwenden. Weitere Details dazu finden Sie in den folgenden Anweisungen.



SSL-Zertifikat generieren:
Ermöglicht die Erstellung eines neuen selbstsignierten SSL-Zertifikats.

SSL-Zertifikat anzeigen:
Überprüfen Sie das aktuell installierte SSL-Zertifikat.

Download SSL-Zertifikat:
Ermöglicht das Herunterladen des aktuell installierten SSL-Zertifikats.

Optionale Passphrase
Ist der privater Schlüssel des SSL-Zertifikats mit einem Passwort geschützt, dann müssen Sie hier die „Passphrase“ eingeben. Der Webserver kann ansonsten nicht automatisch starten, da er den hochgeladenen Schlüssel nicht entschlüsseln kann.

SSL-Zertifikat hochladen:
Ermöglicht das Hochladen eines Zertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde. Dieses Zertifikat muss im PEM-Dateiformat vorliegen.

Zertifikatsanforderung generieren:
Die Funktion „Zertifikat-Request erzeugen“ ermöglicht das Erstellen einer Certificate-Signing-Request (CSR), die an eine Zertifizierungsstelle gesendet werden kann, um ein signiertes Zertifikat zu beantragen. Auf dem LANTIME wird dadurch ein Zertifikat und ein privater Schlüssel angelegt. Der Speicherort für die CSR ist *„/mnt/flash/data/https.req“*, der passende Schlüssel wird unter *„/mnt/flash/data/https.req.pk“* abgelegt.

Antragsteller (SAN - Subject Alternative Name)
Im Feld „Antragsteller (SAN)“ können Sie zusätzliche Hostnamen (Sites, IP-Adressen, Common Names usw.) angeben, die durch ein einzelnes SSL-Zertifikat, z. B. ein Multi-Domain-Zertifikat, geschützt werden sollen. Mehrere SANs müssen als eine komma-separierte Liste eingetragen werden.

Hinweis:
Wenn Sie das bei der Zertifizierungsstelle eingereichte Zertifikat über den LANTIME und die Funktion „Zertifikat-Request erzeugen“ generiert haben, dann ist der passende Schlüssel für dieses Zertifikat bereits unter *„/mnt/flash/data/https.req.pk“* abgelegt. Nach dem Hochladen des signierten Zertifikates wird dieser zuvor erzeugte private Schlüssel verwendet.

Wenn das eingereichte und signierte Zertifikat nicht auf dem LANTIME erzeugt wurde, dann muss die PEM-Datei den privaten Schlüssel und das Zertifikat selbst enthalten.

Der Inhalt des privaten Schlüssels beginnt mit:
„—BEGIN RSA PRIVATE KEY—“
und endet mit
„—END RSA PRIVATE KEY—“

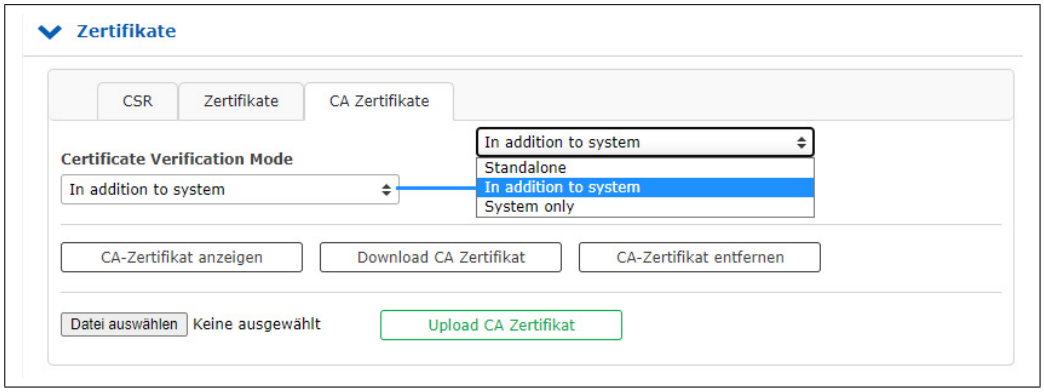
das Zertifikat selbst beginnt mit
„—BEGIN CERTIFICATE—“
und endet mit
„—END CERTIFICATE—“.

Dieses Beispiel ist ein Auszug aus einer PEM-Datei:

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

10.1.4.3 CA Zertifikate

Die Funktionen in dem Menü „Sicherheit → Zertifikate → CA Zertifikate“ können genutzt werden, um eine eigene, nicht öffentliche Wurzelzertifizierungsstelle dem LANTIME hinzuzufügen. Dadurch können Programme und Dienste die eine TLS-Verbindung aufbauen, wie z.B. der LDAP-Dienst, den angefragten Server eindeutig identifizieren, obwohl kein (meist kostenpflichtiges) Zertifikat einer öffentlichen Zertifizierungsstelle genutzt wird.



Der Certificate Verification Mode kann wie folgt gewählt werden:

Standalone: Der LANTIME nutzt ausschließlich das hochgeladene eigene Wurzelzertifikat um Verbindungen zu verifizieren.

In addition to system: Der LANTIME nutzt das hochgeladene eigene Wurzelzertifikat sowie die systembekannten öffentlichen Zertifizierungsstellenzertifikate.

System only: Der LANTIME nutzt die systembekannten öffentlichen Zertifizierungsstellenzertifikate.

10.1.4.4 Hochladen von signierten mehrstufigen/verketteten Zertifikaten

Die folgenden Schritte erfordern einen SSH-Zugang zu Ihrem Zeitserver.

Neben SSL-Zertifikaten werden auch mehrstufige/verkettete Zertifikate unterstützt. Die Zertifikatskette wird in einer eigenen Datei (*„/etc/https_ca.pem“*) gespeichert, die wie das Webserverzertifikat und der private Schlüssel im PEM-Format vorliegen muss. Die Zertifikatsketten-Datei enthält die Zertifikate, die jeweils, wie oben gezeigt, durch die Zeilen BEGIN und END CERTIFICATE eingeschlossen sind.

Die mehrstufigen/verketteten Zertifikate können nur über die Kommandozeile bzw. einen File Transfer eingespielt werden. Nachdem diese Zertifikate gespeichert wurden, muss der Webserver mit dem Befehl **„restart https“** neu gestartet werden, um die Änderungen zu übernehmen. Durch das Ausführen des Befehls **„saveconfig“** werden die Einstellungen dauerhaft gespeichert.

Alternativ erscheint im Webinterface das gelbe Banner, welches eine geänderte Konfiguration signalisiert. Durch einen Klick auf **„Jetzt als Startkonfiguration speichern“** kann ebenfalls die Änderungen persistent übernommen werden.

Durch das Hinzufügen der Zwischenzertifikate über die *„/etc/https_ca.pem“* wird der automatische Update-Prozess bei späteren Firmware-Updates nicht beeinträchtigt. Somit werden neue/eingeschränkte „cipher-suites“ automatisch übernommen.

10.1.4.5 SNMP

Das Simple Network Management Protocol (SNMP) wird in Netzwerkmanagementsystemen zur Statusüberwachung von Geräten eingesetzt. SNMP arbeitet mit der Abfrage von „Objekten". Über ein solches Objekt können wir Informationen über ein Netzwerkgerät sammeln. Die sogenannte Management Information Base (MIB) ist eine Datei, die alle Objekte enthält, die über SNMP verwaltet werden können.

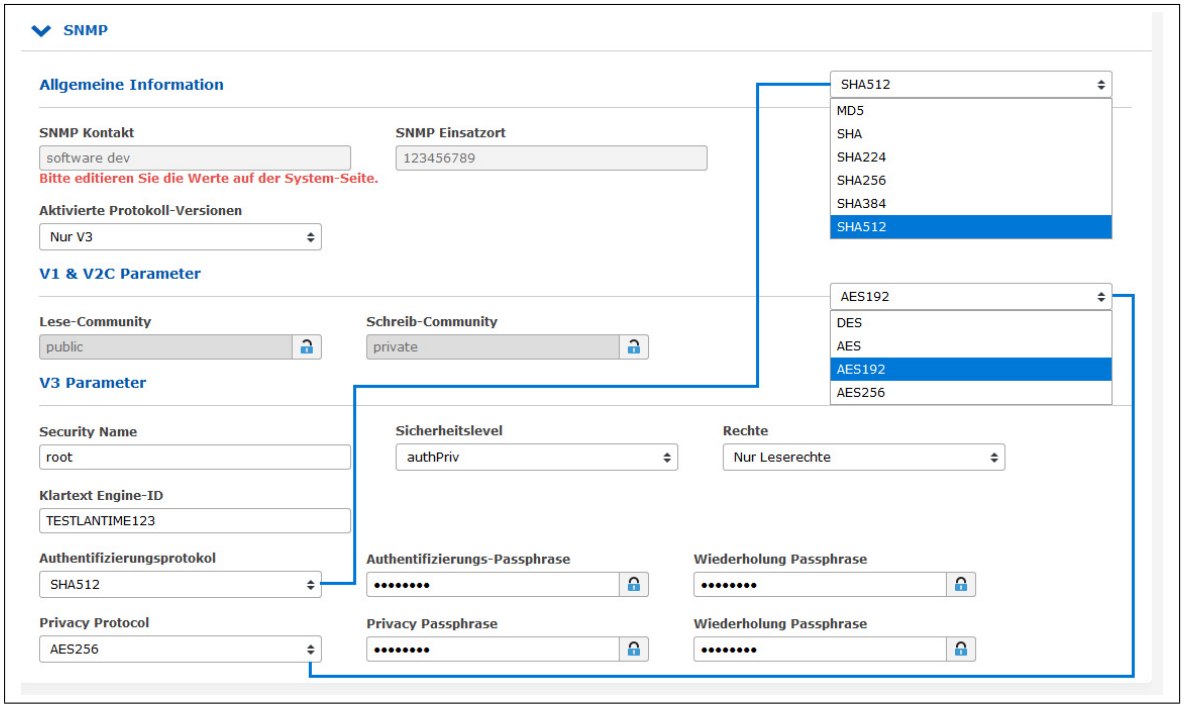
Die Meinberg SNMP-MIB-Dateien können auf der Seite „System → Dienste und Funktionen → SNMP MIB" heruntergeladen werden. Die Dateien „MBG-SNMP-ROOT-MIB.mib" und „MBG-LANTIME-NG-MIB.mib" müssen zur Überwachung eines LANTIME-Systems verwendet werden.

(siehe auch Kapitel „Das Webinterface → System → Dienste und Funktionen").

Standardmäßig ist der SNMP-Dienst auf einem LANTIME-System nicht aktiviert. Der Dienst kann auf jeder Schnittstelle auf der Seite „Netzwerk → Netzwerkdienste" aktiviert werden.

(siehe auch Kapitel „Das Webinterface → Netzwerk → Netzwerkdienste")

Im Folgenden werden die verschiedenen SNMP-Konfigurationsparameter beschrieben:



Aktivierte Protokoll-Versionen:
Konfiguration der SNMP-Protokollversion. Die folgenden Optionen können ausgewählt werden: „Nur V1/V2", „Nur V3", „V1/V2/V3".

V1/V2 Parameter

Lese-Community:
Die Read-Community wird nur für die SNMP-Versionen V1 und V2 verwendet. Es ist wie eine Benutzerkennung oder ein Passwort, das den Zugriff auf die LANTIME SNMP-Objekte ermöglicht. Das SNMP-Überwachungssystem sendet den gelesenen Community-String zusammen mit allen SNMP-Anfragen. Wenn der Community-String korrekt ist, antwortet der LANTIME mit den angeforderten Informationen. Wenn der Community-String falsch ist, verwirft der LANTIME einfach die Anfrage und antwortet nicht.

Schreib-Community:
Die Write-Community wird nur für die SNMP-Versionen V1 und V2 verwendet. Es ist wie eine Benutzerkennung oder ein Passwort, das den Zugriff auf die LANTIME SNMP-Objekte ermöglicht. Das SNMP-Monitoring-System sendet die Write-Community-Zeichenkette zusammen mit allen SNMP-SET-Befehlen. Wenn der Community-String korrekt ist, wird der Befehl SNMP-SET ausgeführt. Wenn der Community-String falsch ist, wird der Befehl SNMP-SET nicht ausgeführt.

V3 Parameter

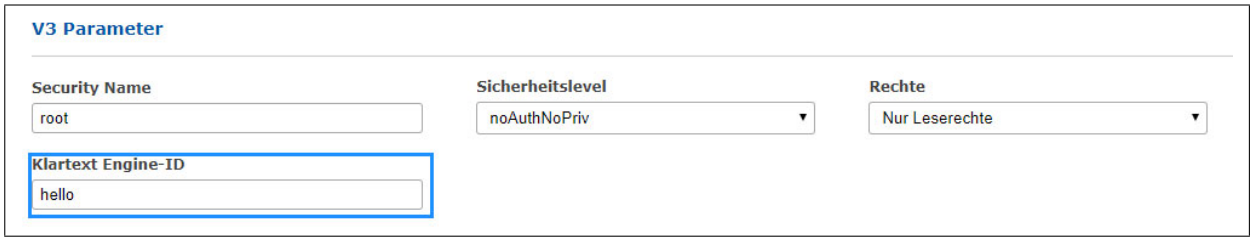
Security Name:
SNMP V3 Benutzername

Sicherheitslevel:
Nachrichten können unauthentifiziert, authentifiziert oder authentifiziert und verschlüsselt gesendet werden, indem die zu verwendende Sicherheitsstufe festgelegt wird:

noAuthnoPriv - unauthentifiziert und unverschlüsselt
authNoPriv - authentifiziert und unverschlüsselt
authPriv - authentifiziert und verschlüsselt

Klartext Engine-ID:
Innerhalb einer administrativen Domäne ist eine SNMP V3 Engine ID eine eindeutige Kennung einer SNMP-Engine. Hier kann eine Zeichenkette mit maximal 27 Zeichen eingegeben werden. Die Zeichenkette wird verwendet, um die hex engineID unter Verwendung des in RFC3411 beschriebenen Textformatschemas zu erzeugen. Wenn z.B. der String „hello“ als engineID konfiguriert ist, wäre die generierte hex engineID 800015dd0468656c6c6c6f.

- 15dd ist die hexadezimale Darstellung der Meinberg Unternehmens-ID 5597.
- 04 ist ein Indikator dafür, dass das Textformatschema verwendet wird, um die Engine-ID zu generieren.
- 68656c6c6c6f ist die hexadezimale Darstellung der Zeichenkette „hello“.



Rechte:
Konfiguration der Zugriffsebene (Lesezugriff oder Lese-/Schreibzugriff).

Authentifizierungsprotokoll:
Die für die Authentifizierung verwendeten Protokolle sind MD5 und SHA (Secure Hash Algorithm):

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

Authentifizierungs-Passphrase:
Benutzerpassphrase, die mindestens 8 Zeichen lang sein muss.

Datenschutzprotokoll:
Die für die Verschlüsselung verwendeten Protokolle sind DES (Data Encryption Standard) und AES (Advanced Encryption Standard):

- DES
- AES
- AES192
- AES256

Datenschutz-Passphrase:
Eine Passphrase, die beim Verschlüsseln von Paketen verwendet wird. Sie muss mindestens 8 Zeichen lang sein.

10.1.4.6 SHS-Konfiguration

SHS ist die Abkürzung für Secure Hybrid System und ist auf LANTIME-Systemen mit zwei Referenzuhren verfügbar. Wenn der SHS-Modus aktiviert ist, wird nur die aktuell aktive Uhr zum Weiterleiten des Zeitsignals an den NTP-Dienst verwendet, die andere Uhr wird als „nicht ausgewählt“ angezeigt und nur zum Messen und Vergleichen einer Zeitdifferenz zwischen beiden Empfängern verwendet.

In dieser Hinsicht unterscheidet sich SHS von einem redundanten Modus. Im redundanten Modus schaltet eine Schalteinheit je nach Verfügbarkeit und Synchronisationsstatus zwischen der einen und der anderen Uhr um und der aktive Empfänger übergibt das Zeitsignal an den NTP-Dienst.

Der SHS-Modus sorgt für einen sicheren Betrieb und tritt in Aktion, wenn eine Zeitdifferenz zwischen beiden Empfängern ein konfigurierbares Zeitlimit überschreitet.

In diesem Fall werden Alarme ausgelöst und über konfigurierte Benachrichtigungskanäle (z.B. SNMP-Trap, E-Mail, Syslog-Nachricht) gesendet. Außerdem sollte der NTP auch in diesem Fall gestoppt werden, um den sicheren Betrieb des Zeitmessdienstes zu unterstützen. Deshalb müssen Sie in diesem Schritt „NTP-Dienst bei Zeitlimitfehler stoppen“ wählen.

Andererseits wird bei IMS-Systemen mit zwei Referenzuhren das von den Empfängern kommende Zeitsignal mit einer RSC-Karte (Redundant Switch Control Unit) kontinuierlich gemessen und miteinander verglichen. Die Messungen werden an den SHS-Modus weitergeleitet, wenn dieser aktiviert ist. Ähnlich wie bei LANTIME-Systemen mit SHS können die Alarme ausgelöst werden, wenn eine Differenz der beiden Signale die konfigurierten Zeitbegrenzungseinstellungen überschreitet und der NTP-Dienst zum Stoppen konfiguriert sein sollte.

SHS-Modus
Der SHS-Modus kann über dieses Auswahlfeld selektiv aktiviert oder deaktiviert werden. Wenn der SHS-Modus deaktiviert ist, findet kein Zeitvergleich statt und die Zeiten beider Empfänger werden direkt an den NTP-Dienst übertragen. Der NTP-Dienst entscheidet dann selbstständig, welche Zeit für die Synchronisation verwendet wird (redundanter Modus).

Time Limit Warning Level
Überschreitet die berechnete Zeitdifferenz zwischen den beiden Referenzuhren den konfigurierten Wert, erzeugt der LANTIME einen Alarm „SHS Time Limit Warning“. Dieser Alarm kann per E-Mail oder SNMP-Trap gesendet werden, wenn er in den Benachrichtigungseinstellungen entsprechend konfiguriert ist.

(Siehe auch Konfigurationskapitel „Das Webinterface → Benachrichtigung → E-Mail-Information“)

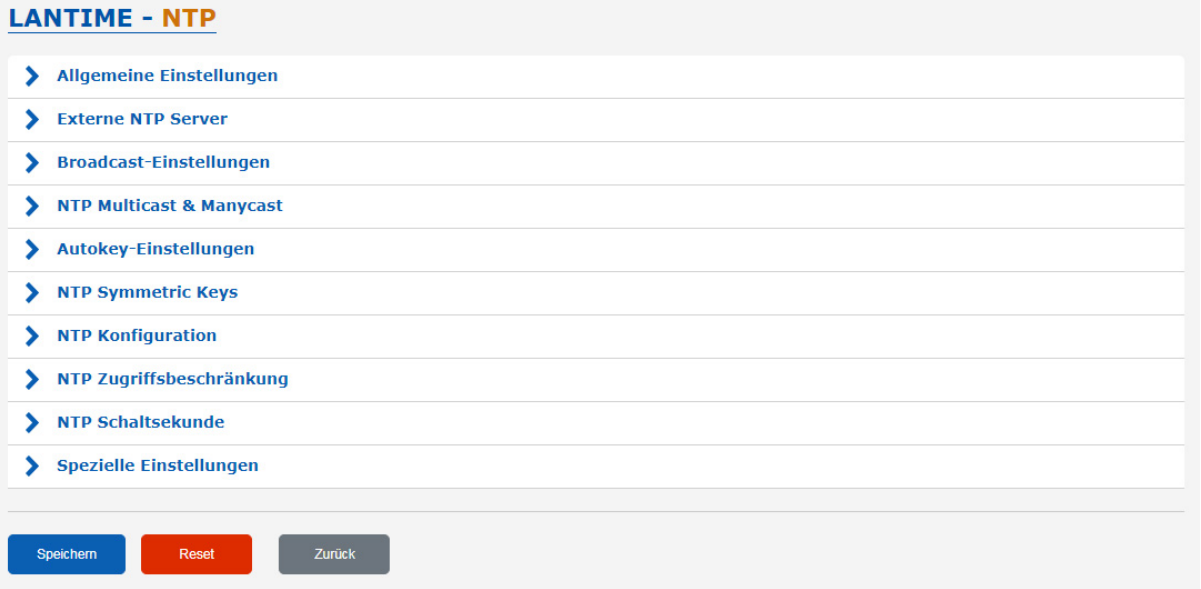
Bei LANTIME IMS-Systemen mit eingebauter RSC wird der Parameter in Nanosekunden konfiguriert. Für Systeme ohne RSC in Millisekunden.

Time Limit Error-Level (ms)
Überschreitet die berechnete Zeitdifferenz zwischen den beiden Referenzuhren den konfigurierten Wert, erzeugt der LANTIME einen Alarm „SHS Time Limit Warnung“. Dieser Alarm kann per E-Mail oder SNMP-Trap gesendet werden, wenn er in den Benachrichtigungseinstellungen entsprechend konfiguriert ist.

Bei LANTIME IMS-Systemen mit eingebauter RSC wird der Parameter in Nanosekunden konfiguriert. Für Systeme ohne RSC in Millisekunden.

NTP-Dienst bei Zeitlimitfehler stoppen
Hier können Sie entscheiden, ob der NTP-Dienst mit dem kritischen „TimeLimitError“ beendet werden soll. In diesem Fall würde ein anfragender NTP-Client keine Antwort mehr vom Zeitserver erhalten.

10.1.5 NTP



Auf der Seite NTP-Konfiguration werden die zusätzlichen NTP-Parameter eingerichtet, die für einen spezifizierten Betrieb des NTP-Subsystems erforderlich sind.

10.1.5.1 Allgemeine Einstellungen

Stratum-Level wenn nicht synchron
Der Stratum-Level für NTP bezieht sich auf einen „Abstand" zu einer Referenzquelle und nicht auf die Genauigkeit. So hat beispielsweise ein Zeitserver mit einer internen Referenz wie GPS oder DCF77 intern einen „Level 0" und wird von einem externen Netzwerk als „Level 1" betrachtet. Mit der Einstellung „Stratum Level wenn nicht synchron" wird der Stratum-Wert konfiguriert, mit dem sich der Server im Netzwerk präsentiert, wenn keine Referenzzeitquelle verfügbar ist. Dieser Wert wird erst wirksam, wenn die konfigurierte NTP-Trustime für den internen Referenztakt abgelaufen ist und keine weiteren Zeitquellen wie z.B. externe NTP-Server zur Verfügung stehen.

Stratumwechsel deaktivieren
Durch die Aktivierung dieser Betriebsart präsentiert sich der Server immer (auch asynchron) als Stratum 1-Server im Netzwerk. Die Einstellung bei „Stratum-Level wenn nicht synchron" ist nicht mehr wirksam.

Beispiele:

a) Ein LANTIME, der mit seiner internen Referenzuhr wie GPS oder DCF77 synchronisiert wird, fungiert als Stratum 1 NTP-Server. Wenn die Funktion „Stratumwechsel deaktivieren" aktiv ist, fungiert der NTP-Server als Stratum 1-Server, wenn die Referenzuhr asynchron läuft und keine anderen Zeitquellen zur Verfügung stehen.

b) Ein LANTIME, der nur von einem externen NTP-Server mit Stratum 3 synchronisiert wird, fungiert in einem Netzwerk als Stratum 4 NTP-Server. Wenn die Funktion „Stratumwechsel deaktivieren" aktiviert ist, arbeitet der NTP-Server weiterhin als Stratum 4 NTP-Server, auch wenn die Verbindung zum externen NTP-Server unterbrochen wird.

c) Wechselt NTP des LANTIME mit aktiver Funktion „Stratumwechsel deaktivieren" von seinem internen Referenztaktgeber zu einem externen NTP-Server mit Stratum 2, ändert sich der Stratum des LANTIME von 1 auf 3.

NTP Trustime

Diese Einstellung legt fest, wie lange NTP der internen Referenzuhr eines Servers „vertrauen" soll, nachdem diese asynchron geworden ist. Der Status einer asynchronen Referenzuhr wird auch als „freilaufend" bezeichnet. Die Genauigkeit einer „freilaufenden" Referenzuhr hängt vom Typ des integrierten Oszillators ab. Die Vertrauenszeit sollte daher in Abhängigkeit von der Genauigkeit der „freilaufenden" Referenzuhr eingestellt werden.

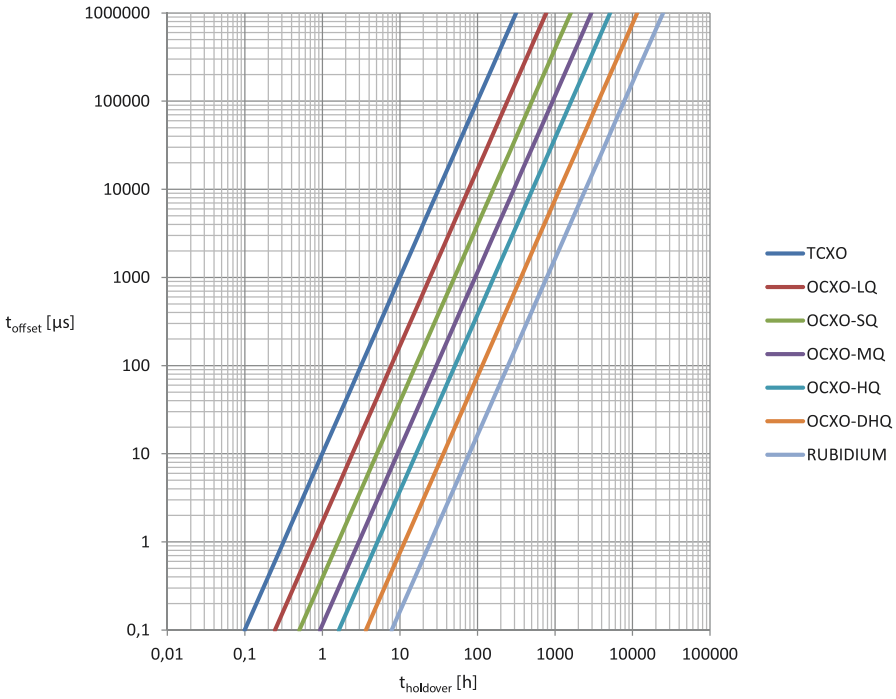


Abbildung: Verhältnis zwischen Holdover-Zeit (x) und Offset (y) unter Verwendung der eingesetzten Meinberg-Oszillatoren

Wie konfiguriere ich die richtige Trusttime in meiner Anwendungsumgebung?
Als Beispiel nehmen wir jetzt an, dass unser Empfänger einen eingebauten TCXO-Oszillator verfügt. Die Trusttime soll ab einem Offset von 1ms ablaufen. Anhand der Grafik kann abgelesen werden, dass nach 10 Stunden Holdover-Zeit dieser Offset erreicht wird. Demzufolge sollte eine Trusttime von 10 Stunden konfiguriert werden.

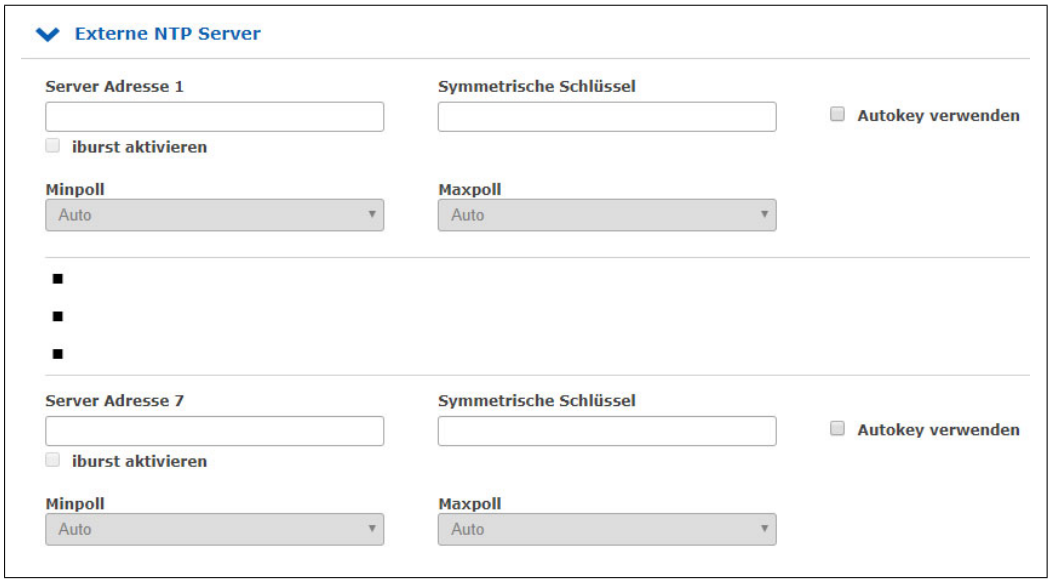
Vorgehensweise: Zunächst sollte in Erfahrung gebracht werden, welcher Oszillator eingesetzt wird. Gehen Sie dazu in das Webinterface-Menü „Monitoring und Management → Uhr → ?? → Oszillator Typ“. Danach können Sie sich für sich einen Offset festlegen, ab dem der NTP seinen Stratum bzw. die Trusttime verlieren soll.

Eine Liste der Oszillatoren, die für Meinberg Referenzuhren verfügbar sind:
https://www.meinberg.de/german/specs/gpsopt.htm

Vertrauenswürdige Schlüssel
In diesem Feld können Sie die IDs der symmetrischen Schlüssel eingeben, die für die Authentifizierung verwendet werden sollen. Wenn Sie mehr als einen Schlüssel haben, müssen die IDs mit einem Leerzeichen eingegeben werden, um sie voneinander zu trennen. Die symmetrischen Schlüssel können Sie im Untermenü „NTP Symmetric Keys“ auf der NTP-Seite konfigurieren. Weitere Informationen finden Sie im Unterkapitel „NTP Symmetric Keys“.

10.1.5.2 Externe NTP-Server

Über das Konfigurationsformular können Sie bis zu 7 externe NTP-Server als Backup für die internen Referenzuhr eingeben.



Server-Adresse:
IP oder Hostname eines externen Servers.

Symmetrische Schlüssel:
In diesem optionalen Feld können Sie die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit dem externen Server verwendet werden soll.

Damit die Authentifizierung funktioniert, müssen folgende Punkte berücksichtigt werden:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Untermenü „NTP → NTP Symmetric Keys“ auf der NTP-Seite bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Lokale Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben.

c) Auf dem externen Server muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Minpoll und Maxpoll (nicht verfügbar auf Geräten, die die MRS-Funktion unterstützen):
Mit diesen Einstellungen können Sie das minimale und maximale Abfrageintervall (Abfragezyklus) für einen bestimmten externen Server festlegen. NTP beginnt mit dem minimalen Abfrageintervall und ändert sich Schritt für Schritt zum Maximum des Abfrageintervalls.

iburst aktivieren (nicht verfügbar auf Geräten, die die MRS-Funktion unterstützen):
Die iburst-Aktivierung beschleunigt die anfängliche Synchronisation mit einem externen Server.

Besonderheit LANTIME/MRS:
Alle externen NTP-Server werden der NTP-Konfigurationsdatei */etc/ntp.conf* als **„noselect“** hinzugefügt. Dies hat zur Folge, dass alle Server vom NTPD für statistische Zwecke angefordert werden, aber die Server werden vom NTPD niemals als Synchronisierungs-Peer ausgewählt. Die LANTIME MRS-Logik wählt dann den besten Server unter allen externen Servern aus. Der Auswahlalgorithmus für den besten externen NTP-Server wird in den folgenden Schritten beschrieben:

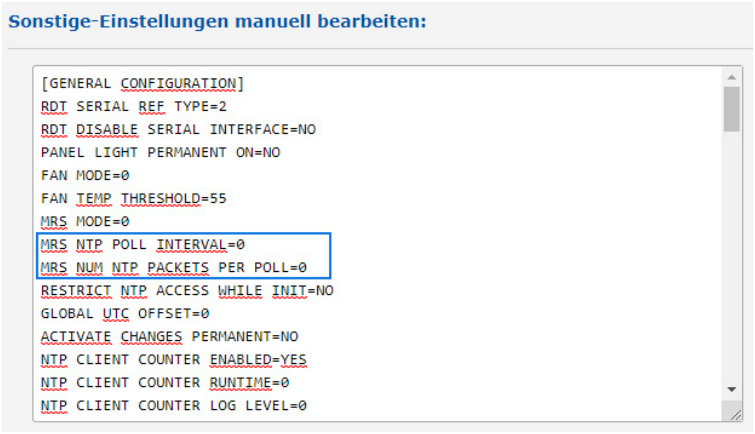
- Auswahl, welcher Server akzeptiert wird
- Gruppen von verschiedenen Offsets werden erstellt
- Auswahl der größten Gruppe
- Ausreißer werden gesucht und aus dieser Gruppe entfernt
- der Median wird als bester Server verwendet
- Prüfung, ob „last_best_external_NTP_server“ verwendet werden kann - um häufige Wechsel zwischen den NTP Servern zu reduzieren

Der beste Server kann im Web-Interface im Menü „Statistik → NTP-Status“ und in dem Menü „Uhr → Status & Konfiguration → MRS-Status“ überprüft werden. Der ermittelte Offset wird dann zur Steuerung des internen Oszillators verwendet, falls keine andere Referenzquelle mit einer höheren Priorität zur Verfügung steht.

Aufgrund dieser Besonderheit unterscheiden sich die Konfigurationsmöglichkeiten für externe NTP-Server. Die Parameter Minpoll, Maxpoll und Iburst können auf einem LANTIME/MRS nicht konfiguriert werden.

Für einen LANTIME/MRS können Sie das Standardabfrageintervall von 32 Sekunden über die manuelle Konfiguration des Servers einstellen. Um fortzufahren, folgen Sie dieser Menüführung:

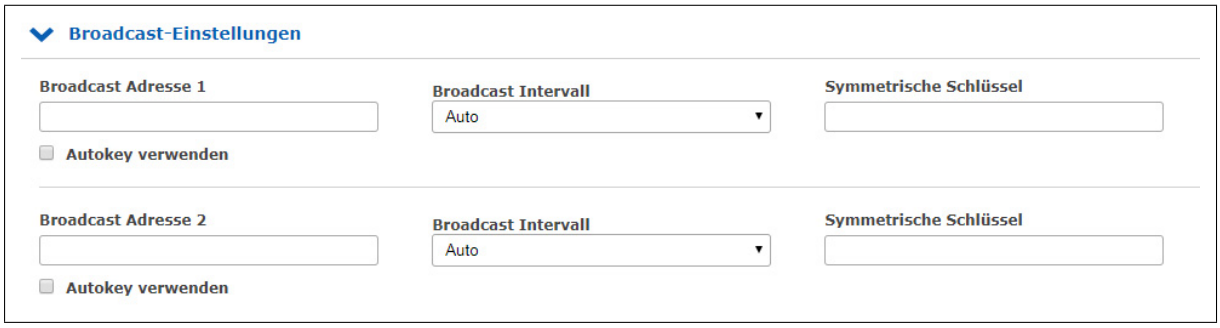
Webinterface - „System → Dienste und Funktionen → Manuelle Konfiguration → Standardkonfiguration → Sonstige Konfiguration“.



Mit dem Parameter „MRS NTP POLL INTERVAL“ können Sie das Polling-Intervall des externen Servers anpassen. Standardmäßig ist dieser Wert auf 0 gesetzt, d.h. externe Server werden alle 32 Sekunden abgefragt. Die Werte können zwischen 1 und 10 eingestellt werden und werden als Potenz von 2 verwendet, z.B. wenn dieser Wert auf 6 gesetzt wird, entspricht das $2_6 = 64$ Sekunden für ein Abfrageintervall.

Mit dem Parameter „MRS NUM NTP PACKETS PER POLL“ können Sie die Anzahl der gesendeten NTP-Abfragen pro Polling-Intervall einstellen. Standardmäßig ist dieser Wert auf 0 gesetzt, was bedeutet, dass 4 Pakete in einem bestimmten Polling-Intervall gesendet werden. Setzen Sie einen Wert zwischen 1 und 8, der der tatsächlichen Anzahl der Pakete entspricht.

10.1.5.3 Broadcast-Einstellungen



Wenn die NTP-Zeit im Broadcast-Modus in einem lokalen Netzwerk verteilt werden soll, können Sie in diesem Menü eine gültige Broadcast-Adresse eingeben. Bitte beachten Sie: Ab der NTP4-Version muss der Broadcast-Modus immer mit Authentifizierung verwendet werden.

Broadcast Addresse:
Hier muss eine gültige Broadcast-Adresse eines lokalen Netzwerks eingegeben werden, mit dem der LANTIME verbunden ist.

Broadcast Intervall:
Das Intervall, in dem der Server die NTP-Pakete an die konfigurierte Broadcast-Adresse sendet.

Symmetrische Schlüssel:
In diesem Feld können Sie die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit den NTP-Clients verwendet werden soll.

Folgendes muss beachtet werden, damit die Authentifizierung funktioniert:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Untermenü „NTP → NTP Symmetric Keys“ auf der NTP-Seite bearbeiten.

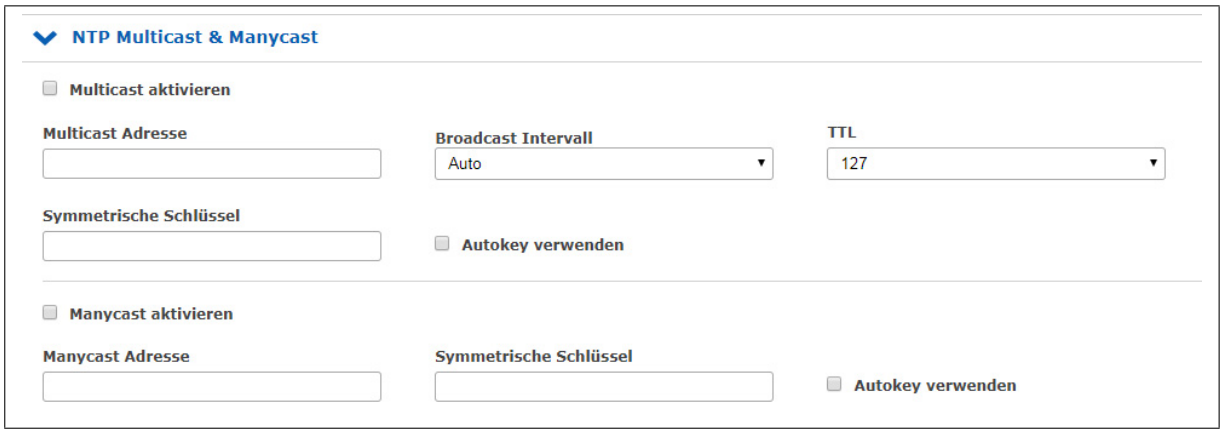
b) Zusätzlich müssen Sie die ID in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben.

c) Auf dem NTP-Client muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Im Folgenden finden Sie einen Auszug aus der NTP-Konfiguration eines Clients, der als Broadcast-Client mit Authentifizierung konfiguriert ist:

```
keys /etc/ntp.key
# Pfad zur NTP-Schlüsseldatei

trustedkey 1
# Die Schlüssel-ID, die für die Authentifizierung verwendet wird.

broadcastclient
# Dieser Client arbeitet als Broadcast-Client.
```

10.1.5.4 NTP Multicast und Manycast



10.1.5.5 NTP-Multicast

NTP Multicast bietet die Möglichkeit, die Zeit durch Multicast im Netzwerk zu verteilen. Die Internet Assigned Numbers Authority (IANA) hat exklusiv die Multicast-IP-Adresse 224.0.1.1.1 für NTP vergeben. Daher wird empfohlen, diese Adresse als Multicast-Adresse zu verwenden. Es können aber auch andere Adressen des Multicast-Adressraums eingestellt werden.

Der Multicast-Adressraum sieht wie folgt aus:

```
Ipv4: 224.0.0.0 -> 239.255.255.255
Ipv6: Jede FF00::/8 Adresse
```

Multicast Adresse: Hier muss eine korrekte Multicast-Adresse eingegeben werden.

Broadcast Intervall: Das Intervall, in dem der Server die NTP-Pakete an die konfigurierte Broadcast-Adresse sendet.

TTL: Der konfigurierte TimeToLive (TTL)-Wert bestimmt, wie viele Hops NTP-Pakete im Netzwerk passieren können. Jeder Netzwerk-Hop reduziert diesen Wert um 1, und wenn der Wert Null erreicht, wird das Netzwerkpaket gelöscht.

Symmetrische Schlüssel: Für NTP Multicast wird eine Authentifizierung empfohlen, ist aber nicht zwingend erforderlich. Wenn die Authentifizierung jedoch auf der Serverseite konfiguriert ist, ist es auch auf der Client-Seite notwendig, dies zu tun.

Im Feld „Symmetrische Schlüssel“ können Sie daher die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit den NTP-Clients verwendet werden soll.

Folgendes muss beachtet werden, damit die Authentifizierung funktioniert:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Untermenü „NTP → NTP Symmetric Keys“ auf der NTP-Seite bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben.

c) Auf dem NTP-Client muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Im Folgenden finden Sie einen Auszug aus der NTP-Konfiguration eines Clients, der als Multicast-Client mit Authentifizierung konfiguriert ist:

```
keys /etc/ntp.key                  # Pfad zur NPT-Schlüsseldatei
trustedkey 1                       # Die Schlüssel-ID, die für die Authentifizierung verwendet wird.
multicastclient 224.0.1.1 key 1    # Der Client hört auf die Multicast-Adresse 224.0.1.1.1 und
                                   # verwendet den Schlüssel mit der ID 1 zur Authentifizierung.
```

10.1.5.6 NTP-Manycast

NTP Manycast beschreibt die Möglichkeit, dass ein oder mehrere NTP-Server hinter einer Multicast-Adresse stehen. Im Gegensatz zur Multicast-Methode senden die Server jedoch keine NTP-Pakete periodisch an diese Mutlicast-IP. Die Manycast-Funktion ist viel mehr eine Methode, um den NTP-Dienst eines anfragenden Clients automatisch neu zu konfigurieren. Der NTP-Dienst des Clients wählt automatisch bis zu 3 Server aus, die für ihn „am besten“ zu sein scheinen. Der NTP-Dienst konfiguriert sich dann selbstständig neu und stellt eine Unicast-Kommunikation mit diesen Servern her. Wie beim Multicasting wird empfohlen, Authentifizierungsmethoden zu verwenden.

Manycast aktivieren: Aktiviert das Manycast-Feature.

Manycast Adresse: Adressfeld zur Eingabe der Manycast-Adresse (Mutlicast-Adressraum)

Der Multicast-Adressbereich ist wie folgt:

```
Ipv4: 224.0.0.0 -> 239.255.255.255
Ipv6: Jede FF00::/8 Adresse
```

Symmetrische Schlüssel: Für NTP Manycast wird eine Schlüsselmethode zur Authentifizierung empfohlen, ist aber nicht zwingend erforderlich. Wenn die Authentifizierungsmethode jedoch auf der Serverseite konfiguriert ist, ist es notwendig, dies auch auf der Client-Seite zu tun.

Im Feld „Symmetrische Schlüssel“ können Sie daher die ID eines symmetrischen Schlüssels eingeben, der für die Authentifizierung mit den NTP-Clients verwendet werden soll.

Folgendes muss beachtet werden, damit die Authentifizierung funktioniert:

a) Die NTP-Schlüsseldatei des Servers muss die ID enthalten. Sie können die Schlüsseldatei im Submenü „NTP → NTP Symmetric Keys“ im NTP-Menü bearbeiten.

b) Zusätzlich müssen Sie die ID in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ eingeben. .

c) Auf dem NTP-Client muss der gleiche Schlüssel mit der gleichen ID konfiguriert werden.

Im Folgenden finden Sie einen Auszug aus der NTP-Konfiguration eines Clients,
der als Multicast-Client mit Authentifizierung konfiguriert ist:

```
keys /etc/ntp.key                 # Pfad zur NPT-Schlüsseldatei
trustedkey 1                      # Die Schlüssel-ID, welche für die Authentifizierung verwendet wird.
manycastclient 224.0.1.2 key 1    # Der Client hört auf die Multicast-Adresse 224.0.1.2 und verwendet
                                  # den Schlüssel mit der ID 1 zur Authentifizierung.
```

10.1.5.7 NTP Autokey Einstellungen

NTP-Version 4 unterstützt neben den symmetrischen Schlüsseln zusätzlich noch das sogenannte Autokey-Verfahren. Die Echtheit der empfangenen Zeit auf den NTP-Clients wird durch symmetrische Schlüssel sehr gut sichergestellt. Allerdings ist für eine höhere Sicherheit der periodische Austausch der verwendeten Schlüssel nötig, um einen Schutz, z.B. vor Replay-Attacken (d.h. Angriffen, bei denen aufgezeichneter Netzwerkverkehr einfach noch einmal abgespielt wird), zu erreichen.

Bei Netzwerken mit sehr vielen Clients kann dieses Austauschen der symmetrischen Schlüssel allerdings mit sehr viel Aufwand verbunden sein, weil auf jedem Client die Schlüssel für den/die NTP Server ausgetauscht werden müssen. Aus diesem Grund wurde von den NTP Entwicklern das Autokey-Verfahren eingeführt, das mit einer Kombination aus Gruppenschlüsseln (group keys) und öffentlichen Schlüsseln (public keys) arbeitet. Alle NTP Clients können somit die Zeitangaben, die sie von Servern ihrer eigenen Autokey-Gruppe erhalten, auf Echtheit überprüfen.

Beim Autokey-Verfahren werden sogenannte sichere Gruppen (secure groups) gebildet, in denen NTP Server und Clients zusammengefasst sind. Es gibt drei verschiedene Typen von Mitgliedern in einer solchen Gruppe:

a) Trusted Host
Ein oder mehrere vertrauenswürdige NTP Server. Um diesen Status zu erhalten, muss der Server ein als „Trusted“ gekennzeichnetes selbst-signiertes Zertifikat besitzen. Er sollte auf dem niedrigsten Stratum Level der Gruppe operieren.

b) Host
Ein oder mehrere NTP Server, die kein „Trusted“-Zertifikat besitzen, sondern nur ein selbstsigniertes Zertifikat (ohne die „Trusted“-Kennzeichnung).

c) Client
Ein oder mehrere NTP-Client-Systeme, die im Gegensatz zu den beiden erstgenannten Typen die Zeit lediglich empfangen und nicht in der Gruppe weiterverteilen. Alle Mitglieder der Gruppe (Trusted Hosts, Hosts und Clients) müssen im Besitz des gleichen Gruppenschlüssels sein. Der Gruppenschlüssel wird von einer Trusted Authority (TA) generiert und muss dann manuell auf alle Gruppenmitglieder verteilt werden (auf einem sicheren Weg, z.B. mittels scp). Die Rolle der TA kann ein Trusted Host in der Gruppe übernehmen (zum Beispiel ein LANTIME), es ist aber auch ohne Probleme möglich, den Gruppenschlüssel von einem nicht der Gruppe zugehörigen TA-Host erzeugen zu lassen.

Die verwendeten Public Keys können auf den Trusted Hosts der Gruppe periodisch manuell neu erzeugt werden (das ist sowohl im Webinterface als auch über das CLI-Setupprogramm möglich, über den Punkt „Generate new NTP public key“ im Bereich „NTP Autokey“ auf der Seite „Security Management“) und damit dann automatisch an alle anderen Mitglieder der Gruppe verteilt werden. Der Gruppenschlüssel bleibt gleich und somit entfällt das manuelle Update von Schlüsseln für alle Gruppenmitglieder.

Ein LANTIME kann in einer solchen Autokey-Gruppe sowohl TA und Trusted Host als auch einfacher Host sein. Um den LANTIME als TA und Trusted Host zu konfigurieren, schalten Sie das Autokey-Verfahren ein und initialisieren Sie per HTTPS-Webinterface den Gruppenschlüssel („Generate groupkey“). Dafür ist ein Crypto-Passwort nötig, das Sie ebenfalls im Webinterface ändern können. Den so erzeugten Gruppenschlüssel müssen Sie dann vom LANTIME herunterladen (z.B. über das HTTPS-Webinterface) und dann auf alle Clients und weiteren NTP Server der Gruppe kopieren (und diese Systeme ebenfalls für die Verwendung von Autokey konfigurieren).

Die ntp.conf aller Gruppenmitglieder muss folgende Zeilen enthalten:

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

Dabei ist „cryptosecret“ in diesem Fall das Crypto-Passwort, das zum Erstellen des Group Keys und aller Public Keys verwendet wurde. Bitte beachten Sie, dass das Crypto-Passwort im Klartext in der ntp.conf steht und somit auf Nicht-LANTIME-Systemen sichergestellt sein sollte, dass nur „root“ diese Datei einsehen kann. Die Clients müssen zusätzlich noch den Eintrag der verwendeten NTP-Server ergänzen, um eine Nutzung von Autokey in Verbindung mit diesen Servern einzuschalten. Das sieht z.B. so aus:

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

In diesem Beispiel wird der NTP Server time.meinberg.de mit Autokey verwendet, während time2.meinberg.de ohne jegliche Überprüfung der Echtheit der Zeit akzeptiert wird.

Möchten Sie den LANTIME zwar als Trusted Host verwenden, aber eine andere TA nutzen, dann erzeugen Sie mithilfe dieser Trusted Authority einen Gruppenschlüssel und binden ihn z.B. mithilfe des Webinterfaces auf Ihrem LANTIME ein (im Menüpunkt „NTP“ im Bereich „NTP Autokey“ den Menüpunkt „Upload Groupkey“).

Wenn Sie den LANTIME als einfachen NTP Server (nicht „trusted“) verwenden möchten, dann müssen Sie den Gruppenschlüssel Ihrer Gruppe hochladen („NTP“ -> “NTP Autokey“ -> “Upload Groupkey“) und ein eigenes, selbstsigniertes Zertifkat erzeugen (ohne es als „Trusted“ zu markieren). Da beim Generieren eines Zertifikats über das Webinterface oder das CLI-Setupprogramm grundsätzlich immer als „Trusted“ markierte Zertifikate erstellt werden, müssen Sie zum Erstellen von Zertifikaten ohne „Trusted“-Merkmal das Programm ntp-keygen manuell auf dem LANTIME aufrufen (in einer SSH-Sitzung):

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

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

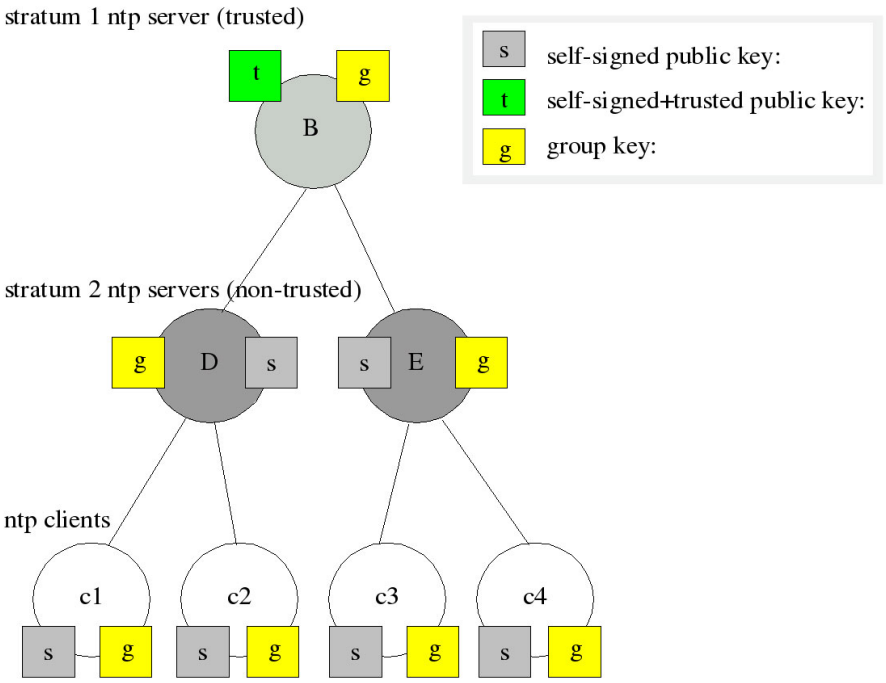
```
cp /etc/ntp/ntpkey_*   /mnt/flash/config/ntp/uploaded_groupkeys
```

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

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

Beispiel:

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

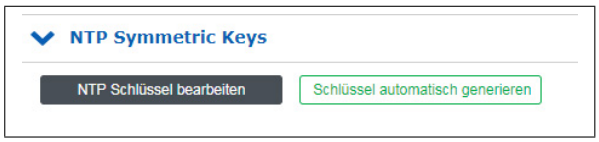


D und E sind NTP Server, die als Hosts der Gruppe nicht Trusted sind. Sie besitzen den Gruppenschlüssel und ein selbstsigniertes Zertifikat (das nicht als „Trusted" markiert wurde). Die Clients besitzen jeweils den Gruppenschlüssel und ebenfalls ein selbstsigniertes Zertifikat.

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

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

10.1.5.8 NTP Symmetrische Schlüssel



Seit der NTP-Version 3 bietet NTP eine Authentifizierungsmethode mit symmetrischen Schlüsseln an. Mit der Schaltfläche „NTP Schlüssel bearbeiten“ kann die NTP-Schlüsseldatei des Servers bearbeitet werden. Bei der Auslieferung des Servers enthält die Datei einen Beispielschlüssel. Mit der Schaltfläche „Schlüssel automatisch generieren“ können MD5- und SHA1-Schlüssel automatisch generiert werden.

Verwendung von AES128-CMAC Schlüsseln
Um einen AES128-CMAC Schlüssel zu nutzen, können wie gewohnt die Schlüsselvorschläge (eigentlich sind dies nur Zufallswerte bzw. ein zufälliger „40-character hex digit string“) erstellt werden.

Anschließend können die generierten SHA1-Schlüssel geändert werden - SHA1 wird in diesem Fall durch AES128CMAC ersetzt.

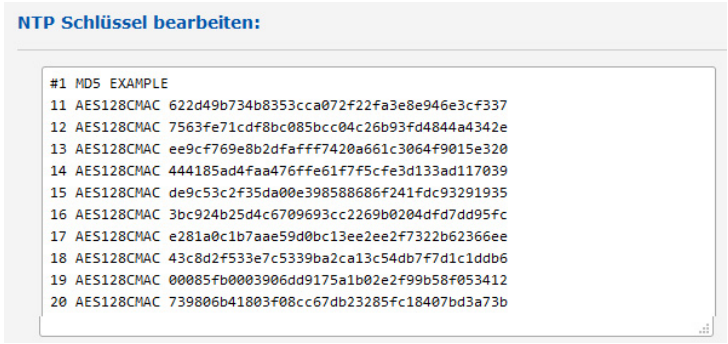


Abb.: Menü „NTP → NTP Symmetric Keys → NTP Schlüssel bearbeiten“

Achtung:
Wenn bereits symmetrische Schlüssel im Einsatz sind, dann muss der Inhalt dieser Datei zwingend zwischengespeichert werden, bevor ein neuer Satz automatisch generiert wird. Der Inhalt der „alten“ Datei muss danach zusammen mit den „neuen“ AES128-CMAC Schlüsseln wieder in das Feld NTP Schlüssel bearbeiten eingesetzt werden.

Im Folgenden finden Sie einen repräsentativen Auszug aus einer NTP-Schlüsseldatei:

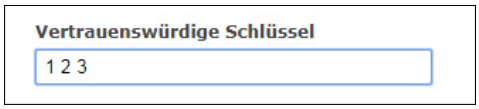
```
1    M          f294fa0                                  # MD5 Key
2    MD5        BtdW/<gj2*2M;!'~qAIN                     # MD5 Key
3    SHA1       094c533b614d9e4bcb6e18a97a7b0e4d459025bd # SHA1 Key
4    AES128CMAC 02eb9a63710dda360d181d9582056a504d965700 # AES128-CMAC Key
```

Die erste Spalte enthält eine eindeutige Schlüssel-ID (Wertebereich 1 - 65535). Die zweite Spalte enthält den Schlüsseltyp („M“ oder „MD5“ für einen MD5-Schlüssel, „SHA1“ für einen SHA1-Schlüssel oder AES128CMAC für einen AES128-CMAC-Schlüssel). Die dritte Spalte enthält die Schlüsselkette, die zwischen 1 und 40 Zeichen lang sein kann.

Wie richte ich die Authentifizierung zwischen einem LANTIME und meinen NTP-Clients ein?

1. Fügen Sie die zu verwendenden Schlüssel in die Schlüsseldatei des Servers ein (wie im Auszug aus einer NTP-Schlüsseldatei dargestellt).

2. Geben Sie die IDs dieser Schlüssel in das Feld „Vertrauenswürdige Schlüssel“ unter „NTP → Allgemeine Einstellungen“ ein, zum Beispiel:



3. Nachfolgend ein exemplarischer Auszug aus der NTP-Konfiguration eines Linux-Clients, der den Schlüssel mit der ID 2 zur Authentifizierung mit dem Server 192.168.100.1 und den Schlüssel mit der ID 3 zur Authentifizierung mit dem Server 192.168.100.2 verwendet:

```
keys /etc/ntp.keys # Pfad zur Schlüsseldatei
trustedkey 2 3 # IDs der zu vertrauenswürdigen Schlüssel

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

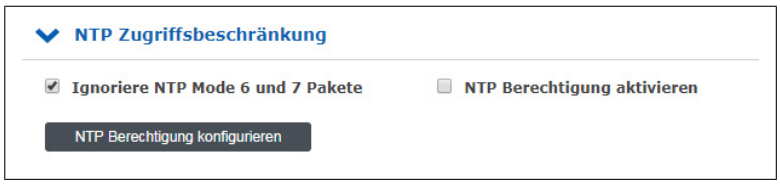
In diesem Fall muss die Schlüsseldatei des Clients die Schlüssel mit den IDs 2 und 3 enthalten, die mit den Schlüsseln des Servers identisch sein müssen.

10.1.5.9 NTP-Konfiguration

Die aktuelle NTP-Konfigurationsdatei wird über die Schaltfläche „NTP Konfigurationsdatei anzeigen“ angezeigt. Diese Datei wird bei jedem Neustart oder jeder Änderung der NTP-Konfiguration automatisch vom System erzeugt und kann nicht direkt bearbeitet werden.

Wenn zusätzliche Einstellungen für NTP (Authentication, Restriction ...) erforderlich sind, die nicht durch die vorhandenen Einstellungsmöglichkeiten auf der NTP-Seite abgedeckt sind, muss eine zusätzliche Konfigurationsdatei verwendet werden. Diese Datei kann über die Schaltfläche „Zusätzliche NTP Parameter bearbeiten“ bearbeitet und verwaltet werden. Bei jeder Erstellung der ‘ntp.conf‘ wird diese zusätzliche Datei automatisch an die ntp.conf angehängt.

10.1.5.10 NTP Zugriffsbeschränkungen



Das Menü „NTP Zugriffsbeschränkung“ kann verwendet werden, um den NTP-Zugang auf bestimmte IP-Adressen zu beschränken.

Um beispielsweise den Zugriff auf alle Adressen aus dem Subnetz 192.168.100.x zu ermöglichen, geben Sie unter IP-Adresse 192.168.100.0 und unter Netzmaske 255.255.255.255.0 ein. Der Zugriff kann auch für einzelne IP-Adressen erfolgen.

Um den eingeschränkten Zugang zu ermöglichen, muss die Option „NTP Berechtigung aktivieren“ aktiviert werden. Client-IP-Adressen, die nicht in den zulässigen IP-Adressbereichen enthalten sind, erhalten keine NTP-Antworten vom LANTIME.

Ignoriere NTP Mode 6 und 7 Pakete
Diese Einstellung bewirkt, dass interne Informationen, wie z.B. Zugriffsstatistiken, nicht von anderen NTP-fähigen Geräten im Netzwerk über den NTP-Dienst des Servers abgefragt werden können. Die Einstellung hat keinen Einfluss auf die Zeitsynchronisation zwischen NTP-Clients und dem Server.

NTP Berechtigung aktivieren
Durch Aktivieren dieser Einstellung werden die folgenden Zeilen in die NTP-Konfiguration des Servers geschrieben:

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

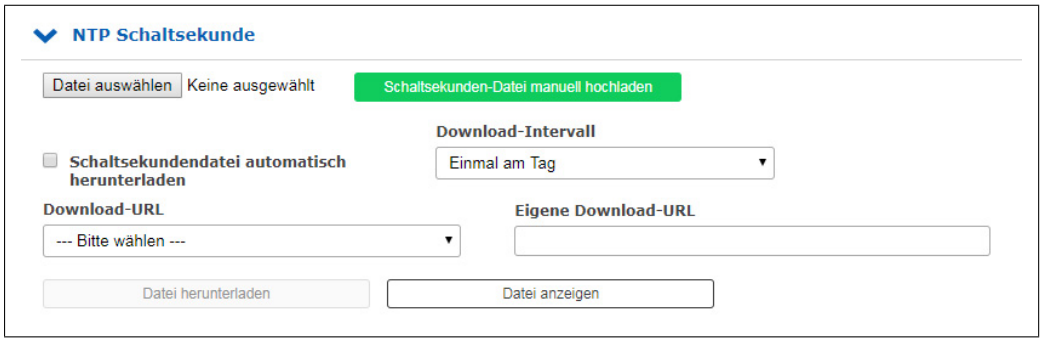
Diese Einstellungen bewirken, dass der Server nicht mehr auf NTP-Anfragen reagiert. Im Untermenü „NTP Berechtigungen konfigurieren“ können Sie eine „Whitelist“ von Client-IP-Adressen oder auch ganzen Subnetzen konfigurieren, deren Anfragen vom Server beantwortet werden dürfen.

10.1.5.11 NTP Schaltsekunde

Die Zeitbasis für die meisten lokalen Zeitzonen der Welt heißt Coordinated Universal Time, UTC, die von mehreren Atomuhren abgeleitet ist, die in verschiedenen Ländern auf der ganzen Welt verteilt sind. Die Erdrotation ist nicht konstant und variiert im Laufe der Zeit, während die mittlere Erdrotationsgeschwindigkeit langsam abnimmt. Aus diesem Grund werden so genannte Schaltsekunden in die UTC-Zeitskala eingefügt, die die UTC-Zeit mit der realen Erdrotation kompensieren. Eine Schaltsekunde wird immer um 23:59:59 (UTC) eingefügt, entweder am 31.12. oder 30.06. (Andere Daten sind theoretisch möglich, wurden aber praktisch noch nicht verwendet).

Einige Protokolle oder Verfahren zur Übertragung der Zeitinformation, z.B. GPS, NTP, PTP, DCF77 und IRIG, können Schaltsekunden voranstellen, um einem Empfänger die Möglichkeit zu geben, sich im Voraus auf eine Schaltsekunde vorzubereiten. Das GPS-Satellitensystem verteilt die Schaltsekundenansage sechs Monate vor dem Schaltsekunden-Ereignis. Meinberg LANTIME-Zeitserver mit GPS-Empfängern erhalten diese Mitteilung automatisch über das GPS-Signal. In der Protokolldatei des LANTIME wird der Eintrag „Leap Second Announced - Schaltsekunde angekündigt“ erzeugt, wenn das Datum der Schaltsekunde empfangen wird.

Andere Synchronisationsmethoden bieten diese Ankündigungsmöglichkeit nicht an, was zu einem zweiten Zeitsprung führen kann. Daher ist es notwendig, die NTP-Schaltsekundendatei auf diesen Systemen aktuell zu halten, damit um Mitternacht (UTC) eine Schaltsekunde korrekt eingefügt wird.



Im Menü „NTP Schaltsekunde“ können Sie die aktuell gespeicherte Schaltsekundendatei ansehen, die Datei manuell hochladen oder einen automatischen Download von den folgenden Quellseiten konfigurieren:

Verfügbare Download-Quellen für Schaltsekundendateien:

1. NIST Schaltsekundendatei:
   ftp://time.nist.gov/pub/ (directory listing)
   ftp://time.nist.gov/pub/leap-seconds.list (aktuelle Schaltsekundendatei)

2. IERS (Earth Rotation and reference systems Service) Schaltsekundendatei:
   https://hpiers.obspm.fr/iers/bul/bulc/ntp/ (Verzeichnisauflistung)
   https://hpiers.obspm.fr/iers/bul/bulc/ntp/leap-seconds.list (aktuelle Schaltsekundendatei)

3. Meinberg Schaltsekundendatei (Kopie der IERS Schaltsekundendatei):
   https://www.meinberg.de/download/ntp/leap-seconds.list
   https://www.meinberg.de/download/ntp/leap_second

10.1.5.12 Spezielle Einstellungen

Zeitskala
Diese Einstellung konfiguriert die Zeitzone des NTP. Die Standardeinstellung ist „UTC“, da NTP standardmäßig auf UTC basiert und Standard NTP Clients UTC Zeit erwarten.

Die Einstellung „LOKALE ZEIT“ sollte nur gewählt werden, wenn der Zeitserver zur Synchronisation bestimmter Clients verwendet wird, die lokale Zeit benötigen. Wenn Sie hier „LOKALE ZEIT“ wählen, muss die genaue Zeitzone im Menü „System → Display“ konfiguriert werden.

Achtung: Die Verwendung von „LOKALE ZEIT“ ist ein Verstoß gegen den NTP-Standard und bewirkt, dass Standard-NTP-Clients fehlerhafte Zeiten akzeptieren und einen entsprechenden Zeitsprung durchführen.

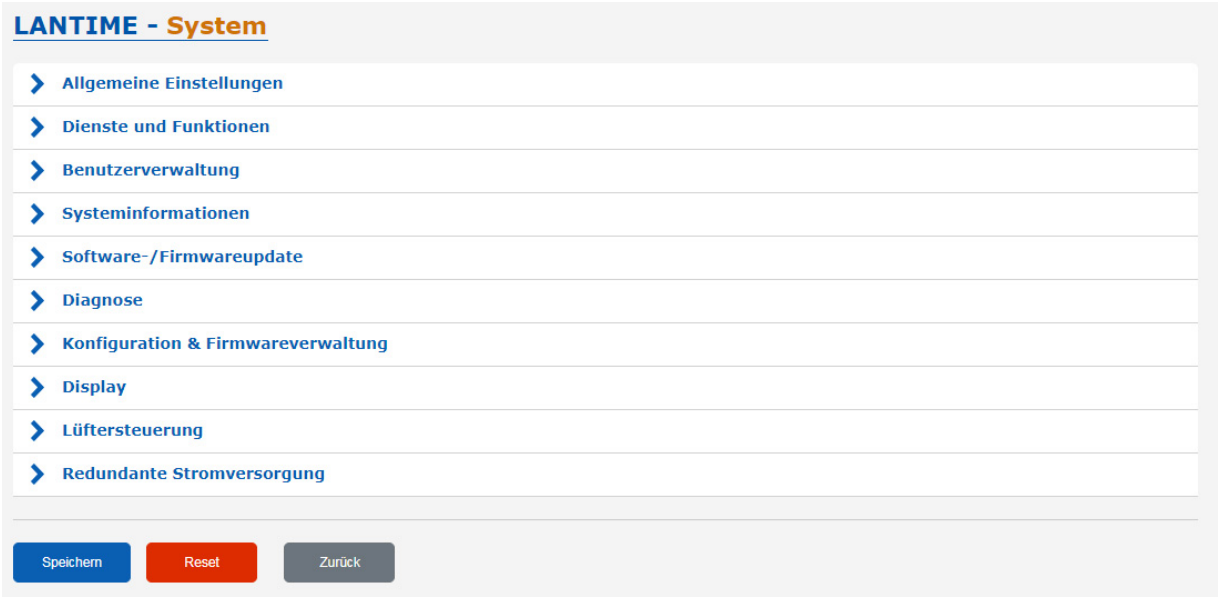
Fester Offset (s)
Dieser Wert wird verwendet, um die Ausgabezeit des NTP-Dienstes zu manipulieren. Der konfigurierte Wert in Sekunden wird zur aktuellen Zeit addiert und bietet die Möglichkeit, die NTP-Zeit bei Bedarf zu manipulieren.

Achtung: Die Verwendung eines „Festen Offset“ ist eine Verletzung des NTP-Standards und bewirkt, dass Standard-NTP-Clients fehlerhafte Zeiten akzeptieren und einen entsprechenden Zeitsprung machen.

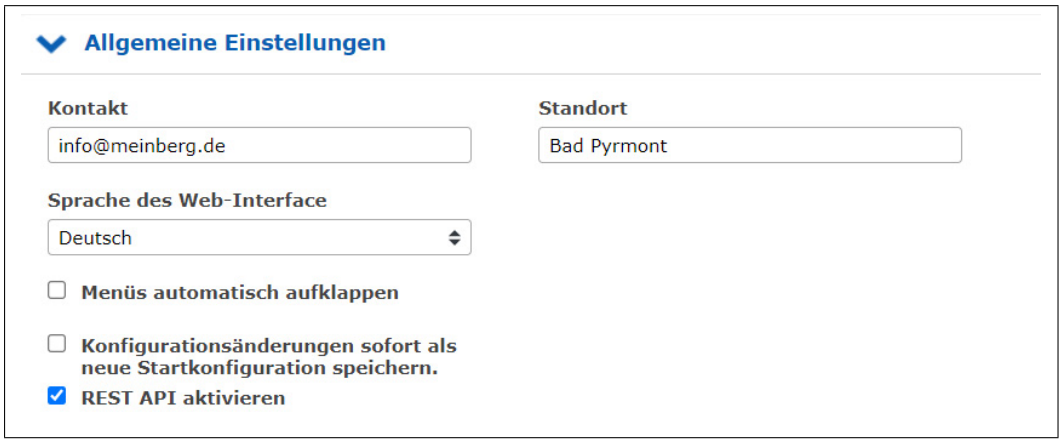
Max. Interner Offset (s)
Dieser Wert in Millisekunden gibt eine minimale Genauigkeit an, die der NTP-Dienst erreichen muss, bevor der Server beginnt, an die Clients Zeit zu verteilen. Die Eingabe eines Wertes von z.B. „1ms“ bedeutet, dass der Dienst wartet, bis die interne Uhr eine Genauigkeit von 1ms oder besser erreicht hat.

MRS Stratum durchreichen
Dieses Feature kommt nur zum Tragen, wenn man einen LANTIME mit MRS-Feature primär über NTP synchronisiert. Wenn „MRS Stratum durchreichen“ nicht aktiviert ist, präsentiert sich der LANTIME als Stratum 1 Server im Netzwerk. Wenn „MRS Stratum durchreichen“ aktiv ist, wird der Stratum des externen NTP Servers berücksichtigt. Ist der externe Server zum Beispiel ein Stratum 1 Server, würde sich der MRS LANTIME als Stratum 2 Server im Netzwerk darstellen.

10.1.6 System



10.1.6.1 Allgemeine Einstellungen



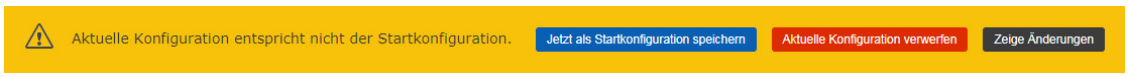
Kontakt:
Ein Eingabefeld zum Speichern der Kontaktinformationen. Diese Information wird auch auf der Hauptseite des Webinterfaces angezeigt und kann über SNMP abgefragt werden.

Ort:
Ein Eingabefeld zum Speichern des Gerätestandortes. Diese Information wird auch auf der Hauptseite des Webinterfaces angezeigt und kann über SNMP abgefragt werden.

Sprache des Web-Interface:
Spracheinstellung des Webinterface.

Menüs automatisch aufklappen:
Wenn diese Funktion aktiviert ist, werden in jedem Konfigurationsdialog alle Untermenüs geöffnet.

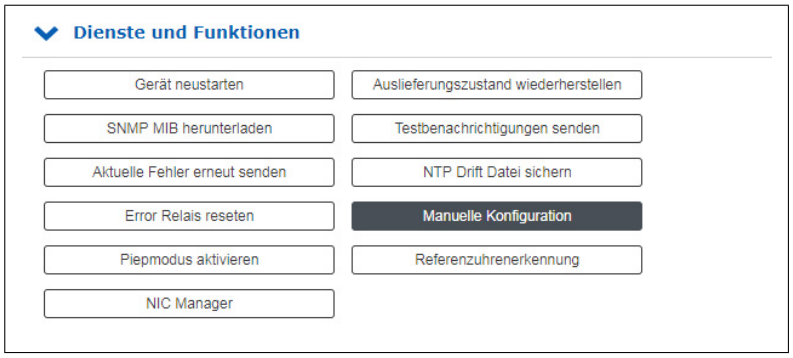
Konfigurationsänderungen sofort als neue Startkonfiguration speichern:
Wenn diese Option aktiviert ist, wird jede Konfigurationsänderung sofort in die Startkonfiguration des LANTIME übernommen (die Startkonfiguration ist die Konfiguration, die beim Booten des LANTIME verwendet wird). Wenn die Option nicht aktiviert ist, wird nach jeder Konfigurationsänderung der folgende Hinweis im Kopf des Web-Interface angezeigt:



Jede Konfigurationsänderung kann dann als Startkonfiguration gespeichert werden, indem Sie mit der Schaltfläche „Jetzt als Startkonfiguration“ bestätigen.

REST API Support
In der 7.04 Version wird erstmalig eine REST API Schnittstelle angeboten um Statusinformationen abzurufen und Konfigurationsanpassungen von externen Managementsystemen über eine sichere HTTPS Verbindung durchführen zu können. Die verfügbaren Objekte sind in einer auf JSON-basierenden Syntax als Baumstruktur abgelegt. Die REST API kann als Dienst per Konfiguration aktiviert und deaktiviert werden. Eine Erläuterung aller verfügbaren Objekte ist in einer integrierten Online Hilfe in der Firmware enthalten und kann über das Web UI aufgerufen werden: https://YOUR-LANTIME-IP-ADRESS/clihelp/

10.1.6.2 Dienste und Funktionen



Gerät neustarten:
Leitet einen Neustart des LANTIME-Betriebssystems ein. Der eingebaute Referenztakt und die vom Taktgeber erzeugten Ausgangssignale bleiben davon unberührt.

SNMP MIB herunterladen:
Laden Sie die Meinberg SNMP MIB-Dateien herunter. Die Archivdatei enthält alle Meinberg SNMP-MIB-Dateien. Um einen LANTIME-Zeitserver mit V7-Firmware über SNMP zu überwachen, werden nur die MBG-SNMP-ROOT-MIB.mib und MBG-LANTIME-NG-MIB.mib-Dateien aus der Archivdatei benötigt.

Aktuelle Fehler erneut senden:
Mit dieser Schaltfläche können Sie dem Benutzer die LANTIME-Fehlerprotokolle per E-Mail oder SNMP-Trap zusenden. Um diese Funktion nutzen zu können, müssen die Fehlerereignisse auf der Seite „Benachrichtigung“ unter „Benachrichtigungsereignisse“ für den gewünschten Kanal (z.B. E-Mail oder SNMP) aktiviert werden. Zusätzlich muss ein E-Mail-Empfänger oder SNMP-Trap-Empfänger konfiguriert werden.

Error Relais zurücksetzen:
Mit dieser Taste kann das Fehlerrelais in einen fehlerfreien Zustand gesetzt werden.

Piepmodus aktivieren:
Diese Funktion kann verwendet werden, um ein LANTIME-Gerät zu finden. Nach dem Betätigen der Taste beginnt der LANTIME einmal pro Sekunde zu piepen und die Alarm-LED auf der Frontplatte blinkt rot. Die Funktion wird durch Drücken der Taste „F2“ auf der Frontplatte beendet.

Auslieferungszustand wiederherstellen:
Setzt den LANTIME auf die Werkseinstellungen zurück. **Achtung:** Die Netzwerkeinstellungen bleiben während des Zurücksetzens über die Weboberfläche erhalten. Sollen auch die Netzwerkeinstellungen zurückgesetzt werden, muss der Reset über die Frontplatte ausgelöst werden. Während des Resets startet der LANTIME neu. Nach dem Neustart kann der LANTIME mit dem Standardbenutzer „root“ und dem Passwort „timeserver“ erneut konfiguriert werden.

Testbenachrichtigung senden:
Senden einer Testbenachrichtigung an die konfigurierten E-Mail-Empfänger und / oder SNMP-Trap-Empfänger.

NTP Drift Datei sichern:
Der NTP-Dienst ermittelt zur Laufzeit die Offsets der Systemuhr und speichert sie in der sogenannten NTP-Driftdatei. Diese Datei wird vom NTP-Dienst verwendet um die Systemuhr automatisch anzupassen, auch wenn kurzfristig keine Zeitquelle verfügbar ist.

Die Funktion „NTP Drift Datei sichern" speichert die aktuelle NTP-Driftdatei */etc/ntp.drift* auf der internen Compact-Flash-Karte unter */mnt/flash/data/ntp.drift*. Beim Neustart des LANTIME kann der Wert aus der gespeicherten Driftdatei vom NTP-Dienst ausgelesen werden, was die anfängliche Zeiteinstellung beschleunigt.

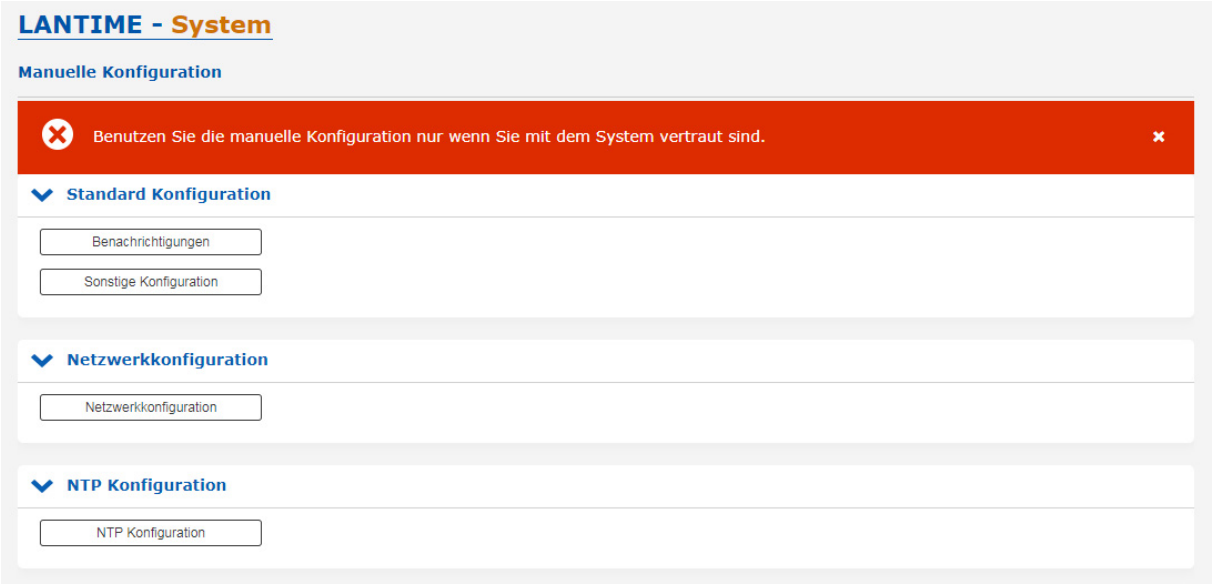
Manuelle Konfiguration:
Die Schaltfläche „Manuelle Konfiguration" ermöglicht einen direkten Zugriff auf die Konfigurationsdateien des LANTIME. Diese Funktion sollte nur von erfahrenen Administratoren genutzt werden.

NIC Manager
Der NIC Manager prüft das System auf die physikalischen Netzwerkschnittstellen. Das betrifft die zusätzlichen Schnittstellen, die über LNE-Module dem System hinzugefügt werden können. Nach dem Einbau und der Initialisierung einer LNE-Karte muss die Funktion ausgeführt werden, damit die Datei „etc/mbg/net.cfg" neu geschrieben wird. Der Netzwerkport-Status kann danach auf der Startseite im Webinterface angezeigt werden.

Auch nach dem Entfernen oder dem Austausch einer LNE sollte die Funktion NIC Manager ausgeführt werden. Das System prüft anhand der MAC-Adressen der einzelnen Netzwerkports, ob diese vorhanden sind, ob sich deren Position (Slot) im System verändert hat oder ob neue Schnittstellen vorhanden sind.

Referenzuhrenerkennung
Diese Funktion muss dann ausgeführt werden, wenn bei IMS-Systemen eine zweite Uhr nachträglich eingebaut wird um eine redundante Empfängerkonfiguration zu erhalten. Das System merkt sich nach dem Hochfahren die serielle Verbindung der eingesetzten Referenzuhr. Wird zum Beispiel bei einem M3000- oder M1000-System mit eingebauter RSC während des Betriebs (Hot-Plug) eine zweite Uhr nachträglich eingebaut, dann muss zur Registrierung der neuen Uhr die Taste „Referenzuhrenerkennung" betätigt werden, damit die serielle Verbindung der zweiten Uhr auf dem System gespeichert wird.

10.1.6.3 Manuelle Konfiguration



- Benachrichtigungseinstellungen
- Verschiedene Konfigurationen
- Netzwerkkonfiguration
- NTP-Konfiguration
- NTP-Broadcast-Konfiguration

Mit „Manuelle Konfiguration“ können Sie die Hauptkonfiguration ändern, indem Sie die Konfigurationsdatei von Hand bearbeiten. Nach der Bearbeitung klicken Sie auf die Schaltfläche „Datei speichern“, um Ihre Änderungen zu speichern, danach werden Sie gefragt, ob Ihre Änderungen durch erneutes Laden der Konfiguration aktiviert werden sollen (dies führt zum erneuten Laden mehrerer Subsysteme wie NTPD, HTTPD usw.).

10.1.6.4 Benutzerverwaltung

Benutzerpasswort ändern
Hier können Sie das Passwort des aktuell authentifizierten Benutzers ändern.

Benutzer anlegen
Es ist möglich, mehrere Benutzerkonten auf einem LANTIME-System zu erstellen. Jedem Konto kann eine von drei Zugriffsebenen zugewiesen werden: Die Super-User-Ebene hat vollen Lese-/Schreibzugriff auf die Konfiguration des LANTIME-Systems, sie kann alle Parameter ändern und hat vollen Shell-Zugriff auf das System, wenn sie sich über Telnet, SSH oder den seriellen Konsolenport anmeldet. Konten auf Administratorebene können Parameter nur über die WEB-Schnittstelle ändern, haben aber keinen Shell-Zugriff. Die Zugriffsebene „Info“ kann nur Status- und Konfigurationsoptionen einsehen, darf aber keine Parameter oder Konfigurationsdateien ändern.

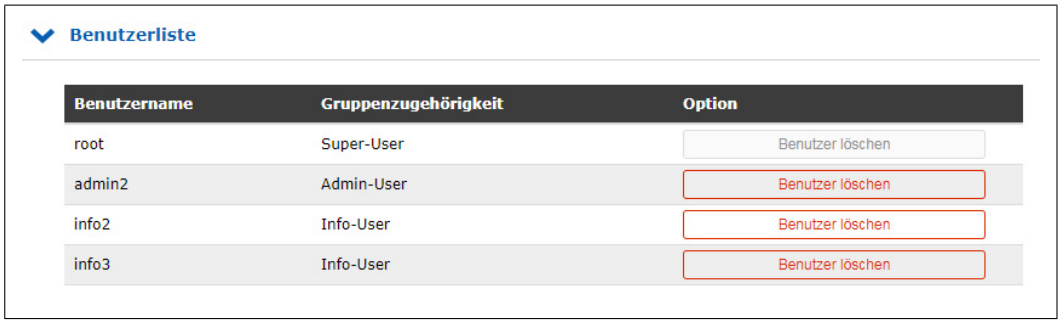
Die folgende Tabelle zeigt die Benutzerrechte der einzelnen Zugriffsebenen im Detail.

	Super User	Admin User	Info User
Vollständiger Zugriff auf die Befehlszeile	✓		
Ändern der Gerätekonfiguration durch das Webinterface	✓	✓	
Bearbeitung der zusätzlichen Konfigurationsdateien, die über das Webinterface* verfügbar sind.	✓		
Ausführen eines Firmware-Updates	✓		
Erstellen einer Diagnosedatei	✓		
Erstellen eines neuen Superuser-Accounts	✓		
Überprüfung aller Konfigurationswerte des Webinterfaces	✓	✓	✓

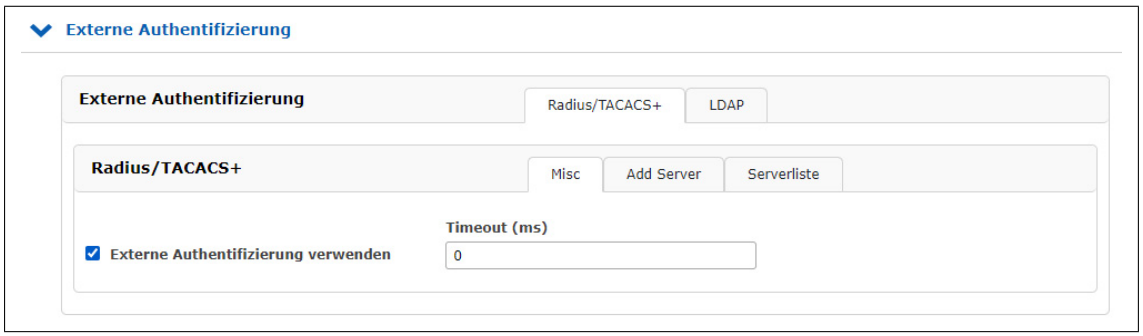
* Zusätzliche Netzwerkkonfiguration, zusätzliche NTP-Konfiguration, benutzerdefinierte Benachrichtigungen

Benutzerliste

Dieses Untermenü gibt Ihnen einen Überblick über alle konfigurierten LANTIME-Benutzer. Durch Anklicken von „Benutzer löschen“ kann ein einzelner Benutzer gelöscht werden.



10.1.6.5 Authentifizierung



Der LANTIME unterstützt Radius und TACACS+ als externe Authentifizierungsmethoden.

Externe Authentifizierung verwenden:
Über dieses Kontrollkästchen können Sie die externe Authentifizierungsfunktion des LANTIME aktivieren oder deaktivieren.

Timeout (ms):/b>
Zeitraum, in dem auf ein Paket „access accept“ von einem Authentifizierungsserver gewartet wird.

Sie können zwischen mehreren Authentifizierungsverfahren wählen:
1. LDAP
2. RADIUS
3. TACACS+

10.1.6.6 LDAP / LDAPS

Lightweight Directory Access Protocol
LDAP basiert auf dem Client-Server-Modell und wird für sogenannte Verzeichnisdienste verwendet. LDAP beschreibt die Kommunikation zwischen dem LDAP-Client und dem Verzeichnisserver. Aus einem solchen Verzeichnis können objektbezogene Daten, wie z.B. Personendaten oder Rechnerkonfigurationen, ausgelesen werden.

10.1.6.7 LDAP Setup

Beispiel LDAP-Einrichtung in Verbindung mit dem Microsoft-Active-Directory (AD)

Dieses Kapitel beschreibt ein Beispiel zur Einrichtung einer LDAP-Verbindung mit dem Microsoft-Active-Diretory mit vom Standard abweichenden Attributen eines Admin-Benutzers. Bitte beachten Sie, dass dies nur ein Beispiel ist und evtl. nicht direkt auf Ihre Verzeichnisstruktur anwendbar ist. Bitte kontaktieren Sie Ihren für den Verzeichnisdienst zuständigen Administrator, um Abweichungen auszumachen und nötige Anpassungen vorzunehmen.

Über den ADSI-Editor des Microsoft-Active-Directory werden folgende Attribute eines LDAP-Benutzers angepasst:

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

Der Name des Benutzers (ldap-ad) die uidNumber und der „HomeDirectory“-Name sind frei wählbar. Dies sind lediglich Beispielwerte. Auch die Attribute (w.z.B sAMAccountName) können durch das Mapping frei gewählt werden. Wichtig ist nur, dass ein Mapping des im Verzeichnisdienst gewählten Attributes durch das dafür im RFC vorgesehenen Attribut definiert wird („shadow uid sAMAccountName“ für dieses Beispiel).

Nachdem „LDAP-Benutzer“, „LDAP-Passwort“, „Search-Scope“ und „Search Base“ angegeben wurden, können die Filter und Mappings definiert werden. Der LDAP-Benutzer wird benötigt, um Informationen aus dem AD auslesen zu können und ist im Normalfall kein Benutzer, der sich anschließend an dem System anmelden soll.

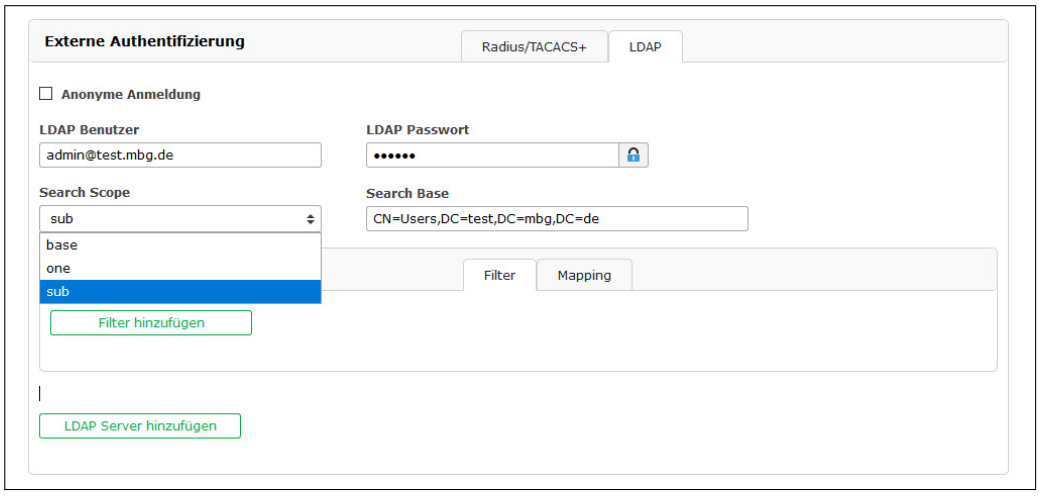


Abb.: Webinterface Menü „System → Benutzerverwaltung → Externe Authentifizierung → LDAP“

In der Beispiel-Domäne test.mbg.de wurde die „Search Base“ „CN=Users,DC=test,DC=mbg“ gewählt und der „Search-Scope“ auf „sub“ eingestellt.

Folgende Filter und Mappings müssen bei dieser Beispielkonfiguration über das Webfrontend des LTOS hinzugefügt werden.

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

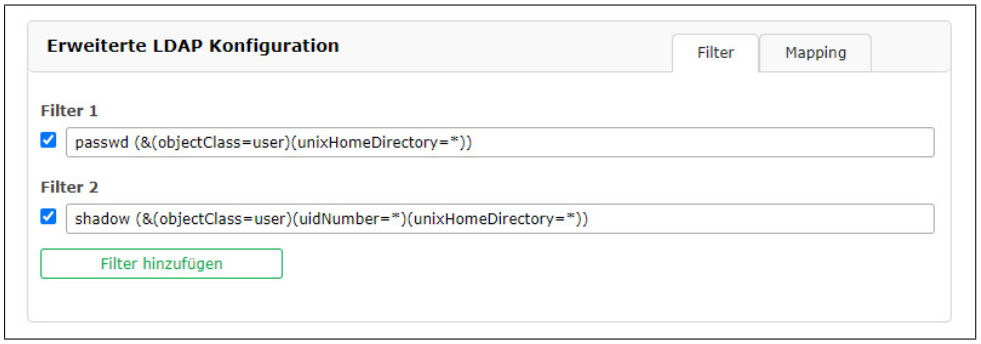


Abb.: LDAP-Submenü „Erweiterte LDAP Konfiguration → Filter“

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

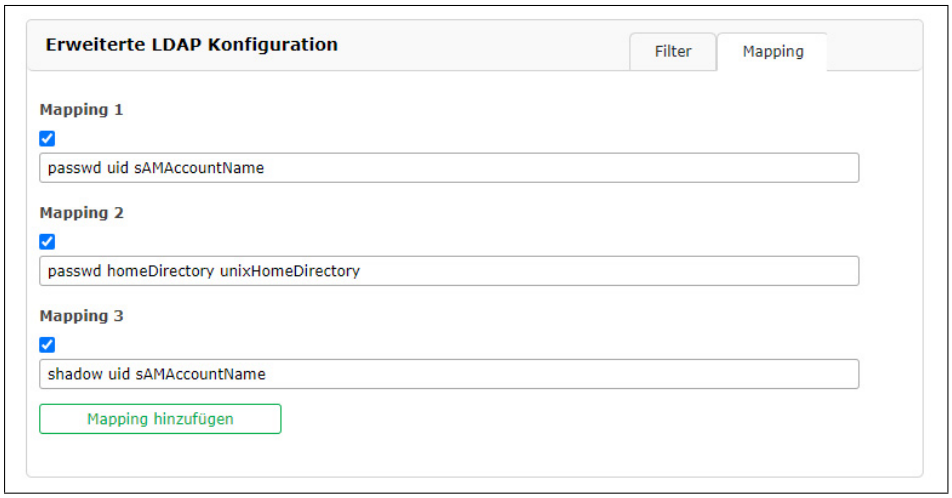


Abb.: LDAP-Submenü „Erweiterte LDAP Konfiguration → Filter“

Die gidNumber kann manchmal mit der Gruppenzugehörigkeit auf anderen Systemen kollidieren. Sprechen Sie mit Ihrem für den Verzeichnisdienst zuständigen Administrator über mögliche Vermeidungsstrategien.

Nachdem die URI des LDAP-Servers vergeben wurde, können die Einstellungen gespeichert werden. Wird LDAP als Protokoll ausgewählt, können sich die konfigurierten LDAP-Benutzer über das Webfrontend (und die CLI sofern eine loginShell für den Super-User vergeben wurde) anmelden. Wird LDAPS als Protokoll ausgewählt muss zuvor das rootca-Zertifikat, dass den LDAP-Server eindeutig identifiziert (siehe CA Zertifikate) hinzugefügt werden.

10.1.6.8 RADIUS

Radius steht für „Remote Authentication Dial In User Service“ und bietet eine zentrale Authentifizierung für LANTIME-Geräte. RADIUS ist ein Client/Server-Protokoll, das in der Anwendungsschicht läuft und UDP als Transportprotokoll verwendet.

Die LANTIME RADIUS-Authentifizierung erfordert, dass für jedes Konto, das sich am LANTIME anmelden kann, ein Vendor Specific Attribute (VSA) namens MBG-Management-Privilege-Level konfiguriert ist. Diese VSA muss der RADIUS-Konfiguration eines externen Authentifizierungsservers hinzugefügt werden. Hier einige zusätzliche Informationen zum Attribut:

```
Name = MBG-Management-Privilege-Level
Datatype = Integer
Vendor-Code = 5597
Vendor assigned attribute number = 1
Value range = 100, 200, 300
```

Zusätzlich müssen Sie für dieses Attribut für jeden RADIUS-Benutzer, der sich am LANTIME anmelden kann, einen Wert von 100 (Super User), 200 (Admin User) oder 300 (Info User) vergeben.

10.1.6.9 TACACS

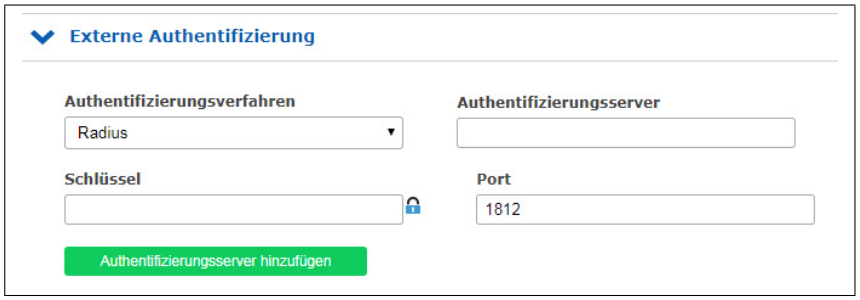
„Terminal Access Controller Acc-Control System“ ist ein Fernauthentifizierungsprotokoll, das dem LANTIME die Möglichkeit gibt, mit einem TACACS-Authentifizierungsserver zu kommunizieren.

Die LANTIME TACACS-Authentifizierung erfordert, dass jedes Konto, das sich am LANTIME anmelden können soll, ein Attribut namens „priv-lvl“ konfiguriert hat. Dieses Attribut muss auf dem TACACS-Server konfiguriert werden.

Für ein Superuser-Konto muss das Attribut „100“, für ein Admin-Konto „200“ und für ein Info-Benutzerkonto „300“ sein. Im Folgenden ein Beispiel für eine tac_plus Server-Konfigurationsdatei:

```
# 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
}
```

Authentifizierungsserver hinzufügen



Über dieses Formular können Sie der LANTIME-Konfiguration einen externen Authentifizierungsserver hinzufügen. Die externe Authentifizierung muss zuerst im Menü „Authentifizierung-Optionen“ aktiviert werden.

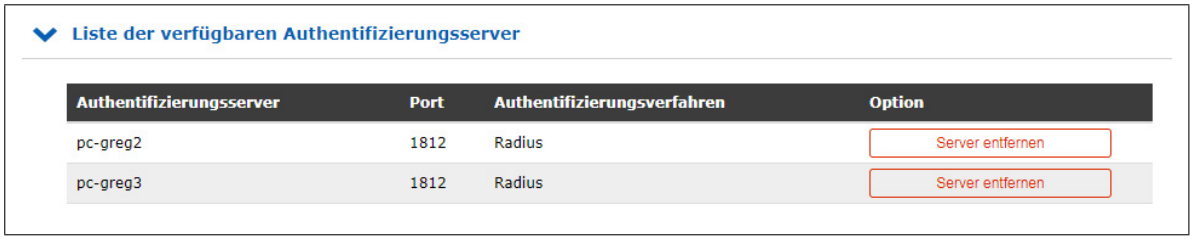
Authentifizierungsverfahren:
Konfiguration der zu verwendenden Authentifizierungsmethode, entweder Radius oder TACACS+. Detaillierte Informationen zu beiden Methoden finden Sie im oberen Teil dieses Kapitels.

Authentifizierungsserver:
Die IP oder der Host des ausgewählten Authentifizierungsservers (IPv4 und IPv6 werden unterstützt).

Schlüssel:
Ein gemeinsamer Schlüssel wird für eine grundlegende Authentifizierung zwischen einem LANTIME und dem Authentifizierungsserver verwendet. In diesem Feld muss das „Shared Secret“ des externen Authentifizierungsservers eingetragen werden. Eine Liste der zulässigen Zeichen, die für den gemeinsame Schlüssel verwendet werden können, finden Sie im Kapitel „Vor dem Start → Text- und Syntaxkonventionen“).

Port:
Abhängig von der Authentifizierungsmethode ist hier bereits der Standard-Port konfiguriert. Bei Bedarf kann der Port geändert werden.

Liste der verfügbaren Authentifizierungsserver



Diese Tabelle gibt Ihnen einen schnellen Überblick über die konfigurierten Authentifizierungsserver. Jeder Server kann entweder von einem Super- oder Admin-Benutzer entfernt werden, indem Sie auf die Schaltfläche „Server entfernen“ klicken.

10.1.6.10 Passwort - Optionen

Dieses Untermenü enthält einige allgemeine Passworteinstellungen.

Mindest-Passwortlänge:
Dieser Parameter legt die Mindestanzahl von Zeichen eines Passworts fest, bevor es vom System als gültiges Passwort akzeptiert wird. Dieser Wert wird sowohl beim Anlegen eines neuen Benutzers als auch beim Ändern eines aktuellen Benutzerkennworts verwendet. Bereits erstellte Passwörter sind davon nicht betroffen. Die maximale Länge eines Passworts beträgt 64 Zeichen.

Nur sichere Passwörter zulassen:
Wenn diese Option aktiviert ist, werden nur sichere Passwörter erlaubt. Ein sicheres Passwort benötigt mindestens:

- einen Kleinbuchstaben[a-z]
- einen Großbuchstaben [A-Z]
- einee Zahl [0-9]
- ein Sonderzeichen

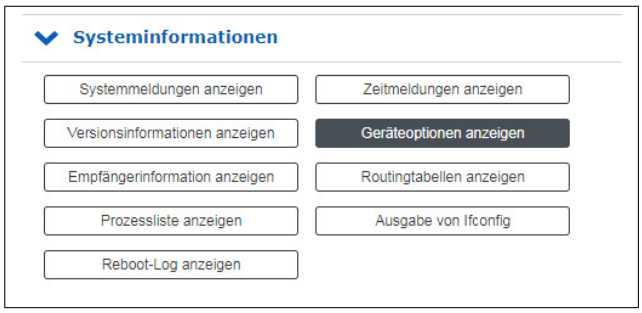
Eine Liste der zulässigen Zeichen, die als Sonderzeichen verwendet werden können, finden Sie im Kapitel „Vor dem Start → Text- und Syntaxkonventionen“.

Passwort muss zyklisch geändert werden:
Die Benutzer werden gezwungen sein, in regelmäßigen Abständen Passwörter zu ändern. Wenn ein Passwort abgelaufen ist, kann sich der Benutzer nicht am Gerät anmelden, bevor er sein aktuelles Passwort geändert hat. Mögliche Intervalle sind:

- Monatlich
- Quartalsweise
- Halbjährlich
- Jährlich

Autovervollständigung von Passwörtern deaktivieren:
Nachdem diese Funktion aktiviert ist, wird Ihr Browser die Anmeldeinformationen eines LANTIME nicht automatisch vervollständigen.

10.1.6.11 Systeminformationen



Das Menü „Systeminformationen“ bietet die Möglichkeit, wichtige Protokolldateien und Einstellungen des LANTIME anzuzeigen.

Systemmeldungen anzeigen: Anzeigen der LANTIME SYSLOG-Datei, die in */var/log/messages* gespeichert ist.

Versionsinformationen anziegen: Anzeige der zusätzlichen Geräteinformationen (Modell, Firmware, Seriennummer, eingebaute Hardwarekomponenten, etc.)

Empfängerinformation anzeigen: Anzeige der zusätzlichen Statusinformationen der eingebauten Referenzuhr.

Prozessliste anzeigen: Anzeige aller aktuell laufenden Prozesse.

Reboot Log anzeigen: Anzeigen der in */mnt/flash/data/reboot.log* gespeicherten Reboot-Logs. Die Protokolldatei enthält Informationen über frühere Systemneustarts.

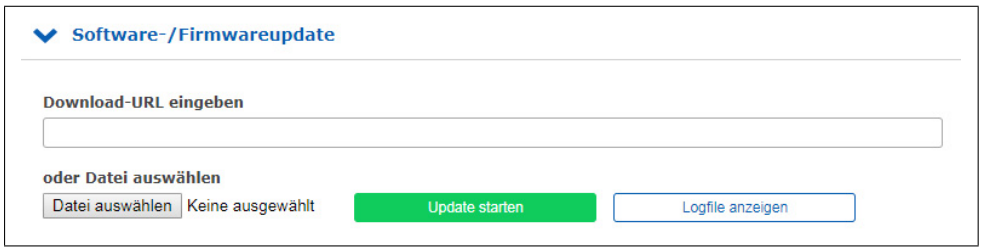
Zeitmeldungen anzeigen: Anzeige der Datei */var/log/lantime_messages*.

Geräteoptionen anzeigen: Anzeige zusätzlicher Systemparameter.

Routingtabelle anzeigen: Anzeige der Netzwerk-Routingtabelle.

Ausgabe von Ifconfig: Anzeige von Informationen für alle Netzwerkschnittstellen (Ausgabe des Befehls „ifconfig -a“)

10.1.6.12 Software-/Firmwareupdate



Wenn Sie die Firmware Ihres LANTIME aktualisieren müssen, benötigen Sie eine bestimmte Aktualisierungsdatei. Sie können die neueste LANTIME-Firmwareversion von unserer Website herunterladen:
https://www.meinberg.de/german/sw/firmware.htm

Die Aktualisierungsdatei kann auf den LANTIME hochgeladen werden, indem Sie zuerst die Datei auf Ihrem lokalen Computer mit der Schaltfläche „Durchsuchen“ auswählen und dann auf „Update starten“ klicken. Danach werden Sie aufgefordert, den Start des Aktualisierungsprozesses zu bestätigen.

Es werden bei der Installation möglicherweise Fehler festegestellt, wie z.B. ein unbrauchbares Update-File oder eine fehlende Signatur der Update-Datei. Aus Sicherheitsgründen werden bei der Installation einige Informationen angezeigt. Nachfolgend ein Auszug von möglichen Warn- bzw. Infomeldungen:

An error occured while checking update file - Update aborted.

Running Preflight Checks

```
Checking digital signature of file ...
WARNING: Could not verify digital signature of update file: Error: invalid file format/type.

WARNING: This file does not seem to have been digitally signed, please double check that it is a valid
update file and has not been corrupted/modified.

INFO: Version information in update file: 6.24.21.
OK: Installation file is readable.
INFO: This is a release file, image version is 6.24.21
OK: Update file is suitable for this system [x86].

ERROR: This update does not provide the following required features: cq7atom_support
```

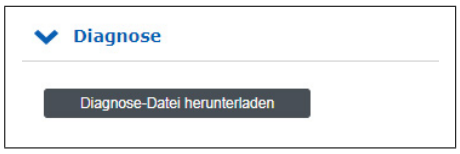
In diesem Beispiel wird versucht ein Update-Paket zu installieren, welches den Q7-Prozessor der CPU nicht unterstützt.

LANTIME - Updates für Referenzuhren und HPS-Module
Bitte beachten Sie, dass „Refclock Updates“ und „HPS100 Firmware Updates“ nur auf Systemen durchführbar sind, die mit einer LANTIME Firmware LTOS > 6.24.013 laufen.

Auf dieser Seite finden Sie die aktuellsten Firmware-Update Pakete:
https://www.meinberg.de/german/sw/refclock-updates.htm

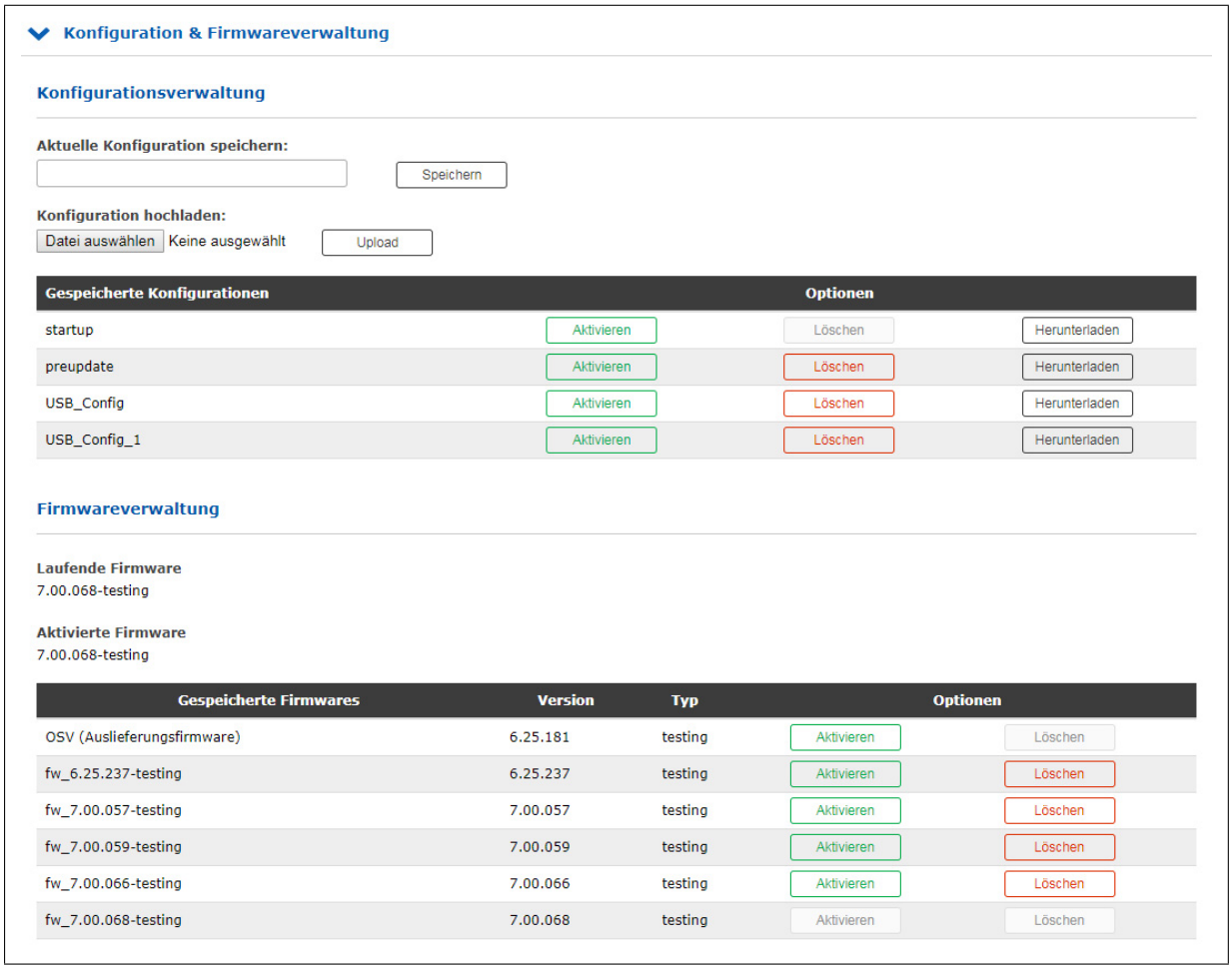
Hinweis: Nach einem erfolgten Modul-Update wird keine neue Firmware-Version im Firmware-Management angezeigt. Refclock- und HPS100-Updates sind sofort nach dem Reboot aktiv.

10.1.6.13 Download Diagnosedatei



Eine Diagnosedatei, die alle Statusdaten eines, seit dem letzten Neustart protokollierten, LANTIME-Systems enthält, kann von allen LANTIME-Servern heruntergeladen werden. Das Dateiformat der Diagnosedatei ist ein tgz-archiv. Das Archiv enthält alle wichtigen Konfigurationen und Logfiles. In den meisten Support-Fällen ist es die erste Aktion, den Benutzer aufzufordern, die Diagnose-Datei herunterzuladen, da es sehr hilfreich ist, den aktuellen Zustand des LANTIME zu identifizieren um mögliche Fehler zu finden.

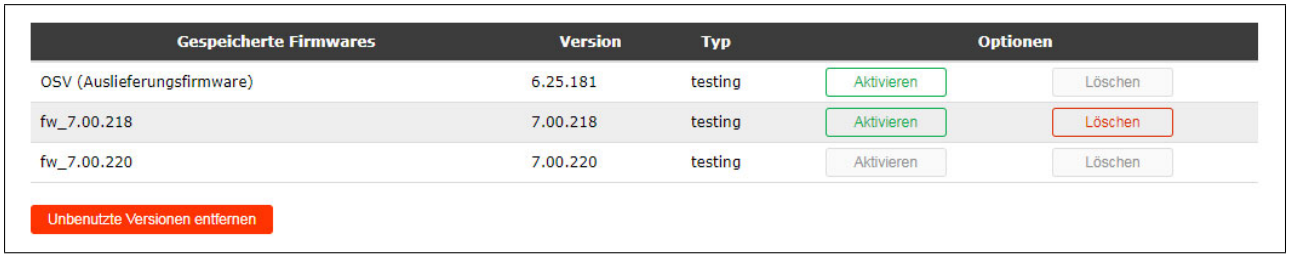
10.1.6.14 Konfiguration und Firmwareverwaltung



In diesem Menü können Sie verschiedene Konfigurationsdateien zur Sicherung auf dem Flash-Speicher des LANTIME sichern. Mit der Schaltfläche „Aktivieren“ kann eine gespeicherte Konfiguration geladen werden, mit der Schaltfläche „Löschen“ kann eine Konfigurationsdatei gelöscht und mit der Schaltfläche „Download“ eine Datei heruntergeladen werden.

Zusätzlich kann mehr als eine Firmware-Version auf dem LANTIME archiviert werden. Wenn eine aktualisierte Version in der Umgebung nicht korrekt arbeitet, ist es möglich, eine der etablierten Versionen im LANTIME wieder zu aktivieren.

Unbenutzte Versionen entfernen



Mit dieser Schaltfläche können alle nicht genutzten Firmware-Versionen gelöscht werden. Es bleiben nur die aktive Firmware und die OSV (Original Shipped Version) auf dem System erhalten.

10.1.6.15 Display

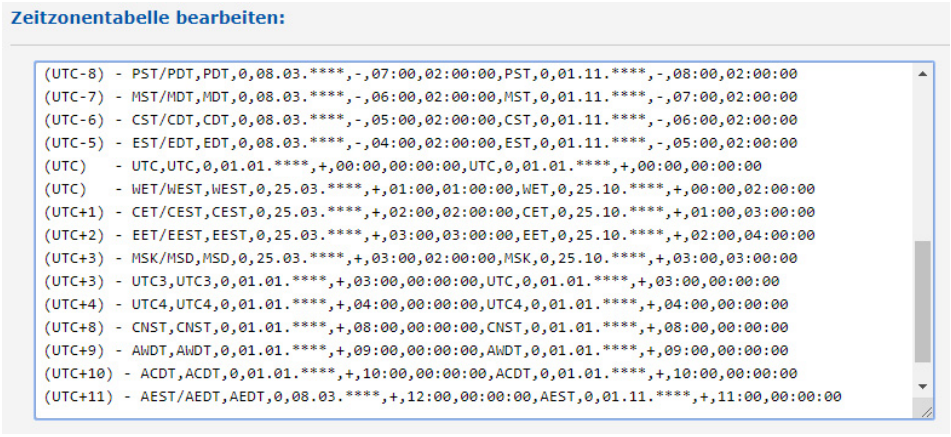
Displaybeleuchtung dauerhaft aktivieren:
Über dieses Kontrollkästchen kann die Displaybeleuchtung der Frontplatte dauerhaft eingeschaltet werden.

Zeitzone:
Zeit- und Zeitzoneneinstellung für das LANTIME-Display, die im Abschnitt „Datum/Uhrzeit“ auf der Startseite der Weboberfläche angezeigt wird.

Hinweis: Diese Einstellung hat keinen Einfluss auf die Zeit, die vom LANTIME über NTP, PTP, serielle Zeitstrings oder IRIG bereitgestellt wird.

Ausnahme:
Falls NTP so konfiguriert ist, dass es anstelle von UTC eine Ortszeit bereitstellt, müssen Sie hier in der Einstellung der Anzeigezeitzone die genaue Ortszeitzone konfigurieren. Diese Einstellung wird dann auch für NTP verwendet.

Zeitzonentabelle bearbeiten:
Mit der Schaltfläche „Zeitzonentabelle bearbeiten“ können Sie neue Zeitzonendefinitionen hinzufügen.



Beispiel:

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

Diese Zeichenkette ist die Zeitzonendefinition für Mitteleuropa. Wenn Sie eine neue Zeitzoneneinstellung benötigen, muss diese im gleichen Format konfiguriert werden. Die Zeichenkette enthält verschiedene Informationen, jede Information ist durch ein Komma getrennt. Eine detaillierte Beschreibung der verschiedenen Zeichenkettenteile am Beispiel der Zeitzoneneinstellung für Mitteleuropa ist wie folgt:

1. Feld: Anzeigename der Zeitzone. Dieser Name wird in der Liste der verfügbaren Zeitzonen angezeigt → (UTC+1) - CET/CEST

2. Feld: Abkürzung der Zeitzone mit Sommerzeit (max. 4 Buchstaben) → CEST

3. Feld: Wochentag der Umstellung auf Sommerzeit → 0 = (Sonntag)

4. Feld: Datum der Umstellung auf Sommerzeit (dd.mm.****) → 25.03.****
(Die Umstellung erfolgt am ersten Sonntag ab dem 25.03.)

5. Feld: Vorzeichen (+ oder -), addieren oder subtrahieren des Offsets von UTC → +

6. Feld: UTC-Offset Sommerzeit (hh:mm) → 02:00

7. Feld: Umschaltzeitpunkt → 02:00

8. Feld: Abkürzung der Standardzeitzone → CET

9. Feld: Wochentag der Umstellung auf Standardzeit → 0 (Sonntag)

10. Feld: Datum der Umstellung auf die Standardzeit (dd.mm.****) →
25.10.**** (Die Umstellung auf die Normalzeit erfolgt am ersten Sonntag ab dem 25.10.)

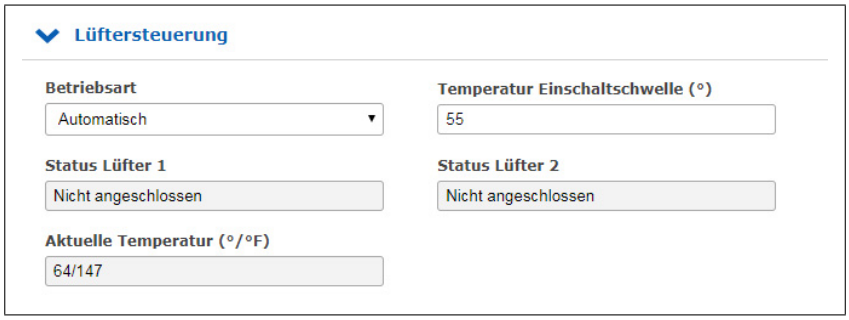
11. Field: Vorzeichen (+ oder -), addieren oder subtrahieren des Offsets von UTC → +

12. Field: UTC-Offset (hh:mm) → 01:00

13. Field: Zeitpunkt der Umstellung → 03:00

10.1.6.16 Lüftersteuerung

Diese Parameter sind nur bei LANTIME IMS-Geräten mit eingebautem Lüftermodul konfigurierbar.



Betriebsart: Einstellung der Betriebsart. Die folgenden Optionen stehen zur Verfügung:

Automatisch: In diesem Modus schalten sich die Lüfter automatisch ein, sobald die aktuelle Systemtemperatur den eingestellten Temperaturschwellenwert überschreitet.

Ein: In diesem Modus laufen die Lüfter permanent.
Aus: In diesem Modus sind die Lüfter dauerhaft ausgeschaltet.

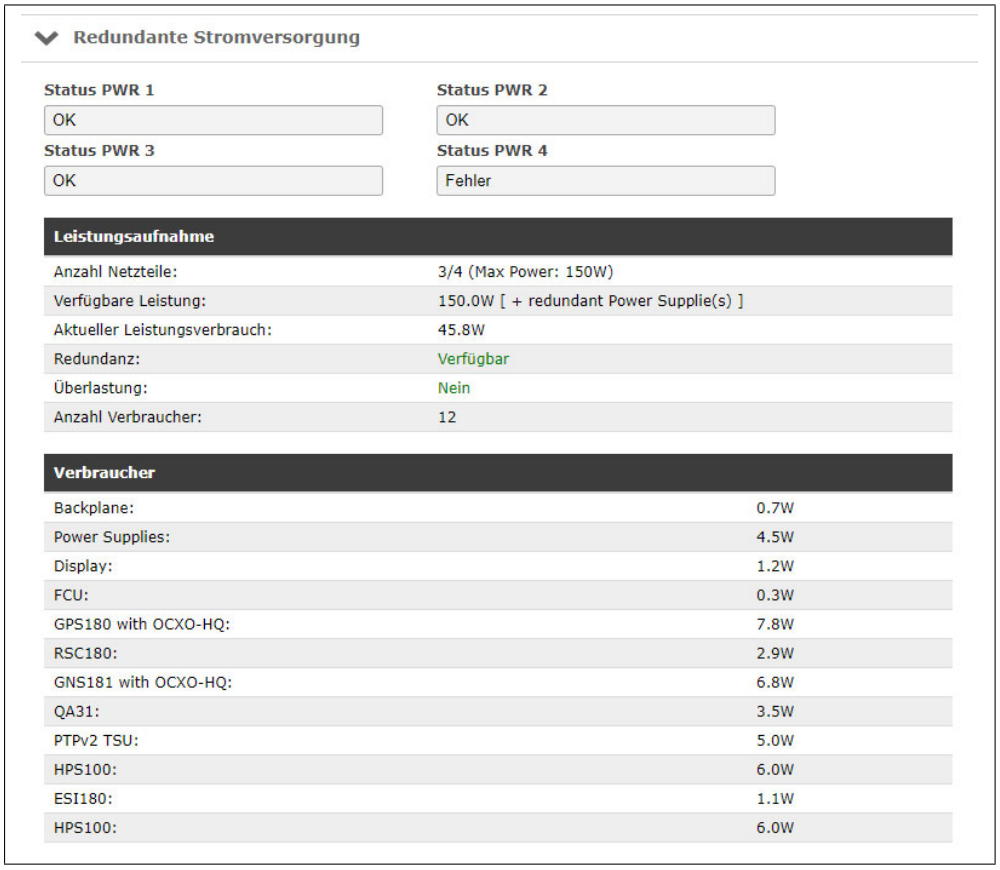
Temperatur Einschaltschwelle (°): Angabe der Systemtemperaturschwelle in Grad Celsius. Der konfigurierte Temperaturwert wird bei der Steuerung des Lüfters berücksichtigt, wenn der Lüftermodus „Automatisch“ gewählt ist.

Status Lüfter 1: Statusanzeige des 1. Lüfters.
Status Lüfter 2: Statusanzeige des 2. Lüfters.

Aktuelle Temperatur (°/°F): Anzeige der aktuellen Temperatur in Grad Celsius und Fahrenheit.

10.1.6.17 Redundante Stromversorgung

Falls es sich bei Ihrem LANTIME um ein IMS System handelt, werden in diesem Untermenü alle verfügbaren Netzteile angezeigt und ausgewertet.



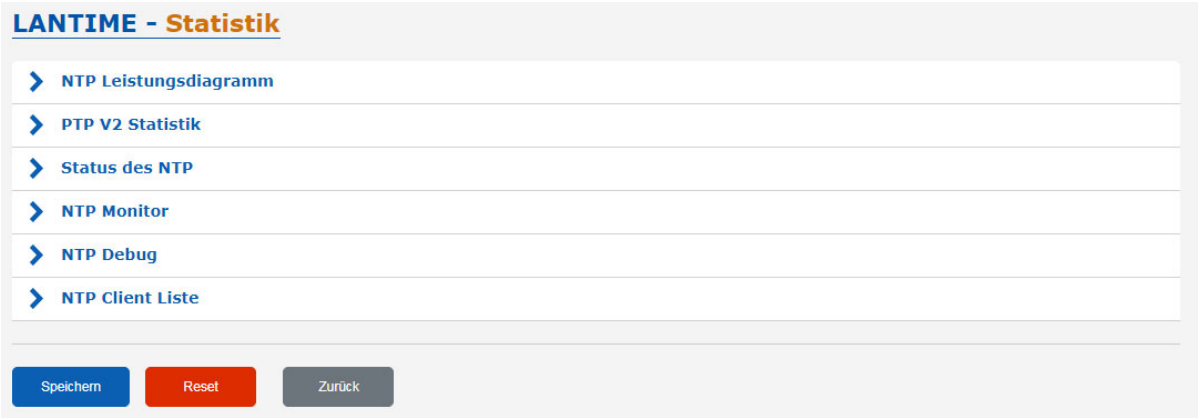
Leistungsaufnahme
Die verfügbare Leistung ergibt sich aus der Anzahl der eingesetzten Netzteile. Im Beispiel haben wir drei Netzteile mit jeweils 50 Watt Leistung - das ergibt in der Summe 150 Watt wenn alle Netzteile mit Spannung versorgt werden.

Solange, wie in diesem Beispiel, in der Reihe „Aktueller Leistungsverbrauch“ ein Wert kleiner 50W angezeigt wird, reicht ein Netzteil aus um das System zu versorgen. Bei einem Wert größer oder gleich 50W werden zwei Netzteile zur Versorgung bzw. drei aktive Netzteile benötigt um Redundanz zu gewährleisten.

Das Feld „Redundanz“ steht auf „verfügbar“, wenn die „Verfügbare Leistung“ minus dem „Aktuellen Leistungsverbrauch“ größer oder gleich 50W ist. Das Feld „Überlastung“ zeigt immer „Nein“ an, solange der „Aktuelle Leistungsverbrauch“ kleiner oder gleich der „Verfügbaren Leistung“ ist.

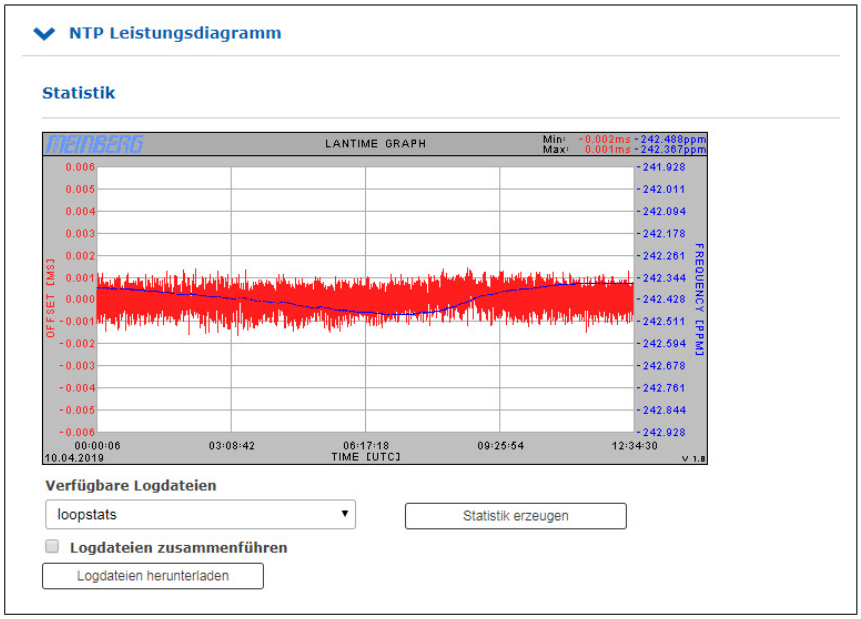
Verbraucher
In dieser Tabelle werden alle Verbraucher des Systems aufgelistet. Die Backplane, die CPU, die Netzteile, die Empfänger und alle anderen eingesetzten Module. Die Summe aller Verbraucher ergibt den Wert, der als „Aktueller Leistungsverbrauch“ angezeigt wird.

10.1.7 Statistik



10.1.7.1 NTP Leistungsdiagramm

Im Untermenü NTP-Leistungsdiagramm werden die NTP-Statistiken (Loopstats) in Form eines Graphen dargestellt.



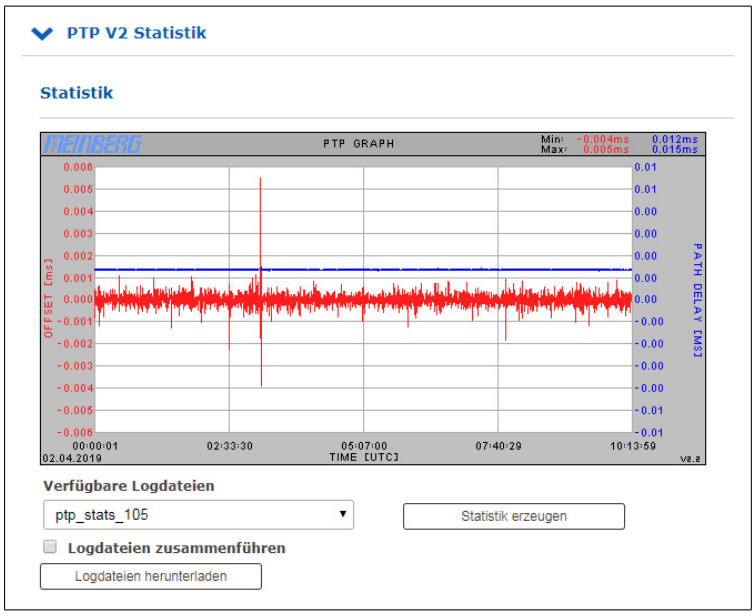
Die roten Linien und die primäre Y-Achse stellen den Versatz zwischen der Systemzeit und der NTP-Referenzzeitquelle (in ms) dar. Die blaue Linie und die sekundäre Y-Achse hingegen veranschaulichen die Frequenzanpassung des Oszillators, der vom ntpd (in PPM) auf der CPU aufgebaut ist, um die Systemzeit an die Referenzzeitquelle anzupassen.

Der minimale und maximale Messwert der Frequenzabweichung und der Offsets kann in der rechten oberen Ecke der Abbildung abgelesen werden.

Verfügbare Logdateien:
Sie können die verfügbaren Protokolldaten über das Dropdown-Menü auswählen. Die ntpd erstellt für jeden Tag eine neue Loopstats-Datei.

Logdateien zusammenführen:
Nach dem Aktivieren des Kontrollkästchens und dem Klicken auf „Statistik erzeugen“ werden alle verfügbaren Protokolldateien zusammengeführt und als eine Grafik angezeigt.

10.1.7.2 PTP V2 Statistik

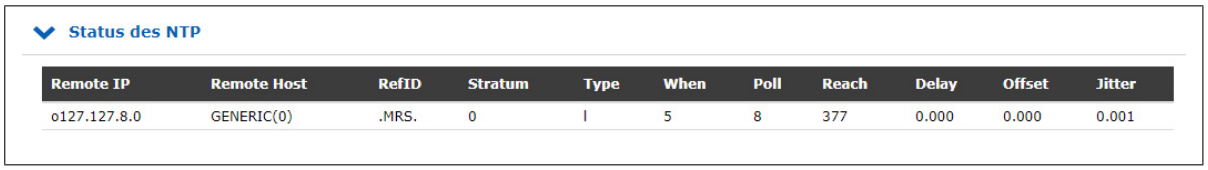


Diese Grafik ist nur verfügbar, wenn der LANTIME mit einem PTP-Modul ausgestattet ist, das als PTP-SLAVE konfiguriert ist.

Die rote Linie zeigt den zeitlichen Abstand zwischen der Zeit des eingebauten Referenztaktgebers und dem eingehenden PTP-Signal (in Mikrosekunden). Die blaue Linie zeigt die vom PTP-Modul bestimmte Wegverzögerung (Path Delay).

10.1.7.3 NTP Status

In diesem Menü wird die Ausgabe des NTP-Befehls „ntpq -p“ angezeigt. Der Befehl listet alle Referenzzeitquellen (Peers) auf, die dem NTP-Dienst zur Verfügung stehen. Das folgende Beispiel zeigt die Ausgabe „ntpq -p“ eines LANTIME mit eingebauter GNSS-Referenzuhr und 2 konfigurierten externen NTP-Zeitservern:


Status des NTP

Remote IP	Remote Host	RefID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
o127.127.8.0	GENERIC(0)	.MRS.	0	l	5	8	377	0.000	0.000	0.001

Remote IP:
IP-Adresse des NTP-Peers oder 127.127.x.x.x, wenn es sich um eine Hardware-Zeitreferenz handelt, z.B. eine Funkuhr oder einen GPS-Empfänger.

Eine Legende von Codes, die neben jeder IP-Adresse von NTP-Peers stehen, ist wie folgend:

‘*‘	Dieser Server ist für die Synchronisation ausgewählt.
‘o‘	Die Systemsynchronisation wird aus einem Puls pro Sekunde (PPS) Signal abgeleitet, entweder indirekt über den PPS-Referenztakttreiber oder direkt über eine Kernel-Schnittstelle.
‘+‘	Der Peer ist ein Kandidat für die Synchronisation.
‘-‘	Der Server ist nicht für die Synchronisation geeignet.
‘x‘	Der Server wird als Falseticker erkannt und ist nicht für die Synchronisation geeignet.
‘#‘	Der Server ist ein „Überlebender“, aber nicht unter den ersten sechs Servern.
“	Der Peer wird als nicht erreichbar verworfen oder mit diesem Server synchronisiert (Sync-Loop).

Remote Host:
Aufgelöster DNS-Name

RefID:
Die Zeitreferenz des NTP-Peers.

Stratum:
Stratumwert des NTP-Peers.

Type:
Typ des NTP-Peers:

l:	Lokaler Referenztaktgeber
b:	Broadcast oder Multicast
u:	Unicast
s:	symmetrischer Peer
a:	Manycast

When:
Wert in Sekunden. Zeigt an, wann der NTP-Peer zuletzt abgefragt wurde.

Poll:
Zeitraum in Sekunden. Gibt das Intervall an, in dem der NTP-Peer abgefragt wird.

Reach:
Oktalwert. Zeigt den Status der letzten 8 Abfragen an. Der Wert „377“ bedeutet, dass die letzten 8 Abfragen erfolgreich waren.

Delay:
Wert in ms. Zeigt die Laufzeit des NTP-Pakets an.

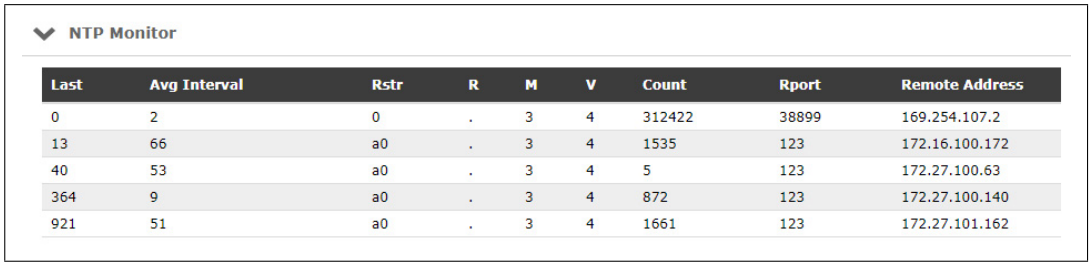
Offset:
Die NTP-Software vergleicht in regelmäßigen Abständen ihre eigene Systemzeit mit ihren Referenzzeitquellen. Dieser Prozess wird als „Polling“ bezeichnet. Nach jedem Polling-Vorgang wird die Paketauslösezeit ermittelt, berechnet und die aktuelle Zeitdifferenz („Offset“) berechnet und in Millisekunden angezeigt.

Jitter:
Die Paketübertragungszeit ändert sich mehr oder weniger je nach den Eigenschaften des Netzwerks während des „Pollings“ externer NTP-Quellen bei jedem Zeitvergleich, und auch der berechnete Zeitversatz variiert. Aus diesem Grund werden die Ergebnisse aufeinanderfolgender Zeitvergleiche gefiltert, indem gewichtete Mittelwerte für Paketlaufzeit und Zeitabstand berechnet werden. Die Abweichungen der einzelnen Werte von diesen Mittelwerten werden als „Jitter“ bezeichnet, und je höher der Jitterwert, desto ungenauer ist der berechnete Zeitabstand. Andererseits zeigt ein stetig zunehmender mittlerer Zeitversatz an, dass die Systemzeit von der Referenzzeit abweicht. Der Wert wird in Millisekunden angezeigt.

10.1.7.4 NTP Monitor

Das Untermenü „NTP Monlist“ listet alle NTP-Clients auf, die die LANTIME-Zeit über NTP abgefragt haben. Die Liste wird mit dem NTP Query-Tool erstellt und angezeigt. Der folgende ntpq-Befehl wird ausgegeben: *ntpq -c mrulist*

Weitere Informationen über das NTP Query-Tool finden Sie in der NTP-Dokumentation unter:
http://doc.ntp.org/current-stable/ntpq.html



Last:
Zeit in Sekunden. Gibt an, wann der Client die Zeit vom LANTIME angefordert hat.

Avg Interval:
Intervall: Durchschnittliche Zeit in Sekunden zwischen zwei NTP-Anfragen.

Rstr:
Zeigt an, ob für diese Remote-IP Restrict Flags aktiv sind.

R:
Zeigt an, ob die „Rate Control“ aktiv ist oder nicht.

M:
NTP-Paket-Identifikation
0 → reserved
1 → symmetric active
2 → symmetric passive
3 → client
4 → server
5 → broadcast
6 → NTP control message
7 → reserved

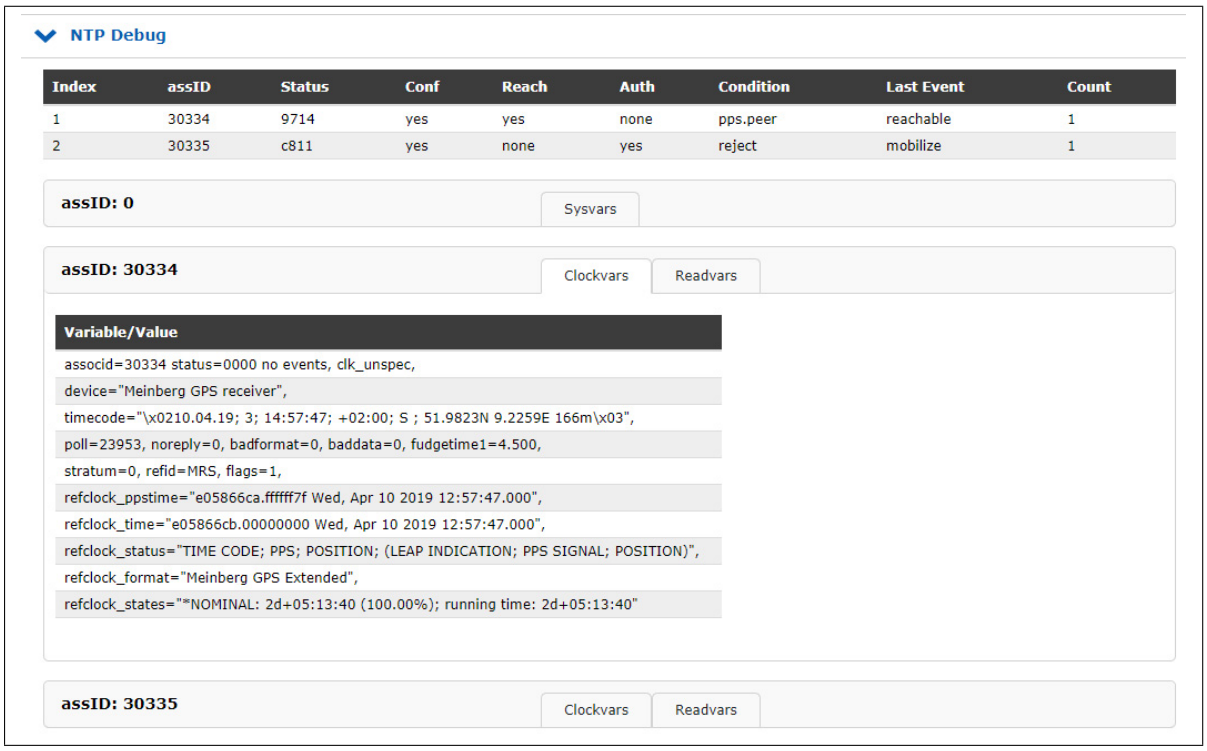
V:
NTP Version

Count:
Anzahl der von der entfernten Adresse empfangenen Pakete

Rport:
„Quell-Port“ des letzten empfangenen Pakets

Remote Address:
IP-Adresse des anfragenden Gerätes

10.1.7.5 NTP Debug



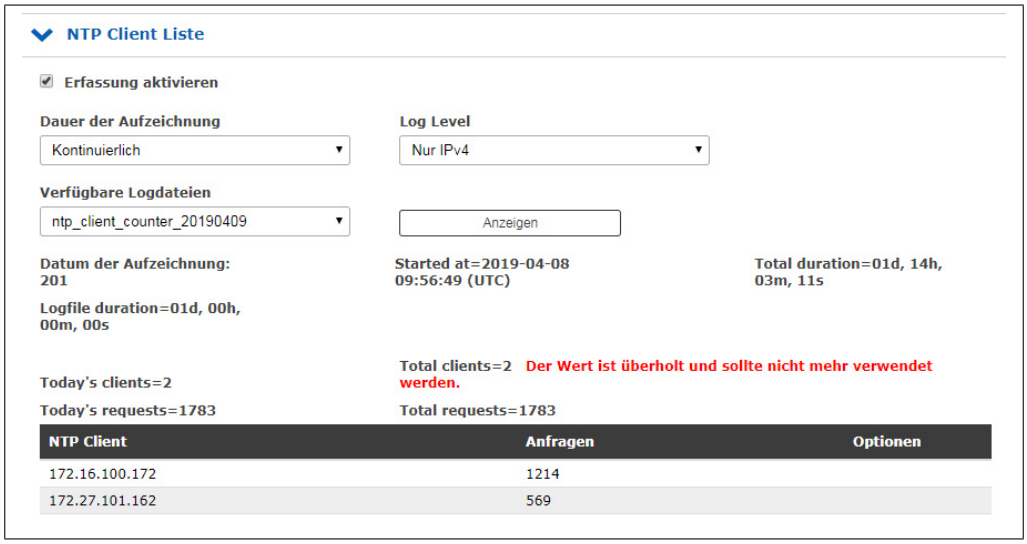
Das NTP Debug-Menü zeigt NTP-Debug-Informationen an, die vom LANTIME mit dem NTP Query-Tool (ntpq) abgefragt wurden. Das „ntpq“ wird mit den folgenden Parametern ausgeführt:

- „clockvar“
- „associations“
- „readvar“

Weitere Informationen über das Abfragetool finden Sie in der NTP-Dokumentation unter:
http://doc.ntp.org/current-stable/ntpq.html

10.1.7.6 NTP Client Liste

Zusätzlich zu den nativen NTP-Logging-Funktionen bietet der LANTIME die Möglichkeit, eine Liste aller NTP-Clients zu führen. Die Funktion ist standardmäßig ausgeschaltet und kann bei Bedarf aktiviert werden.



Erfassung aktivieren:
Aktiviert diese Funktion im LANTIME.

Dauer der Aufzeichnung:
Die Dauer, für die der LANTIME die Client-Liste führt. Bei der Konfiguration der kontinuierlichen Aufzeichnung werden alte Tagesstatistiken nach wenigen Tagen automatisch gelöscht um Platz zu sparen.

Log Level:
Legt fest, welche Version des IP-Protokolls berücksichtigt wird. Erhältlich sind IPv4, IPv6 oder beide Versionen in Kombination.

Verfügbare Protokolldateien:
Wenn die Client-Protokollierung aktiviert ist, werden an dieser Stelle Protokolldateien zur Anzeige bereitgestellt. Wählen Sie im Auswahlfeld die gewünschte Tagesstatistik aus und verwenden Sie die Schaltfläche „Anzeigen“, um die Statistik anzuzeigen. Sie erhalten dann eine entsprechende Client-Liste sowie weitere Statistiken.

NTP Client	Anfragen	Optionen
172.16.100.172	1214	Details
172.27.101.162	569	Details

Ein Klick auf Details zeigt Ihnen nun auch detaillierte Informationen über die empfangenen NTP-Pakete eines bestimmten Clients.

- Die Spalten 0-23 zeigen die Stunde des Tages an.
- Die 3 zusätzlichen Zeilen liefern Informationen darüber, ob das empfangene NTP-Paket den Modus 3, 4 oder einen anderen hat.
- Modus 3 → Client
- Modus 4 → Server

10.1.8 Sync Monitoring

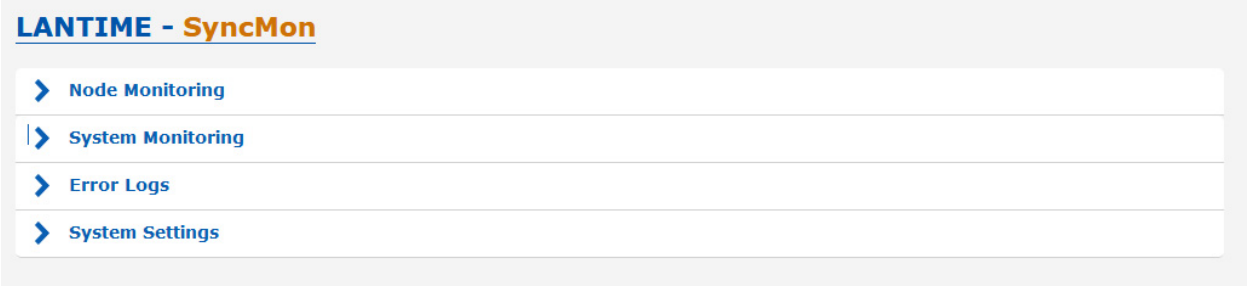


Abbildung: Der Sync-Monitor-Dialog im LANTIME Webinterface.

10.1.8.1 Einleitung Sync Monitor

Die Funktion **Sync Monitoring** dient zum Messen, Überwachen und Berichten der Genauigkeit von Netzwerkknoten gegenüber einer UTC-rückverfolgbaren Quelle (z.B. GPS, Multi-GNSS oder lokalem Zeitdienst, z.B. NPL). Sync Monitoring kann Knoten überwachen, die über die Netzwerkprotokolle PTP (IEEE 1588v2) oder NTP (RFC1305) synchronisiert sind.

PTP-Knoten müssen den Meinberg TLV-Ansatz oder Standard-PTPv2-Management-Meldungen unterstützen, da sie sonst nicht überwacht werden können. NTP-Knoten können nur überwacht werden, wenn sie so konfiguriert sind, dass sie auf NTP-Client-Anfragen reagieren (Hinweis: Ein NTP-Client, der den Windows Time-Service W32Time verwendet, reagiert nicht auf NTP-Client-Anfragen gemäß Standardkonfiguration. W32Time muss konfiguriert werden, um gleichzeitig als Client und Server zu fungieren. Andernfalls kann der Knoten nicht über SyncMon überwacht werden).

Es können aber auch alle konfigurierten MRS-, FDM-, PIO- und ESI-Eingänge (wie PPS- und Frequenz-Eingänge) überwacht werden, wenn eine ESI-Karte (Extension Signal Input) vorhanden ist. Die Funktion Sync Monitor ist ab sofort auf Meinberg IMS-Systemen mit Firmware-Version 7.00 oder höher und für die PTP-Überwachung mit integrierter HPS-100 PTP-Karte mit einer Lizenz von mindestens 1024 Clients verfügbar.

Der Sync-Monitor kann auch als Knoten unabhängig von einer Hauptuhr ausgeführt werden. In diesem Fall kann ein Sync-Monitor-Knoten grundsätzlich überall im Netzwerk platziert werden - dann aber so nah wie möglich an den Slaves, um deren tatsächliche Genauigkeit messen zu können. Gleichzeitig können Sie auch die Leistung einer Grandmaster-Clock überwachen und die potenzielle Netzwerkasymmetrie messen, die in der Verbindung zwischen einem GM und dem Sync-Monitoring-Knoten vorhanden ist.

Es ist möglich, bis zu 1000 Knoten für die Überwachung in der Sync Monitoring-Schnittstelle zu konfigurieren, die auf einem Standard-LANTIME- oder IMS-System läuft. Sie können Überwachungs- und Protokollierungsintervalle für jeden einzelnen Knoten separat festlegen. Außerdem kann für jeden Knoten eine Offset-Grenze konfiguriert werden, die bei Überschreitung des Grenzwertes für diesen Knoten eine Alarmmeldung auslöst (über SNMP, E-Mail oder einen benutzerdefinierten Kanal). Für NTP-Knoten können Sie auch ein Stratum-Limit definieren, der auch bei Überschreitung des definierten Levels eine Alarmierung auslösen kann.

Darüber hinaus ist es für jeden Knoten möglich, alle Überwachungsdaten und deren Protokolldateien herunterzuladen, die zur Erstellung eines Berichts oder für weitere statistische Analysen verwendet werden können. Die Daten jedes überwachten Knotens können online über das SYSLOG-Protokoll mit verschiedenen Formaten gesendet werden oder ein „rsync"-Dienst zum Kopieren der Messdaten auf einen externen Datenserver aktiviert werden. Online-Daten jedes Knotens können über den WEB-Service wie *„curl"* oder *„wget"* im JSON-Format gelesen werden, um aktuelle Daten in anderen Managementsystemen zu verwenden.

Eine JSON-Datei für jeden Knoten ist verfügbar unter: */www/htdocs/syncmon/[alias].json*, wobei[alias] ein Platzhalter für den Node-Alias ist.

10.1.8.2 Sync Monitor - Erste Schritte

Beim ersten Start von SyncMon wird keine Überwachung aktiviert. Um die Überwachung zu aktivieren, muss mindestens ein Knoten hinzugefügt werden. Klicken Sie auf die Schaltfläche „Add Node“, um einen neuen Überwachungsknoten hinzuzufügen.

10.1.8.3 Sync Monitor Status und Konfiguration

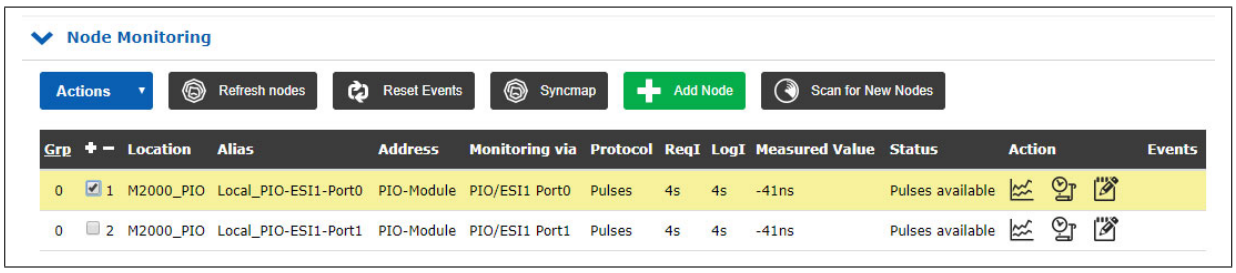


Abbildung: Sync Monitor Benutzeroberfläche auf LANTIME-Systemen mit einer FW 7.00 oder höher.

Das „Node Monitoring“ zeigt den aktuellen Status und die Konfiguration aller überwachten Knoten an. Ein Überwachungsknoten kann entweder ein Gerät im Netzwerk wie NTP-Server oder PTP-Systeme oder ein Lantime-spezifisches Eingangsmodul für z.B. Impulse oder Frequenzen sein. Jede Zeile in der Tabelle repräsentiert einen überwachten Knoten oder eine Gruppe von Knoten. Die Tabelle kann im Flat- oder Gruppenmodus angezeigt werden. Im Flat-Modus werden nur Knoten in einer Zeile angezeigt. Zur Strukturierung der Tabelle kann der Gruppenmodus durch Klick auf die Schaltfläche **„Grp“** in der ersten Spalte ausgewählt werden - alle Knoten mit der gleichen Nummer werden gruppiert und können separat geöffnet werden.

Der Status auf der WEB-Schnittstelle wird alle 10 Sekunden automatisch aktualisiert. Im Dialogfeld „Sync Monitor Status und Konfiguration“ können Sie neue Knoten hinzufügen, um deren Genauigkeit zu messen und deren Synchronisationsleistung zu überwachen. Durch Auswahl der Schaltfläche **„+ Add Node“** gelangen Sie zu einem Konfigurationsdialog, um einen neuen Knoten zur Überwachung hinzuzufügen.

Schaltfläche „Refresh nodes“:
Auf diese Weise kann man sich einen Überblick über die aktuellen Werte zu diesem Zeitpunkt verschaffen, auch wenn das Abfrageintervall höher ist. Alle konfigurierten Knoten werden aktualisiert. Eine neue Messung wird durchgeführt und der Status in der Tabelle der Knoten wird aktualisiert. Der aktualisierte Wert wird der Liste der Messwerte hinzugefügt, um den Mittelwert zu berechnen. Es wird keine Messung an allen HPS-Karten mit PTP durchgeführt.

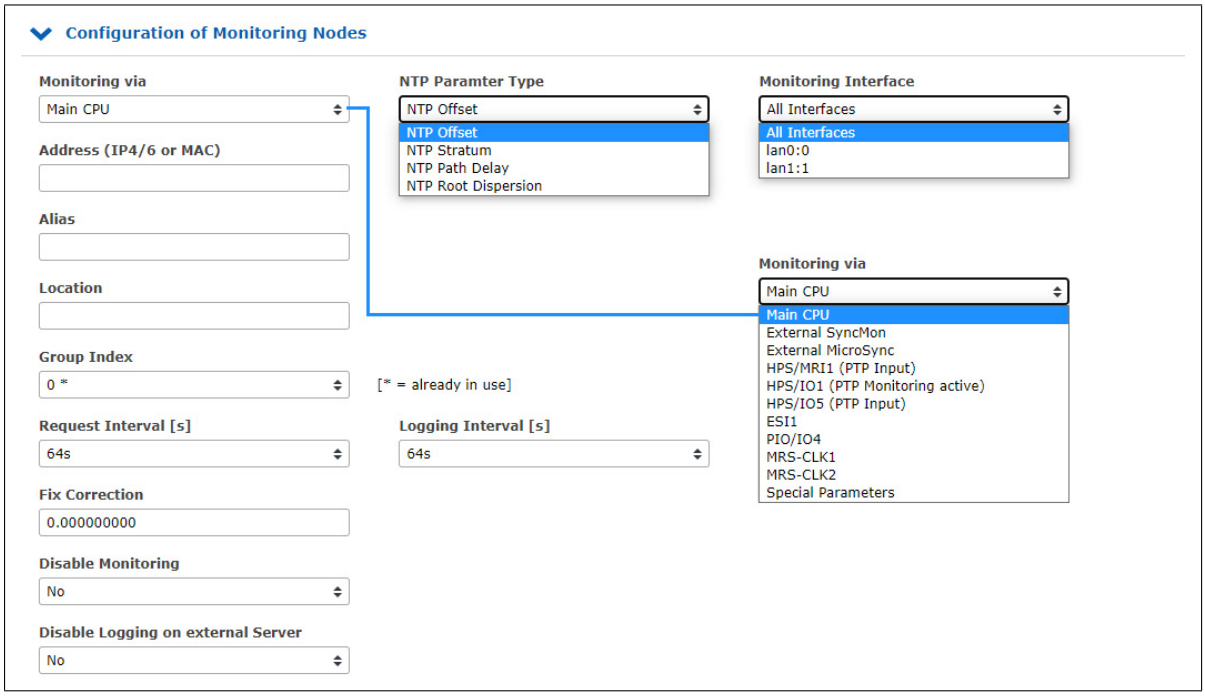
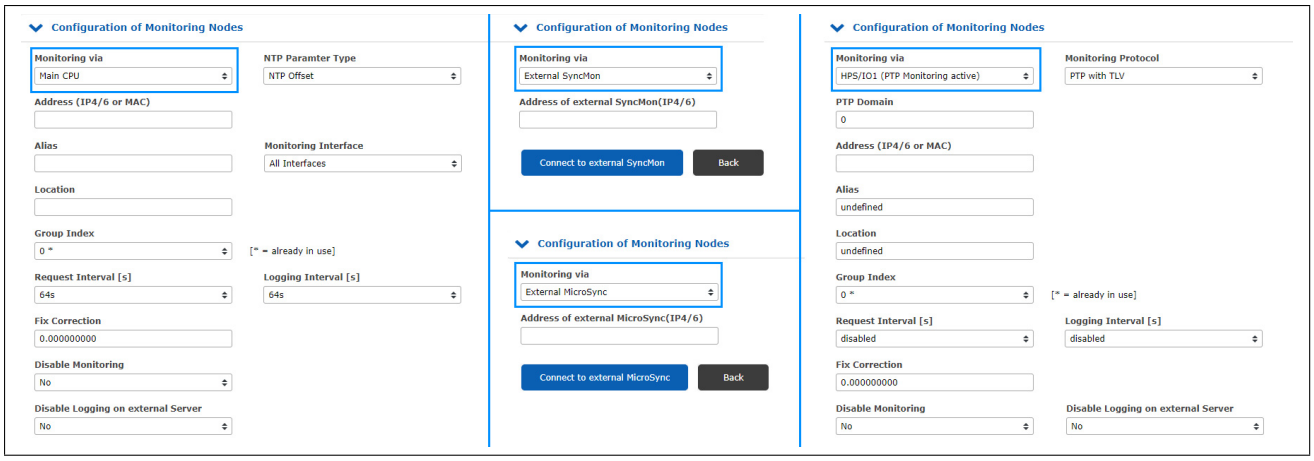


Abbildung: Add Node Konfiguration.

Die Funktionen im Konfigurationsdialog „Add Node“ hängen von der Auswahl des ersten Parameters „Monitoring über“ ab und liefern verschiedene Eingabemasken mit unterschiedlichen Optionen:



Monitoring über:
Wählen Sie eine Überwachungsinstanz aus der Dropdown-Liste aus. Die Dropdown-Liste erscheint in verschiedenen Hardwarekonfigurationen unterschiedlich. Die folgenden Optionen stehen zur Verfügung:

Main CPU: Diese Monitoring-Instanz ist immer verfügbar und unabhängig von der Hardware-Konfiguration des LANTIME-Systems. Es kann nur native NTP-Knoten überwachen, die auf NTP Client Anfragen reagieren (Hinweis: Ein NTP-Client, der den Windows Time Service W32Time verwendet, kann nicht auf NTP-Client-Anfragen antworten - gemäß Standardkonfiguration. W32Time muss konfiguriert werden, um als Client und Server zur gleichen Zeit zu agieren. Andernfalls kann der Knoten nicht über SyncMon überwacht werden). Alle zugeordneten Schnittstellen können gleichzeitig überwacht werden oder Sie können eine bestimmte Schnittstelle aus einer Liste auswählen, falls vorhanden.

Über die Auswahlbox „NTP Parameter Type“ kann ausgewählt werden, ob der „NTP Offset“, „NTP Stratum“, „NTP Path Delay“ oder „NTP Root Dispersion“ gespeichert werden soll.

Wenn mehrere Netzwerkschnittstellen vorhanden sind kann über die Auswahlbox "Monitoring Interfaceëine spezifische Schnittstelle oder alle Schnittstellen ausgewählt werden.

External SyncMon: Diese Überwachungsinstanz kann Knoten und Sensoren anderer Lantime-Geräte mit aktiviertem SyncMon überwachen. Bei der Auswahl des externen SyncMon mit IP-Adresse wird eine Liste der verfügbaren Knoten von diesem externen SyncMon heruntergeladen. Konfiguration und Daten werden über den WEB-Service (Curl) übertragen.

External Microsync: Hiermit können MRS Referenzen von externen MicroSync Geräten überwacht werden. Bei der Auswahl des externen MicroSync mit IP-Adresse wird eine Liste der verfügbaren Referenzen von diesem externen MicroSync heruntergeladen. Konfiguration und Daten werden über den WEB-Service (Curl) übertragen.

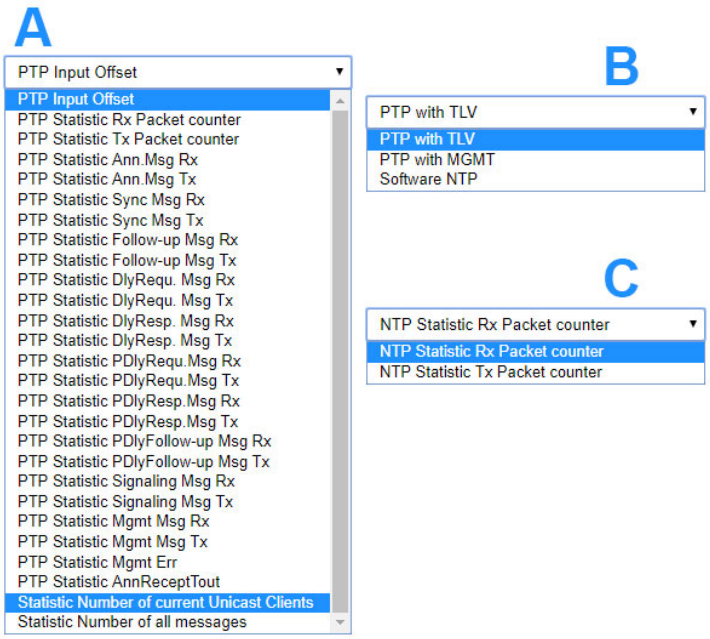
HPS: HPS100-Karten können zur Überwachung von PTP oder NTP über einen eigenen Netzwerkanschluss verwendet werden.

Wenn ein HPS-Modul als PTP-Slave konfiguriert ist (siehe Lantime PTP-Konfiguration), dann wird die HPS-Karte sich wie ein Standard-PTP-Slave verhalten, mit all seinen Optionen wie Profile und netzwerkspezifischen Konfigurationen - aber es kann immer nur ein PTP-Master zur gleichen Zeit mit einem HPS-Modul überwacht werden.

Wenn die HPS als Überwachungssystem konfiguriert werden soll (siehe Lantime PTP-Konfiguration), dann muss sie mindestens mit einer 1024er-Client-Lizenz ausgestattet sein.
Ist das der Fall, dann können mehrere PTP-Knoten über den Netzwerkanschluss der HPS-Karte überwacht werden. Diese Überwachungsinstanz kann PTP-Knoten überwachen, die die Protokolle PTP mit TLV (proprietär für einen Meinberg Sync Node), PTP mit MGMT (definiert im IEEE 1588v2 Standard) und NTP mit Software-Zeitstempel unterstützen.

Das spezielle Protokoll „PTP mit TLV“ ist wie ein umgekehrtes PTP: Ein PTP-Delay-Request-Paket mit einem speziellen TLV wird an das PTP-System gesendet und dieses antwortet mit einem Synchronisationspaket und einem Delay-Response-Paket. Mit diesem Verfahren kann der Offset von der internen Referenz auf dem PTP-Gerät gemessen werden, auch wenn sich dieses PTP-System im Master-, Slave- oder Passiv-Modus befindet.

Statistic Types:



HPS-Karten im PTP- oder NTP-Modus unterstützen Paketstatistiken, die individuell überwacht werden können:

A: HPS im PTPv2 Betriebsmodus.
B: HPS im Überwachungsmodus.
C: HPS im NTP-Modus.

ESI: Diese Überwachungsinstanz kann PPS- und Frequenz-Knoten mit der ESI-Karte (Extension Signal Input) überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Verfügbare Optionen sind: PPS0, Freq In0, Freq In1, BITS In2.

MRS-CLK: Diese Überwachungsinstanz kann alle aktivierten MRS-Eingangssignale für jeden MRS-Referenztakt überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Verfügbare Optionen sind: GNSS/GPS, NTP, PTP, PPS, IRIG, 10MHz, E1, 2048kHz, je nach Hardware-Optionen (siehe Registerkarte „Uhr“ im Web-Interface).

PIO: Diese Überwachungsinstanz kann PPS- und Frequenz-Knoten mit der PIO-Karte (Programmable Input Output) überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Das hängt von der Konfiguration der PIO-Karte ab. Verfügbare Optionen sind: PPS0, PPS1, PPS2, PPS3, Freq In0, Freq In1, Freq In1, Freq In2, Freq In3.

FDM: Diese Überwachungsinstanz kann 50/60Hz Netzknoten mit der FDM-Karte (Frequency Deviation Monitor) überwachen. Aus einer Dropdown-Liste können Sie auswählen, welches Signal Sie überwachen möchten. Die verfügbaren Optionen sind: Zeitabweichung oder Frequenzabweichung.

Special Parameters: Diese Überwachungsinstanz kann verschiedene Parameter überwachen, wenn diese aktiviert sind:

Process Memory:
Hiermit kann die Speicherauslastung von System-Prozessen überwacht werden. Dazu muss der Name des Processes angegeben werden und die Werte werden in **%** dargestellt.

ID of selected HPS card:
Diese Option wird nur angeboten, wenn im System eine HPS-Karte als PTP-Slave aktiv ist. Wenn mehrere HPS-Karten im System als PTP-Slave vorhanden sind, dann wird die beste Karte über den internen PTP-BMCA (Best Master Clock Algorithm) ausgewählt und als MRS/PTP-Referenz benutzt. Mit diesem Parameter kann die ausgewählte ID der Karte überwacht werden.

ID of selected NTP server:
Diese Option wird nur angeboten, wenn im System externe NTP-Server konfiguriert wurden. Sind mehrere externe NTP Server konfiguriert, dann wird der beste externe NTP Server über ein spezielles NTP-Selektierungsverfahren ausgewählt und als MRS/NTP-Referenz benutzt. Mit diesem Parameter kann die ausgewählte ID der externen NTP Server überwacht werden.

Adresse (IP4/6 oder MAC):
IPv4/IPv6 oder MAC-Adresse eines Knotens, den Sie über das Netzwerk überwachen möchten. Hostnamen sind nicht erlaubt.

Alias:
Aliasname für einen Überwachungsknoten, um ihn in der gesamten Tabellenübersicht leicht zu finden. Der Aliasname, der vom Benutzer konfiguriert wird, definiert den Namen des Verzeichnisses auf der Flash-Disk („Base Path for logfiles for history of days“) jedes Knotens. Der Aliasname muss eindeutig sein und ein Wort ohne Leerzeichen mit einer maximalen Länge von 63 Zeichen (Leerzeichen werden automatisch in‘_‘ umgewandelt). Es ist möglich, den gleichen Knoten (z.B. die gleiche IP-Adresse) mit unterschiedlichen Aliasnamen zu überwachen - dies kann nützlich sein, wenn Sie den gleichen Knoten von verschiedenen Überwachungsmodulen aus überwachen möchten (z.B. verschiedene HPS100 IMS-Karten mit getrennten Netzwerkpfaden).

Location:
Geben Sie einen physischen Standort eines Überwachungsknotens ein, damit Sie diesen Knoten in der vollständigen Tabelle leicht erkennen können. Der Ortsname muss ein Wort ohne Leerzeichen mit einer maximalen Länge von 63 Zeichen sein (Leerzeichen werden automatisch in ‘_‘ umgewandelt).

Group Index:
Sie können überwachte Knoten innerhalb einer logischen Gruppe anordnen, indem Sie ihnen den gleichen Index zuweisen (z.B. können Knoten mit dem gleichen Gruppenindex von gleicher Art (NTP, PTP, PPS) oder am gleichen Ort usw. sein). Knoten mit dem gleichen Gruppenindex werden automatisch in der Tabelle sortiert. Die Tabelle kann im Flat- oder Gruppenmodus angezeigt werden. Im Flat-Modus werden nur Knoten in einer Zeile angezeigt. Zur Strukturierung der Tabelle kann der Gruppenmodus durch Drücken der Schaltfläche **„Grp“** über der ersten Spalte ausgewählt werden - dann werden alle Knoten mit der gleichen Gruppennummer zu einer Zeile zusammengefasst und können separat geöffnet werden.

Request Interval (s):
Intervall in Sekunden, in dem ein Überwachungsknoten Anfragen an die Slaves/Clients sendet. Das minimale Anfrageintervall beträgt 1s, das maximale 3600s. Ein Standardintervall ist 64s. Wenn das Anfrageintervall deaktiviert ist (0), werden keine Anfragen an die Knoten gesendet und keine Daten protokolliert.

Logging Interval (s):
Intervall in Sekunden, in dem der gemessene Offset und Stratum in eine Protokolldatei geschrieben werden. Wenn das Log-Intervall deaktiviert ist, werden keine Daten in der Logdatei gespeichert. Wenn das Anfrageintervall aktiviert und das Protokollintervall deaktiviert wurde, werden die Knoten überwacht und Grenzwerte und Benachrichtigungen überprüft, aber keine Daten gespeichert. Wenn das Anfrageintervall kleiner als das Aufzeichnungsintervall ist, wird der Mittelwert der gemessenen Offsets im Anfrageintervall protokolliert und der Minimal- und Maximalwert im Protokollintervall zusätzlich festgehalten.

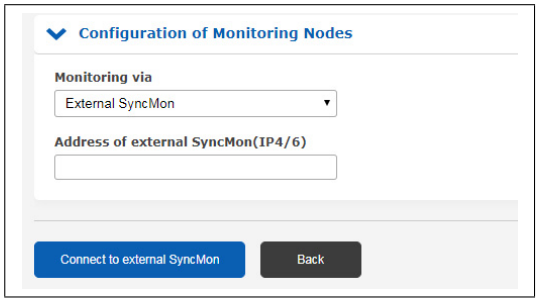
Fix Offset [s]:
Bei einigen Netzwerkknoten ist ein bestimmter Offset bekannt (z.B. Netzwerk-Asymmetrie). Dieser Wert dient als Korrekturwert und kann hier eingetragen werden. Der „Fix Offset“ wird beim gemessenen Wert (Measured Value) immer aufgerechnet. Ein eingetragener fester Offset wird in der Übersicht mit einem * in der Spalte „Measured Value“ angezeigt.

Disable Monitoring:
Die Überwachung kann für jeden Knoten deaktiviert werden. Wenn der Knoten deaktiviert wurde, werden keine Überwachungsdaten an den Knoten gesendet und keine Daten gespeichert.

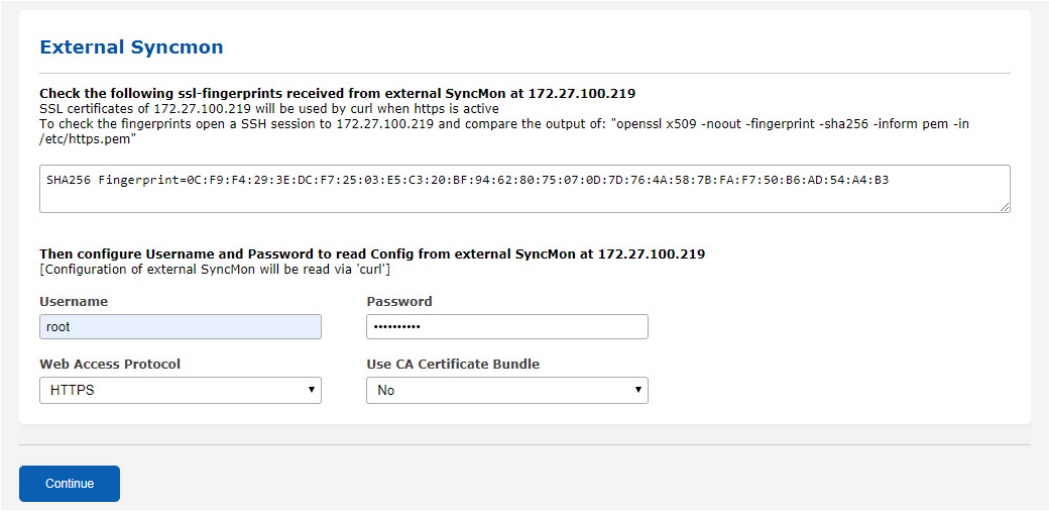
Disable Logging on external Server:
Die gemessenen oder protokollierten Daten können über das SYSLOG- oder RSYNC-Protokoll an einen externen Server gesendet werden. Dies kann für jeden Knoten deaktiviert werden (siehe Systemeinstellungen für externe Serverkonfiguration).

10.1.8.4 External SyncMon

„External SyncMon“ ist eine spezielle Überwachungsinstanz, die Knoten und Sensoren anderer LANTIME-Geräte mit aktiviertem SyncMon überwachen kann. Bei der Auswahl des externen SyncMon mit IP-Adresse wird eine Liste der verfügbaren Knoten von diesem externen SyncMon heruntergeladen. Konfiguration und Daten werden über den WEB-Service (Curl) übertragen.



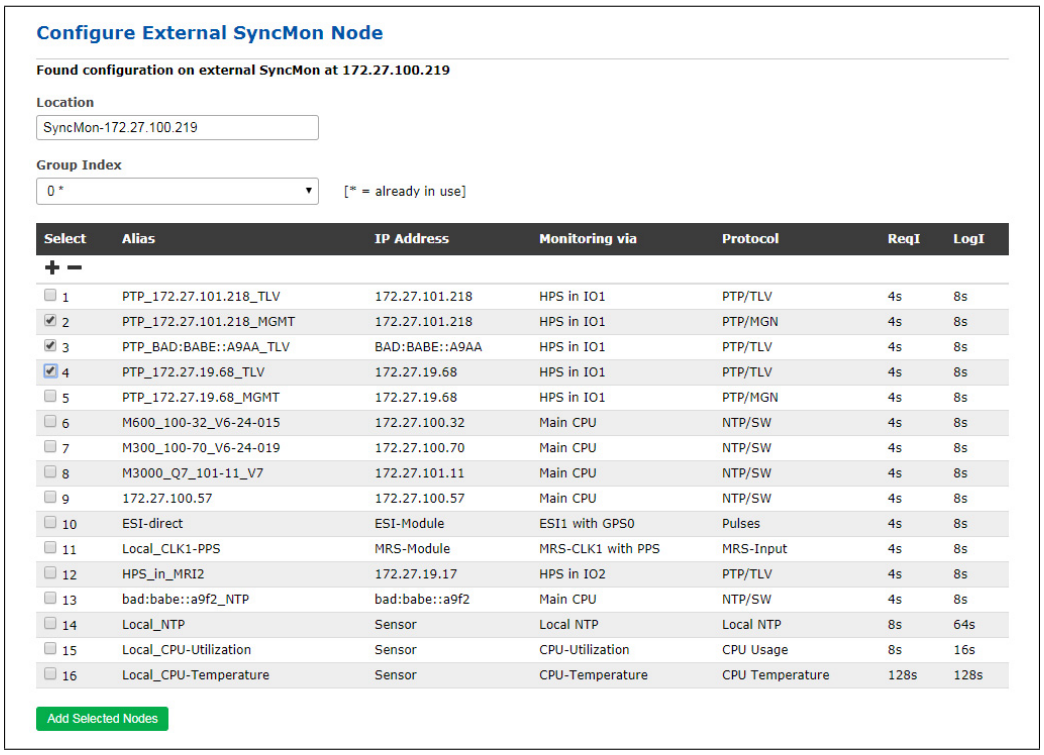
Drücken Sie **„Mit externem SyncMon verbinden“**, dadurch versucht das System sich mit dem externen SyncMon zu verbinden und den SSL-Fingerabdruck dieses Servers anzuzeigen. Überprüfen Sie die folgenden, vom externem SyncMon empfangenen SSL-Fingerabdrücke. Die SSL-Zertifikate werden von curl verwendet wenn https aktiv ist. Um die Fingerabdrücke zu überprüfen, öffnen Sie eine SSH-Sitzung auf dem externen SyncMon und vergleichen Sie die Ausgabe von: „openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem“. Auf diese Weise wird sichergestellt, dass es sich um das richtige Gerät handelt.



Geben Sie dann den Benutzername und das Passwort ein, um die Konfiguration vom externem SyncMon zu lesen - die aktuelle Konfiguration des externen SyncMon wird über *‘curl‘*ausgelesen. Außerdem müssen Sie das WEB-Zugriffsprotokoll (HTTP oder HTTPS) konfigurieren und wenn Sie ein CA-Zertifikatspaket verwenden möchten, um Konfigurations- und Messdaten vom externen SyncMon zu erhalten.

Beachten Sie, dass bei der Verwendung von HTTPS alle Daten verschlüsselt und entschlüsselt werden müssen, was eine Menge CPU-Auslastung für jede Datenanforderung an das externe SyncMon verursacht.

Beachten Sie, wenn Sie das HTTP-Zugriffsprotokoll verwenden möchten, dann müssen Sie den HTTP-Netzwerkdienst auf dem internen und externen LANTIME aktivieren. Das Gleiche gilt für das HTTPS-Protokoll.



Configure External SyncMon Node

Found configuration on external SyncMon at 172.27.100.219

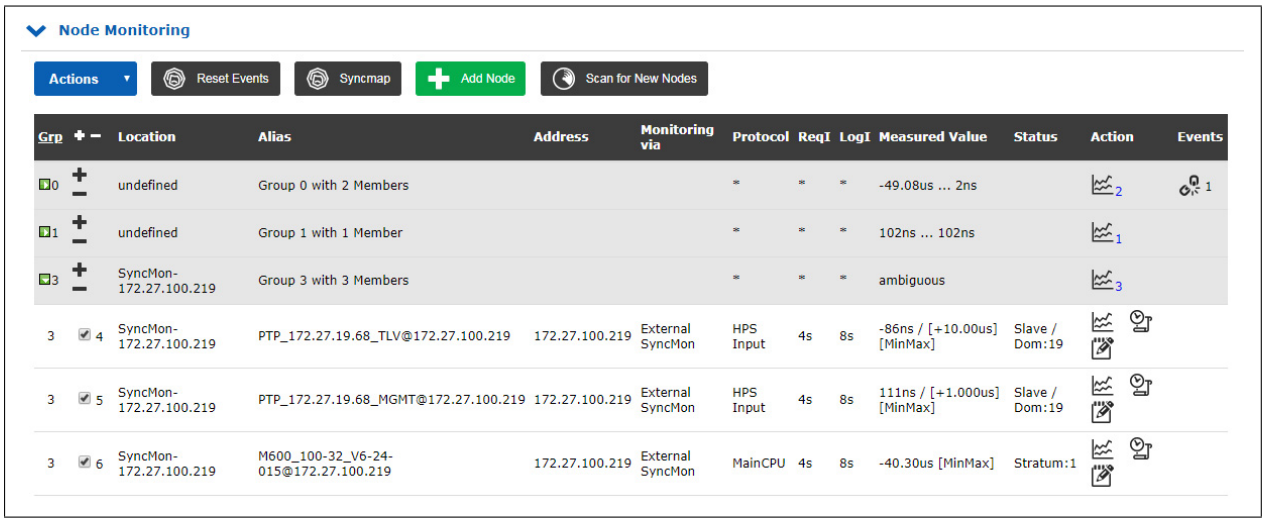
Location: SyncMon-172.27.100.219

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

Um die aktuelle Konfiguration aus dem externen SyncMon zu erhalten, müssen Sie die Knoten auswählen, die Sie von diesem LANTIME überwachen möchten. Es werden nur Knoten angeboten, die nicht deaktiviert und für die externe Protokollierung erlaubt sind. Die Parameter für Anfrage- und Protokollintervall werden von der externen Konfiguration übernommen. Der Standort und der Gruppenindex können für alle ausgewählten Knoten konfiguriert werden. Der Standardort ist „SyncMon-“ plus die IP-Adresse. Die Alias-Namen für die externen SyncMon-Knoten sind der ursprüngliche Alias-Name plus „@IP-Adresse“. Es wird empfohlen, für alle Knoten eines externen SyncMon eine nicht verwendete Gruppen-ID zu verwenden.

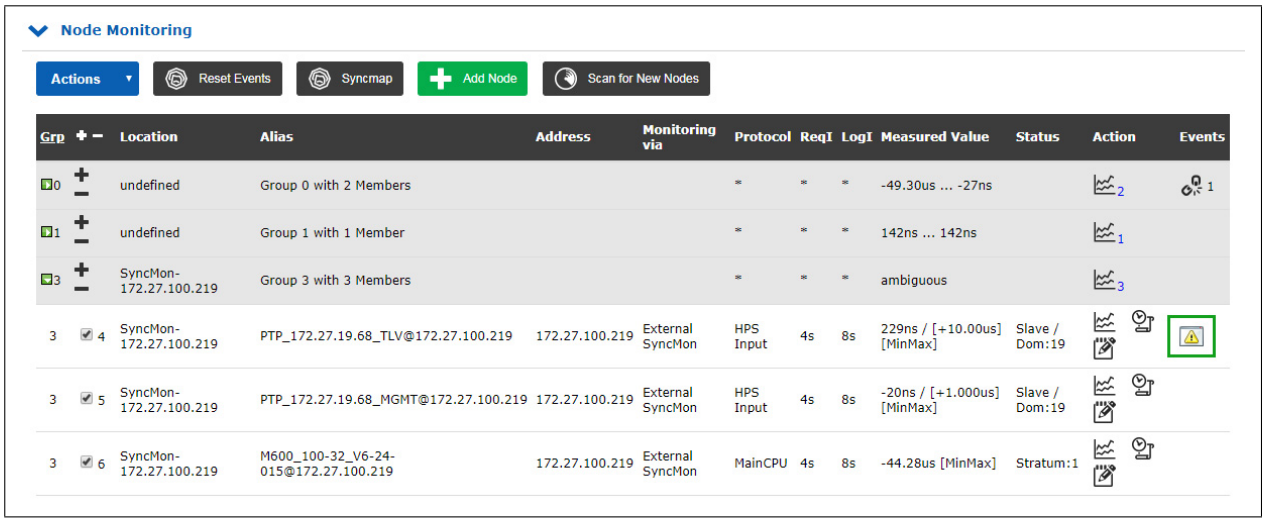


Node Monitoring

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		

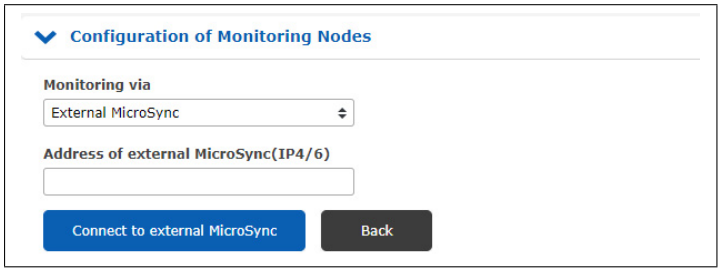
Wenn Änderungen an den Knoten der externen SyncMon-Konfiguration vorgenommen werden, die überwacht werden sollen, wird in der Haupttabelle in der Spalte **Events** für diesen Knoten ein Warnzeichen angezeigt. Dann müssen Sie die Parameter für diesen Knoten manuell ändern.



10.1.8.5 External MicroSync

External MicroSync ist eine spezielle Überwachungsinstanz, die MRS-Referenzen von externen MicroSync-Geräten überwachen kann. Bei der Auswahl des externen MicroSync mit IP-Adresse wird eine Liste der verfügbaren MRS-Referenzen von diesem externen MicroSync heruntergeladen.

Konfiguration und Daten werden über den WEB-Service (Curl) übertragen.

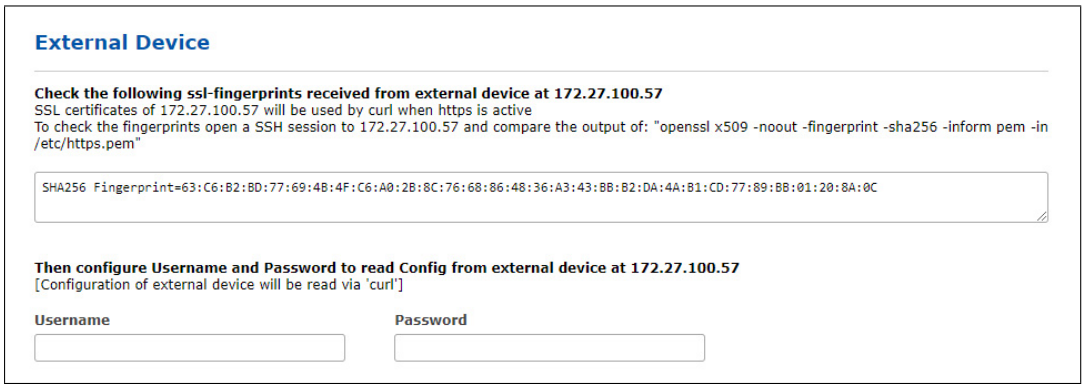


Drücken Sie „Connect to external MicroSync“, dadurch versucht das System sich mit dem externen MicroSync zu verbinden und den SSL-Fingerabdruck dieses Servers anzuzeigen. Überprüfen Sie die folgenden, vom externem SyncMon empfangenen SSL-Fingerabdrücke. Die SSL-Zertifikate werden von curl verwendet. Um die Fingerabdrücke zu überprüfen, öffnen Sie eine SSH-Sitzung auf dem externen MicroSync und vergleichen Sie die Ausgabe von:

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in /etc/https.pem
```

Auf diese Weise wird sichergestellt, dass es sich um das richtige Gerät handelt.

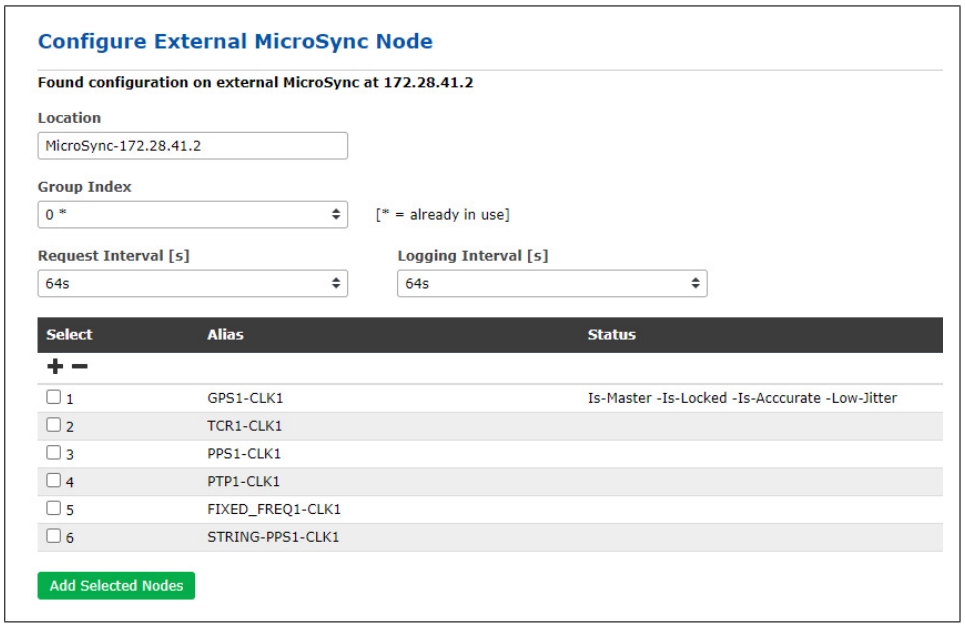
Geben Sie dann Benutzername und Passwort von dem MicroSync-System ein, um die Konfiguration vom externem MicroSync zu lesen - die aktuelle Konfiguration des externen MicroSync wird über ‘curl‘ ausgelesen. Beachten Sie, dass bei der Verwendung von HTTPS alle Daten verschlüsselt und entschlüsselt werden müssen, was eine Menge CPU-Auslastung für jede Datenanforderung an das externe MicroSync-System verursacht.



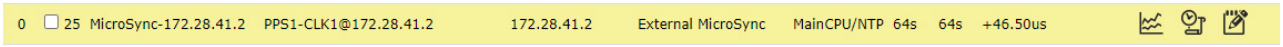
Um die aktuelle Konfiguration aus dem externen MicroSync zu erhalten, müssen Sie die MRS-Referenzen auswählen, die Sie von diesem LANTIME überwachen möchten. Die Parameter für Anfrage- und Protokollintervall werden für alle gleich eingestellt.

Der Standort und der Gruppenindex können für alle ausgewählten MRS-Referenzen konfiguriert werden. Der Standardort ist *MicroSync-** plus die IP-Adresse per Default.

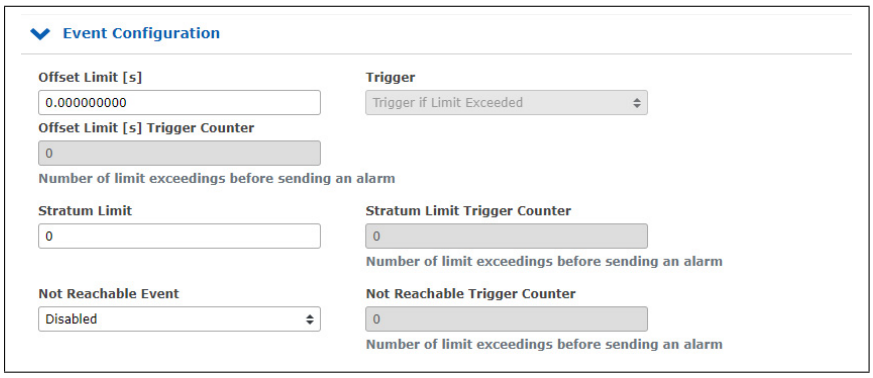
Die Alias-Namen für die externen MicroSync-MRS-Referenzen sind der ursprüngliche Alias-Name plus *@IP-Adresse*. Es wird empfohlen, für alle MRS-Referenzen eines externen MicroSync eine nicht verwendete Gruppen-ID zu verwenden.



Wenn Änderungen an den Knoten der externen MicroSync-Konfiguration vorgenommen werden, die überwacht werden sollen, wird in der Haupttabelle in der Spalte Events für diesen Knoten ein Warnzeichen angezeigt. Dann müssen Sie die Parameter für diesen Knoten manuell ändern.



10.1.8.6 Ereignis-Konfiguration:

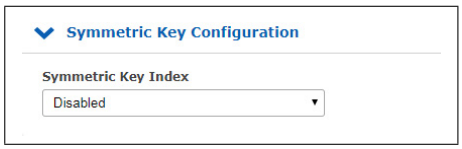


Offset Limit (s):
Offset-Schwellenwert in Sekunden. Der gemessene Offset zwischen einem Knoten und der Referenz wird mit dem konfigurierten Schwellenwert verglichen. Wenn die berechnete Differenz größer als die konfigurierte Offsetgrenze ist, erzeugt der LANTIME einen Alarm „Sync Monitor“ (der als Benachrichtigungs-E-Mail, SNMP-Trap oder an einen externen Syslog-Server gesendet werden kann). Mit der Option „Trigger“ kann die Richtung „Trigger bei Limitüberschreitung“ oder „Trigger bei Limitunterschreitung“ gewählt werden. Mit der Option „Offset Limit[s] Trigger Counter“ wird das Event einmalig ausgelöst, nachdem die Anzahl der Limitüberschreitungen in einer Reihe überschritten wurde.

Stratum Limit:
Schwellenwert für einen NTP-Stratumlevel. Wenn der Stratum-Level eines überwachten Clients höher als das konfigurierte Stratum-Limit ist, wird ein Alarm ausgelöst (per eMail, SNMP-Trap oder an einen externen Syslog-Server gesendet). Mit der Option „Stratum Limit Trigger Counter“ wird das Event einmalig ausgelöst, nachdem die Anzahl der Limitüberschreitungen in einer Reihe überschritten wurde.

Not Reachable Event:
Wenn der konfigurierte Knoten für die Überwachung nicht erreichbar ist, erzeugt der LANTIME einen Alarm „Sync Monitor“ (der als Benachrichtigungs-E-Mail, SNMP-Trap oder an einen externen Syslog-Server gesendet werden kann). Mit dieser Option kann das aktiviert oder deaktiviert werden. Mit der Option „Not Reachable Limit Trigger Counter“ wird das Event einmalig ausgelöst, nachdem die Anzahl der nicht erreichbaren Knoten in einer Reihe überschritten wurde.

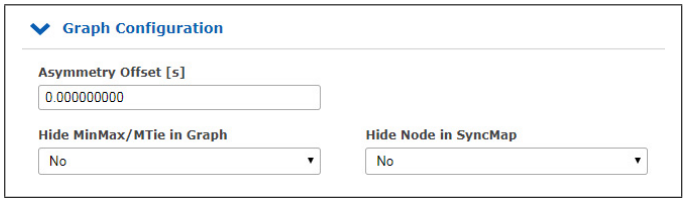
10.1.8.7 Symmetrische Schlüsselkonfiguration



Symmetric Key Index:
Wenn Sie die symmetrische Schlüsselauthentifizierung für SyncMon verwenden möchten, wählen Sie einen Schlüsselindex aus der Liste der bereits verwendeten Schlüssel. Wenn die Schlüssel noch nicht definiert sind, fahren Sie mit dem NTP-Dialog im „Webinterface → NTP → Symmetrische Schlüssel“ fort und erzeugen Sie eine neue Schlüsseldatei, die auf dem überwachten Knoten gespeichert und aktiviert werden muss. Für weitere Informationen zur Symmetrischen Schlüsselerzeugung gehen Sie bitte zur LTOS7-Konfiguration „Webinterface → NTP → NTP Symmetrische Schlüssel“.

10.1.8.8 Grafische Parameter bearbeiten

Asymmetrie-Offset für Grafik:
Wenn eine konstante Asymmetrie der gemessenen Knoten bekannt ist, können Sie diesen Wert für die grafische Ausgabe einstellen - die protokollierten Werte werden nicht geändert - der Asymmetrie-Offset ist wie ein fester Offset nur für die grafische Überwachung.



Ausblenden von Min/Max/MTie-gefüllten Kurven in der Grafik:
Wenn das Anfrage-Intervall kleiner als das Protokoll-Intervall ist, werden zusätzliche Werte für Min und Max in den Protokolldateien gespeichert. Diese Min/Max-Werte werden als gefüllte Kurve in einer grauen Farbe hinter der aufgezeichneten Offset-Kurve angezeigt. Diese Funktion kann deaktiviert werden.

Diesen Knoten in SyncMap ausblenden:
Sie können einen bestimmten Knoten in der SyncMap deaktivieren.

Wenn Sie mit der Konfiguration eines neuen überwachten Knotens fertig sind, speichern Sie die aktuelle Konfiguration indem Sie auf die Schaltfläche „Save Memeber“ klicken. Durch Anklicken der Schaltfläche „Remove Member“ entfernen Sie den aktuell ausgewählten Knoten aus der vollständigen Liste aller überwachten Knoten. Alle erfassten Daten für den jeweiligen Knoten gehen verloren, wenn Sie die gespeicherten Daten nicht vor dem Entfernen gesichert haben.

Durch Anklicken der Schaltfläche **„Remove Existing Data“** werden alle Daten für nur diesen speziellen Knoten gelöscht.

10.1.8.9 Nach neuen Knoten suchen

Scan for new Nodes ist eine automatische Suche nach NTP- und PTP-Knoten in Ihrem Netzwerk. Die Suche nach PTP-Knoten wird von der HPS-Karte nur unterstützt, wenn die Lizenz und Überwachung für mindestens 1024 Clients aktiviert ist.

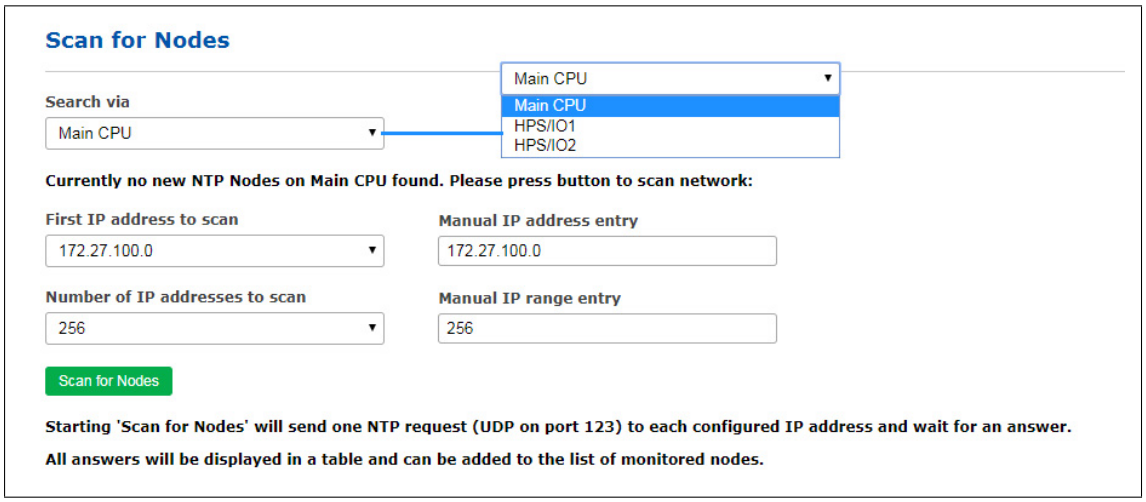


Abbildung: Dialogfeld „Nach neuen Knoten suchen". In dieser temporären Tabelle werden nur neu gefundene Knoten angezeigt. Markieren Sie die Knoten, die Sie in der Tabelle aller überwachten Knoten hinzufügen möchten.

Suchen mit:
Wählen Sie zunächst eine Instanz aus der Dropdown-Liste aus, die Sie für die Suche nach neuen Knoten verwenden können. Mögliche Optionen sind „Main CPU" und „HPS"-Karte. Mit der Main-CPU können Sie nur nach NTP-Knoten suchen. Die Suche nach PTP-Knoten wird von der HPS-Karte nur unterstützt, wenn die Lizenz und Überwachung für 1024 Clients aktiviert ist.

Erste zu scannende IP-Adresse:
Legen Sie die Anfangs-IP-Adresse fest, unter der die Suche mit dem automatischen NTP-Scan beginnen soll. In der Dropdown-Liste finden Sie alle Teilnetzbereiche der einzelnen Netzwerkschnittstellen. Mit „Manuelle IP Adresseingabe" kann ein anderer Startpunkt definiert werden.

Anzahl der zu scannenden IP-Adressen:
Dieser Parameter legt eine Anzahl von IP-Adressen fest, die gescannt werden. An jede IP-Adresse aus dem IP-Bereich wird eine separate NTP-Paketanforderung gesendet. Wenn ein NTP-Client auf diese Anfrage antwortet und seine IP-Adresse noch nicht konfiguriert ist, erscheint dieser Knoten in der Tabelle. Mit „Manuelle IP-Bereichseingabe" kann eine andere Größe des Bereichs definiert werden.

Scannen nach NTP-Knoten über die Main-CPU:
Beim Start von **„Scan for Nodes"** wird eine NTP-Anfrage (UDP auf Port 123) an jede konfigurierte IP-Adresse (IP-Adressbereich) gesendet und auf eine Antwort gewartet.

Alle Antworten werden in einer Tabelle angezeigt und können der Liste der überwachten Knoten hinzugefügt werden. Mit Auswahlfeldern können neue Knoten automatisch in die Liste der überwachten Knoten aufgenommen werden. Die Parameter für Standort, Gruppenindex, Anfrageintervall, Aufzeichnungsintervall, Offsetgrenze und Stratum-Limit können im nächsten Schritt definiert werden, bevor sie in die Tabelle mit den anderen überwachten Knoten aufgenommen werden.

Suche über HPS:
Wird eine HPS-Karte im Überwachungsmodus ausgewählt (unterstützt von der HPS-Karte nur bei aktivierter 1024- oder 2048-Clients-Lizenz und Überwachung), muss die „PTP-Domain" eingerichtet werden.

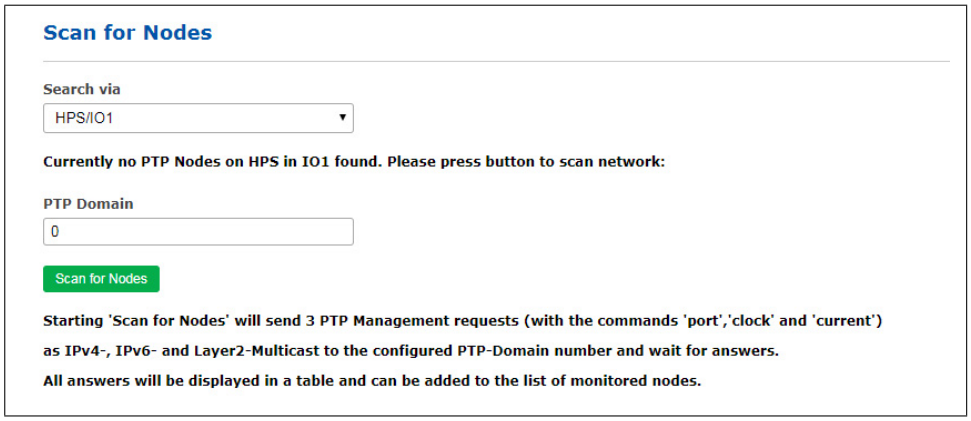


Abbildung: Um das Netzwerk nach PTP-Knoten zu durchsuchen, muss zunächst in der Dropdown-Liste „Search for Nodes“ eine HPS-Karte mit aktiviertem Monitoring ausgewählt werden.

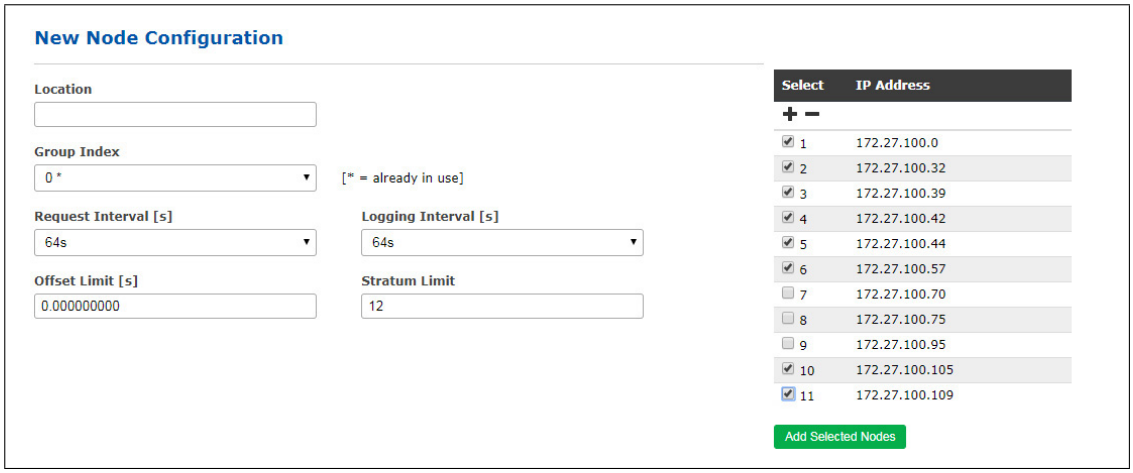
PTP-Domain:
Das mit dieser HPS-Karte verbundene Netzwerk wird in der Domäne gescannt die hier vom Benutzer definiert wurde. Die folgenden Mappings gemäß IEEE 1588-2008 werden gescannt:

- UDP/IPv4/Ethernet,
- UDP/IPv6/Ethernet,
- Ethernet (IEEE 802.3, layer 2).

Beim ersten Start des Scans wird eine PTP-Management-Nachricht im Broadcast-Modus gesendet, um den „Port-Status“ jedes PTP-Knotens zu erhalten - dies geschieht bei IPv4, IPv6 und Layer2.

Alle PTP-Knoten, die auf diese Anfrage antworten, fragen nach dem „aktuellen Status“ und dem „Uhrenstatus“ mit Managementmeldungen die nachfolgend beschrieben werden. Das Ergebnis wird als Liste aller verfügbaren PTP-Knoten angezeigt. Jeder neue PTP-Knoten wird in eine Übersichtstabelle der verfügbaren Knoten eingetragen.

In der Tabelle werden nur neue Knoten angezeigt, die noch nicht konfiguriert wurden. Für jeden Knoten werden die PTP-UUID, MAC-Adresse, IP-Adresse, Herstellername, Feature (wenn ein Knoten PTP mit erweitertem TLV nur zur Überwachung oder PTP-Verwaltung unterstützt), Domänennummer, Status (der aktuelle PTP-Status wie Slave, Master, Listening.....), Offset und Delay (aktuelle Messwerte aus der PTP-Verwaltung) automatisch in der Tabelle angezeigt. Mit Auswahlfeldern können neue Knoten automatisch in die Liste der überwachten Knoten aufgenommen werden. Die Parameter für Standort, Gruppenindex, Anfrageintervall, Aufzeichnungsintervall, Offsetgrenze und Stratum-Limit können im nächsten Schritt definiert werden, bevor die ausgewählten Knoten hinzugefügt werden.



Die Überwachungs-Engine beginnt damit PTP/NTP-Requests in den konfigurierten Intervallen an jeden Knoten aus der Liste zu senden und misst die in den Antworten empfangene Zeit mit ihrer eigenen Zeit (die z.B. auf UTC, GNSS-Synchronisation zurückzuführen ist). Die aktuellen Offset- und Statusinformationen können in der Statusübersichtstabelle im Menü „Node Monitoring“ eingesehen werden.

In der Statusübersichtstabelle der überwachten Knoten finden Sie neben den Statusinformationen 3 Aktionsschaltflächen: Grafik, Fehlerprotokolle und Bearbeitung.

Durch Auswahl der Schaltfläche Grafik wird ein grafisches Diagramm für den ausgewählten Knoten angezeigt. Auf dieser Seite finden Sie verschiedene Funktionen für verschiedene Darstellungsoptionen.

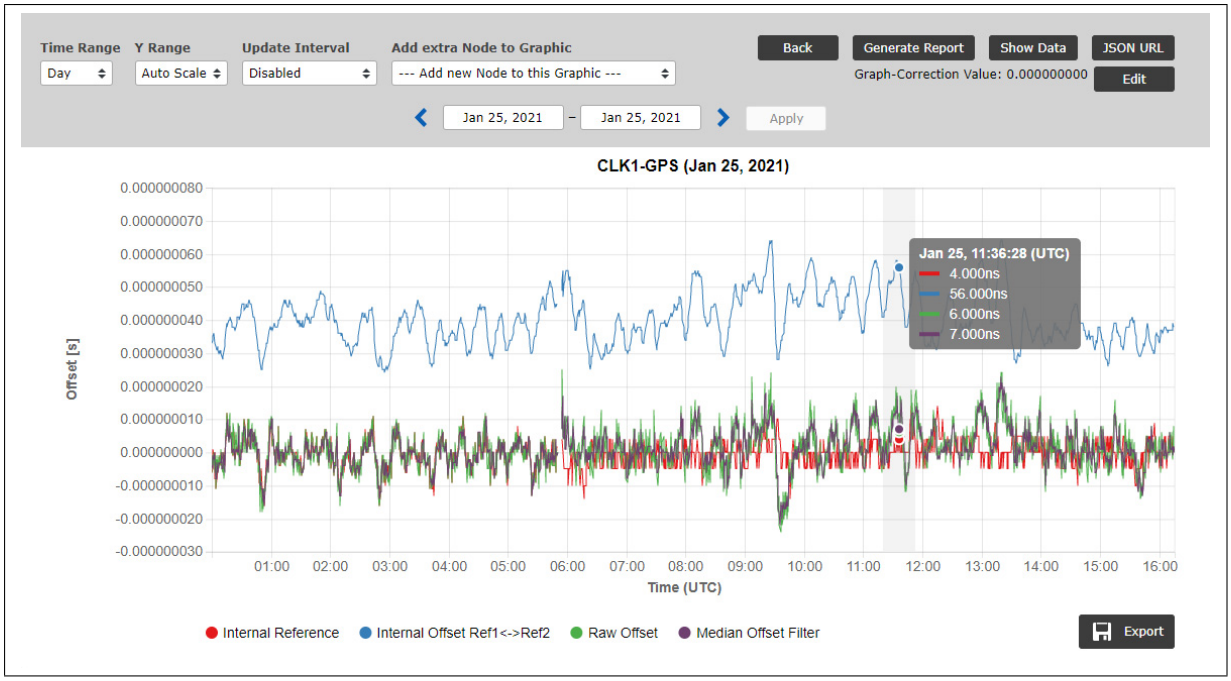
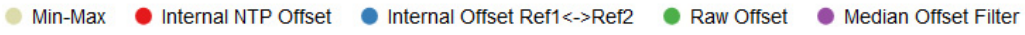


Abbildung: Grafische Darstellung der Offsetwerte für jeden Knoten, wählbar für verschiedene Zeitbereiche (Tag, Woche, Monat oder manuelle Auswahl). Mit vorgegebenen Schaltflächen im „Zeitbereich auswählen“ können Sie für die grafische Darstellung entweder vergangene oder zukünftige Intervalle auswählen.

Offsets werden für jeden NTP/PTP oder anderen überwachten Knoten gesammelt und können als grafische Darstellung für wählbare Zeitintervalle in der Weboberfläche des SyncMon-Knotens dargestellt werden.

Die überwachten Daten werden kontinuierlich auf dem Sync-Knoten „Basispfad für Logdateien des aktuellen Tages“ gespeichert und automatisch auf der Flash-Karte („Basispfad für Logdateien des Tagesverlaufs“) bei Tageswechsel um 0:00 UTC gespeichert. Für die weitere statistische Verarbeitung stehen die Daten jederzeit zur Verfügung.

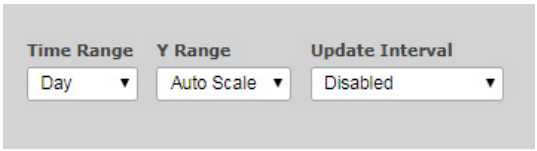
Am unteren Rand des Diagramms zeigt eine Übersicht, welche Farbe welche Daten darstellt. In diesem Fall stellt die rote Linie den internen NTP-Offset dar, der die Referenz für den überwachten NTP-Knoten ist. Die grüne Linie ist der Versatz zwischen einer Referenzzeit des Sync-Knotens und der gemessenen Zeit eines überwachten Systems.



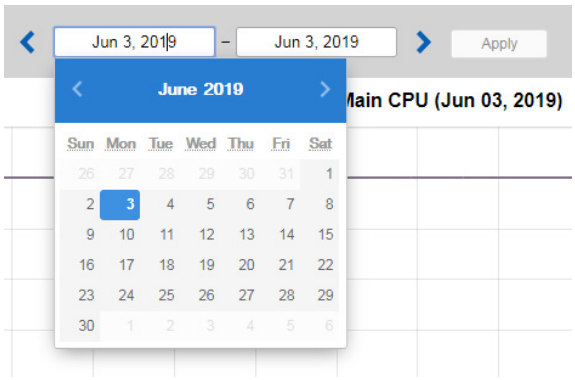
Wenn Sie den Cursor auf ein Element in der unteren Zeile positionieren, wird nur dieses Diagramm angezeigt und alle anderen Diagramme werden ausgeblendet. Wenn Sie auf ein Element in der unteren Zeile klicken, wird dieses Diagramm dauerhaft ausgeblendet.

Bei PTP- und PPS-Signalen ist die Sync-Node-Referenz eine interne Referenzzeit vom Empfänger, z.B. Multi-GNSS (GPS, GLONASS, Galileo, Beidou), externer UTC-Zeitdienst, IRIG TC, Langwellenzeitreferenz (PZF, MSF, WWVB....). Die Referenz des Sync-Knotens wird als rote Linie dargestellt und wenn eine zweite Referenz vorhanden ist, dann stellt die blaue Linie den Versatz zwischen den beiden Referenzuhren dar. Für Multi-GNSS-Referenzuhren im Normalbetrieb sehen Sie etwas im unteren Nanosekundenbereich mit 5ns Auflösung.

Für NTP-überwachte Signale wird der Sync-Knoten mit dem internen NTP synchronisiert, der durch eine interne Referenzuhr (Multi-GNSS oder IRIG-Timecode, Langwelle....) synchronisiert wird. In diesem Fall stellt die rote Linie im Diagramm die interne NTP-Systemzeit dar.



Zeitbereich:
Es gibt verschiedene Zeitbereiche zur Auswahl - Tag, Woche, Monat und Benutzerdefiniert. Bei der Auswahl des benutzerdefinierten Zeitbereichs klicken Sie auf **„Apply“**, um die Grafik mit dem ausgewählten Zeitbereich anzuzeigen. Für andere Optionen ist es auch möglich, zurück zu gehen, um Daten aus der Vergangenheit zu sehen.



Y-Bereich:
Verschiedene Optionen sind verfügbar: automatische Skalierung oder feste Y-Bereiche in Dekadenintervallen: 100ns,1us, 10us, 100us, 1ms, 10ms und 100ms.

Aktualisierungsintervall:
Die automatische Aktualisierung der aktuellen Grafik kann von 1s bis 1 Stunde aktiviert werden.

Für NTP-Knoten ist es möglich, ein Diagramm entweder als Rohdaten oder mit angewandtem Medianfilter oder ein Diagramm nur der internen Referenz (rote Linie) anzuzeigen.

Für PTP-Knoten sind die ausgewählten Grafikmodi:
Gemeldeter Offset von einem PTP-Knoten (Daten, die von einem PTP-Knoten durch ein Standard-MGMT-Protokoll erhalten wurden).

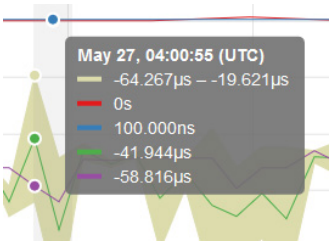
Gemessener Offset zu einem PTP-Knoten
(Offset eines PTP-Slaves gemessen gegen die interne Referenz). Die Messungen sind nur für PTP-Knoten verfügbar, die die Überwachung des PTP-Protokolls mit TLVs unterstützen. Der überwachte Knoten kann sich im Slave-, Master- oder Passivmodus befinden. Neben den durch Reverse-PTP erhaltenen Messwerten stehen auch die gemeldete Wertekurve und die MTIE-gefüllte Kurve zur Verfügung, wenn die MIN- und MAX-Wertmessung auf dem überwachten Knoten unterstützt wird.

Für PPS-Knoten, die über eine ESI- oder PIO-Eingangskarte am Sync-Knoten überwacht werden, stehen Ihnen folgende Grafikmodi zur Verfügung: „Rohdaten“, „Daten mit angewandtem Medianfilter“ und „Nur interne Referenz“ (ein PPS von einer internen Referenzuhr).

Wenn das Anforderungsintervall kleiner als das Protokollintervall ist, werden zusätzliche Min-Max-Werte für dieses Protokollintervall in den Datendateien gespeichert. Diese Min-Max-Werte werden automatisch als gefüllte Kurve im grafischen Diagramm hinzugefügt und der Mittelwert wird als rote Linie in der gefüllten Min/Max-Kurve angezeigt.

X/Y-Bereich vergrößern:
Um den Y-Bereich ein- und auszuzoomen, positionieren Sie den Mauszeiger auf der Y-Achse und scrollen Sie mit dem Mausrad, um ein- und auszuzoomen. Durch einmaliges Drücken der Maustaste auf der Y-Achse wird diese auf den ausgewählten Y-Bereich zurückgesetzt. Beim Drücken der Maustaste und Bewegen der Maus nach oben und unten wird die Y-Achse auf und ab bewegt.

Um den X-Bereich (Zeitachse) ein- und auszuzoomen, positionieren Sie den Mauszeiger im Diagramm und scrollen Sie mit dem Mausrad, um ein- und auszuzoomen. Wenn Sie die Maustaste drücken und die Maus nach links und rechts bewegen, wird die Grafik nach links und rechts verschoben. Wenn Sie mit der Maus über das Diagramm fahren, zeigt eine Info-Ansicht alle Werte aller Diagramme an.



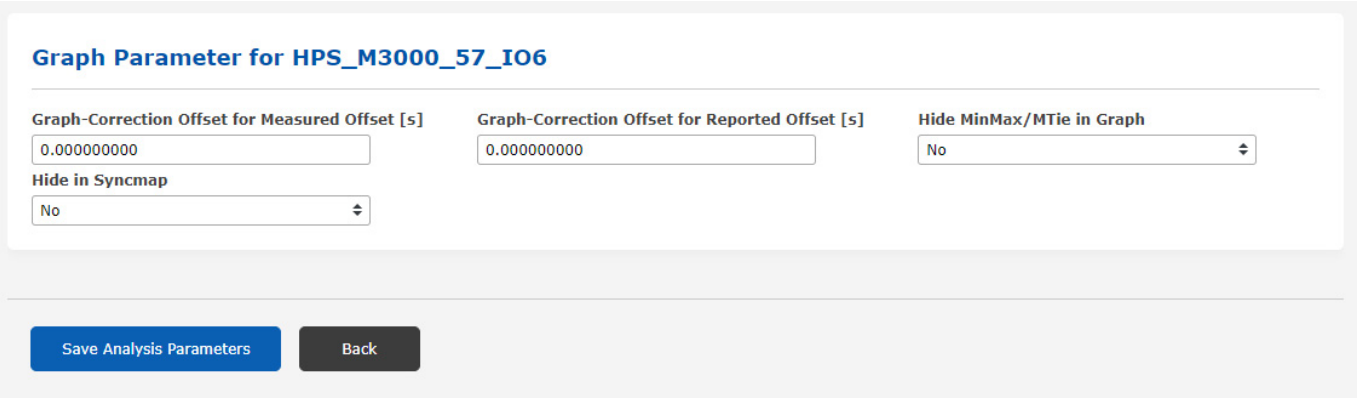
Daten anzeigen:
Mit dem Button **„Daten anzeigen“** können Sie von der grafischen Darstellung in eine Tabellenansicht der aktuell angezeigten Werte wechseln. Die erste Zeile zeigt die Beschreibung jeder Spalte. Mit der Schaltfläche **„Graph anzeigen“** können Sie zur grafischen Ansicht zurückkehren. Wenn Sie heranzoomen, werden nur Daten des gezoomten Zeitbereichs angezeigt.

#	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

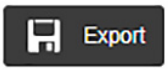
JSON URL:
Mit der Schaltfläche „JSON URL“ erhalten Sie die WEB-Adresse, um den letzten Messwert des ausgewählten Knotens zu erhalten. Damit können die aktuellen Werte über WEB-Zugriff (wget oder curl) aus einem externen Programm gelesen werden. Das JSON-Format ist wie folgt:

```
{
   "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
  }
 }
}
```

Bearbeiten-Button:
Mit der Schaltfläche **„Edit“** können alle grafischen Parameter angezeigt und konfiguriert werden. Der „Graph-Correction Value“ kann verwendet werden, um die Grafik mit einem festen Offset anzupassen (um z.B. eine bekannte Asymmetrie in einem Netzwerk oder die Laufzeit einer Kabellänge zu kompensieren). Im Gegensatz zum „Fix Offset“ wird der „Graph-Correction Value“ nur auf die aktuelle Grafik angewand und nicht auf die gespeicherten Daten.



Export-Schaltfläche:
Mit dem Button **„Export“** wird eine PNG-Datei des aktuellen Graphen erzeugt. Diese Ansicht kann zum Drucken und Speichern verwendet werden.



Schaltfläche Bericht erzeugen:
Mit dieser Auswahl werden die aktuellen Daten des überwachten Knotens in Form eines Berichts aufbereitet. Sie können auch einen Zeitrahmen für erfasste Daten auswählen, aus dem ein Bericht erzeugt wird. Der Bericht enthält die aktuellen Statusdaten, die Monitorkonfiguration, die Überwachung der statistischen Werte über den ausgewählten Zeitraum, ein grafisches Diagramm und optional eine vollständige Sync-Map für den überwachten Knoten.

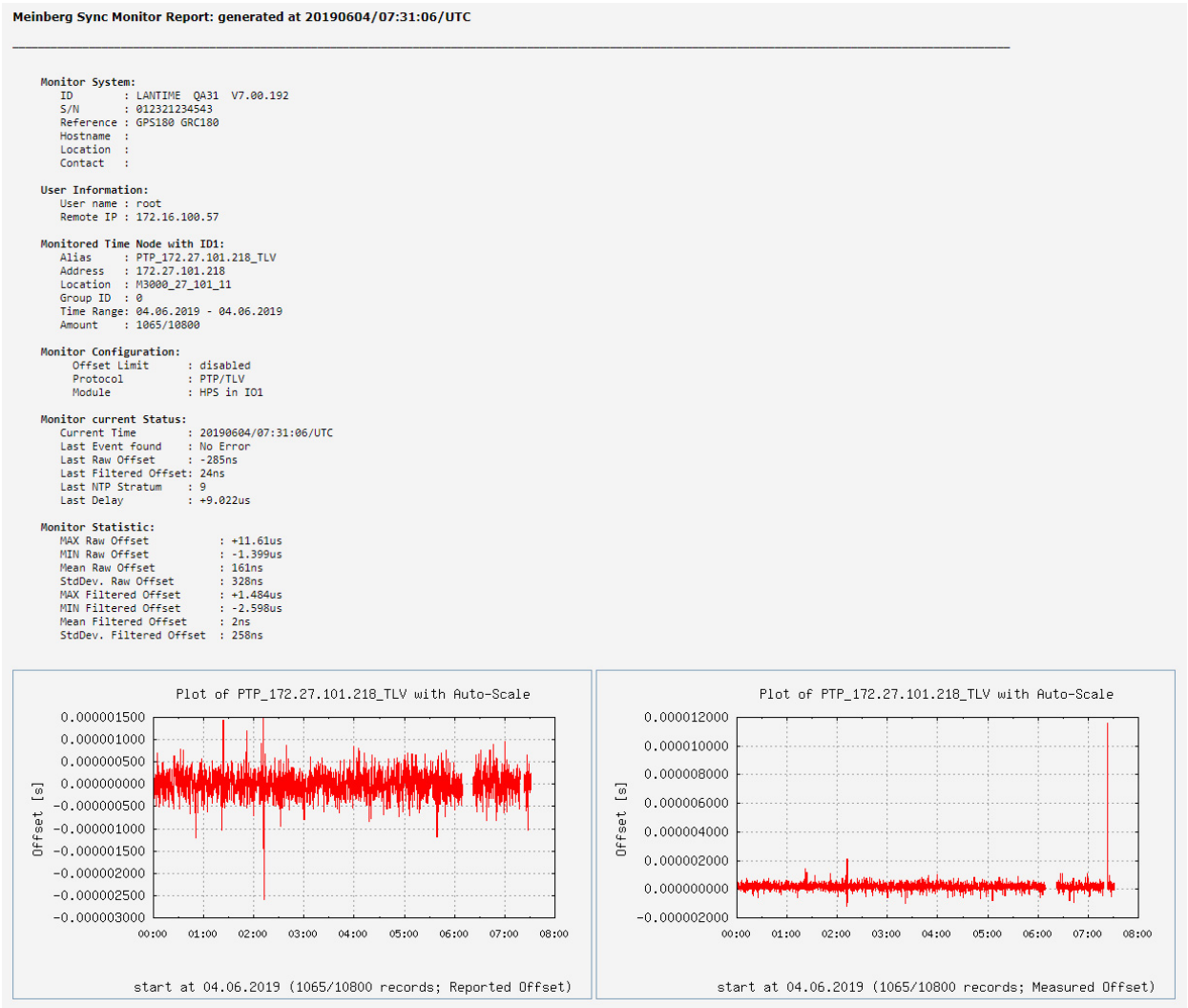


Abbildung: Generierter Bericht für einen ausgewählten Knoten. Der Bericht enthält Statusinformationen über die ausgewählten überwachten Knoten, die Monitorkonfiguration, die Hauptmonitorstatistiken und grafische Diagramme.

Schaltfläche „Back“ in der Graph-Ansicht:
bei der Auswahl der Grafikseite führt die Schaltfläche „Back“ zurück zur Haupttabellenansicht und zeigt die Tabelle mit allen konfigurierten Knoten an. Im Falle von Sensoren wird die Tabelle der Sensoren automatisch geöffnet.

Error-Logs:
Zurück im Hauptmenü vom Sync-Monitor gelangen Sie durch Auswahl der Schaltfläche „Error Logs“ auf die Seite Error-Logs des ausgewählten überwachten Knotens. Auf dieser Seite werden die Logmeldungen seit dem letzten Systemneustart angezeigt. Wenn die Flash-Speicherkarte voll ist, werden die älteren Protokolle überschrieben.

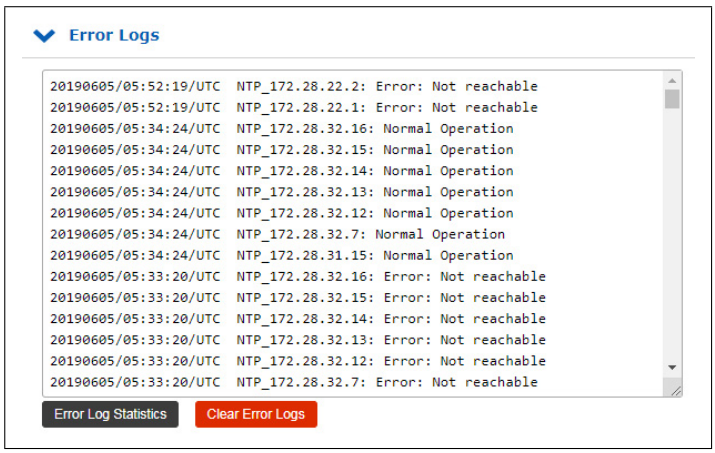
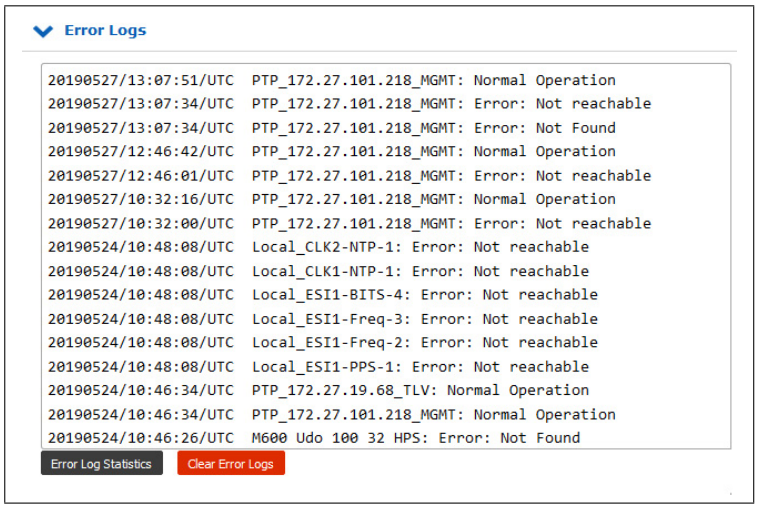
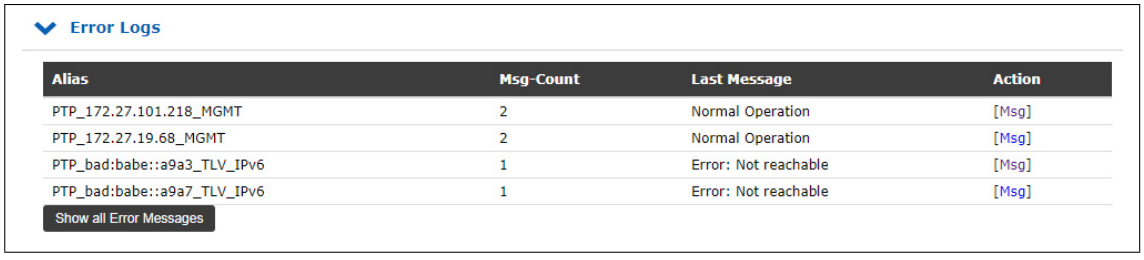


Abbildung: Fehlermeldungen für einen ausgewählten überwachten Knoten.

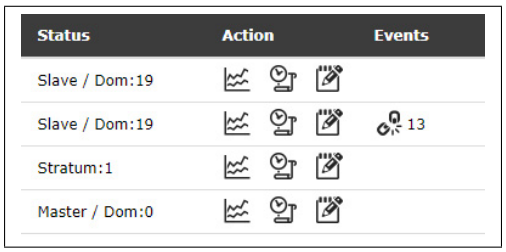
Am unteren Rand der Seite befindet sich eine Schaltfläche **„Show Global Error Logs“**, mit der Sie alle Fehlermeldungen von allen überwachten Knoten anzeigen können.



Mit **„Error-Log löschen“** werden alle Log-Einträge entfernt. Mit **„Error-Log-Statistik“** wird eine Übersicht über die Protokolle aller Knoten angezeigt.

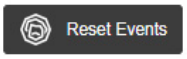


10.1.8.10 Events



In der allgemeinen Übersichtstabelle ist die letzte Spalte Events verschiedenen Alarmen zugeordnet, die für überwachte Knoten definiert sind:

- Offset-Grenze überschritten
- nicht erreichbar
- Stratum Limit überschritten
- Überwachung nicht aktiv



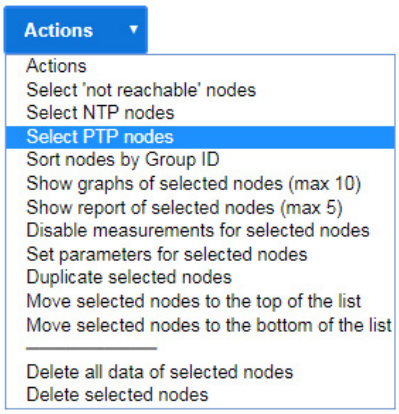
Bei „Offset Limit überschritten“ und „Nicht erreichbar“ wird in der Tabelle der überwachten Knoten in der Spalte Events ein Symbol mit der Anzahl der Ereignisse angezeigt. Diese Ereignisse werden alle 10 Sekunden automatisch aktualisiert. Mit dem Button **„Ereignisse zurücksetzen“**, der sich oberhalb der Übersichtstabelle befindet, können Sie den aktuellen Zähler für die Events zurücksetzen. Diese Ereignisse werden auch in der SyncMap angezeigt.

10.1.8.11 Aktionen für ausgewählte Knoten

In der Firmware-Version 7.00 und neuer können Sie bestimmte Aktionen gleichzeitig auf eine Reihe von ausgewählten Knoten aus der Tabelle anwenden. Aktivieren Sie zunächst die Knoten, die Sie verwalten möchten, entweder durch einzelnes Anklicken eines Kontrollkästchens am Anfang jedes Knotens oder durch Anklicken eines „+"-Zeichens in der oberen Zeile der Tabelle, wenn Sie alle Knoten zusammen auswählen möchten.

Um die Auswahl eines ausgewählten Knotens aufzuheben, klicken Sie entweder erneut in sein Kontrollkästchen und er wird abgewählt oder klicken Sie auf das Symbol **„-"** in der oberen Zeile und Sie werden alle Knoten gleichzeitig abwählen.

Wenn Sie auf die Schaltfläche **„Aktionen für ausgewählte Knoten"** klicken, finden Sie die Aktionen, die Sie über die Knoten anwenden können.



Alle „nicht erreichbaren" Knoten markieren:
Auswahl aller Knoten, deren Offset-Status „nicht erreichbar" anzeigt.

Alle NTP-Knoten markieren:
Auswahl aller Knoten, die über NTP überwacht werden.

Alle PTP-Knoten markieren:
Auswahl aller Knoten, die über PTP überwacht werden, entweder MGMT oder mit TLV-Nachrichten.

Knoten nach Gruppen-ID sortieren:
Die vollständige Liste der Knoten wird nach Gruppen-ID sortiert.

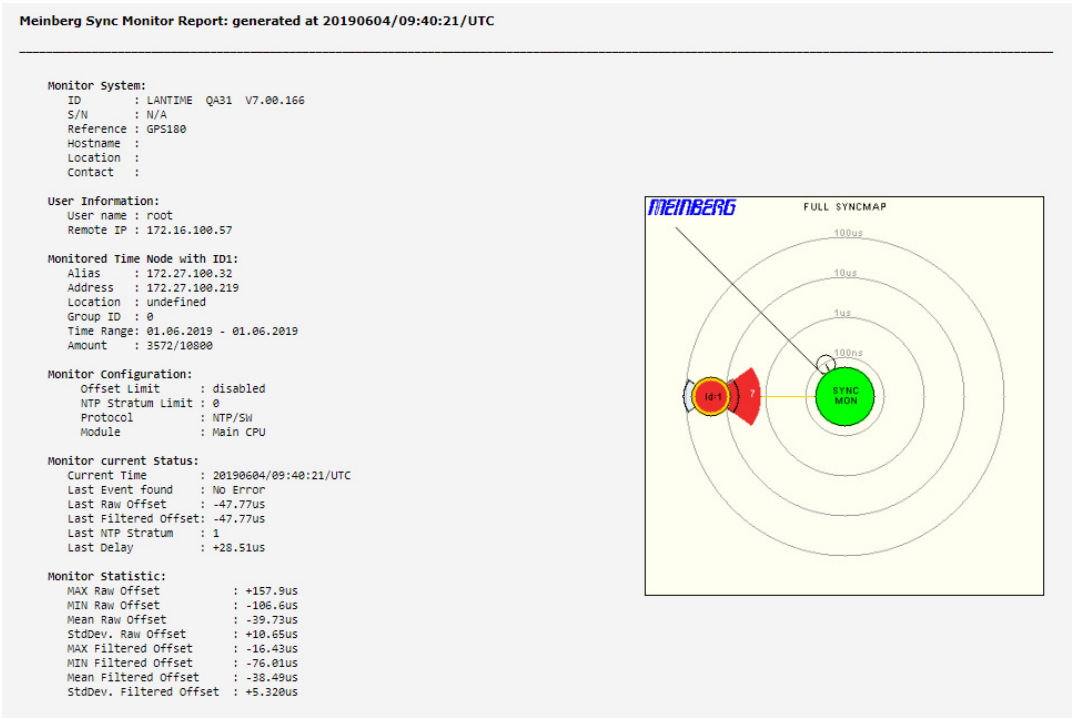
Zeigt die Übersicht des aktuellen Tages an:
Wenn keiner der Knoten primär ausgewählt wurde, werden grafische Diagramme des aktuellen Tages in Miniaturansichtsform für alle Knoten in der Tabelle angezeigt. Neben den grafischen Diagrammen werden auch die Statusinformationen und Statistiken über die aktuellen Tagesmessungen angezeigt.

Übersicht über den Zeitbereich anzeigen:
Wenn keiner der Knoten primär ausgewählt wurde, werden grafische Diagramme des ausgewählten Zeitbereichs in Miniaturansichtsform für alle Knoten in der Tabelle angezeigt. Neben den grafischen Diagrammen werden auch die Statusinformationen und Statistiken über die ausgewählten Zeitbereichsmessungen angezeigt.

Zeigt ein grafisches Diagramm für ausgewählte Knoten an. (max. 10):
Wenn Sie bis zu zehn Knoten in der Tabelle auswählen, können diese im gleichen grafischen Diagramm angezeigt werden. Zuerst müssen Sie einen Zeitraum auswählen, in dem das grafische Diagramm angezeigt wird.

Erstellen eines Berichts für ausgewählte Knoten (max. 5):
Wenn Sie bis zu fünf Knoten in der Tabelle auswählen, werden die aktuellen Daten der ausgewählten Knoten in Form eines Berichts aufbereitet. Zuerst müssen Sie einen Zeitraum auswählen, für den der Bericht generiert wird. Der Bericht enthält die aktuellen Statusdaten, die Konfiguration des Monitors, die Überwachung der statistischen Werte über den ausgewählten Zeitraum und ein grafisches Diagramm, das den Offset-Trend anzeigt.

Außerdem bietet der Bericht auch eine Light-Version einer Sync-Map, die nur die ausgewählten Knoten aus der Tabelle enthält. In der Sync-Map wird jeder einzelne Knoten hervorgehoben und der Rest im Hintergrund dargestellt, um einen Vergleich der Leistung des jeweiligen Knotens im Vergleich zu anderen im Bericht berücksichtigten Knoten zu erhalten.



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
```


Abbildung: Generierter Bericht für ausgewählte Knoten in der Tabelle. Der Bericht enthält Statusinformationen über die ausgewählten überwachten Knoten, die Monitorkonfiguration, die Hauptmonitorstatistiken und grafische Diagramme.

Messungen für ausgewählte Knoten deaktivieren:
Die Knoten, für die Sie Messungen deaktivieren, erhalten den Status „Deaktiviert“. Die Messungen werden für diesen Knoten nicht mehr angefordert und protokolliert. Der zuletzt gemessene Offset wird in der Spalte Offset angezeigt. Um die Messungen erneut zu starten, markieren Sie einen Knoten und wählen Sie **„Messungen für ausgewählte Knoten aktivieren“**.

Parameter für ausgewählte Knoten setzen:
Für die ausgewählten Knoten können Sie gleichzeitig eine Liste von Überwachungsparametern festlegen oder bearbeiten. Wenn Sie diese Funktion auswählen, erscheint der Konfigurationsdialog, in dem Sie jeden der Parameter neu konfigurieren können. Die neue Konfiguration wird auf alle Knoten angewendet, die Sie für diese Aktion ausgewählt haben, nachdem Sie mit der Schaltfläche **„Auf Knoten anwenden“** bestätigt haben.

Duplizieren ausgewählter Knoten:
Die von Ihnen ausgewählten Knoten werden kopiert und unter ihren Ursprungsknoten eingefügt. Anschließend können Sie deren Parameter bearbeiten.

Verschieben Sie ausgewählte Knoten an den Anfang der Liste:
Die ausgewählten Knoten werden an den Anfang der Liste verschoben.

Verschieben ausgewählter Knoten an den unteren Rand der Liste:
Die ausgewählten Knoten werden an den unteren Rand der Liste verschoben.

Alle Daten der ausgewählten Knoten löschen:
Die protokollierten Messdaten der ausgewählten Knoten werden dauerhaft aus dem internen Flash gelöscht.

Markierte Knoten löschen:
Die ausgewählten Knoten werden dauerhaft aus der Liste der Knoten gelöscht. Die bis zu diesem Zeitpunkt protokollierten Messungen bleiben erhalten.

10.1.8.12 Meinberg Sync-Map

Die Meinberg Sync-Map ist eine grafische Darstellung von überwachten Knoten in einem Netzwerk, die als Polardiagramm dargestellt wird. Die Idee der Sync-Map ist es, einen schnellen Überblick über den Synchronisationsstatus aller überwachten Geräte in einer komplexen Netzwerkstruktur zu geben.

Die überwachten Geräte werden als Knoten bezeichnet. Knoten müssen eines der folgenden Signale unterstützen: NTP (RFC1305), PTP (IEEE 1588v2) oder PPS - verbunden mit der ESI (Extension Signal Input) IMS-Karte.

Ziel ist es, einen absoluten Offset der überwachten Knoten in Form von vordefinierten Offset-Grenzen zu visualisieren. Die Daten können nach dem aktuellen Offsetstatus oder über einen wählbaren Zeitbereich (z.B. einen Tag) angezeigt werden. Es ist auch möglich, das dynamische Verhalten der überwachten Knoten der letzten 60 Minuten zu animieren, wobei SyncMaps automatisch jede Minute generiert werden. Dieser Modus wird als SyncMap-Cyclic-Mode bezeichnet.

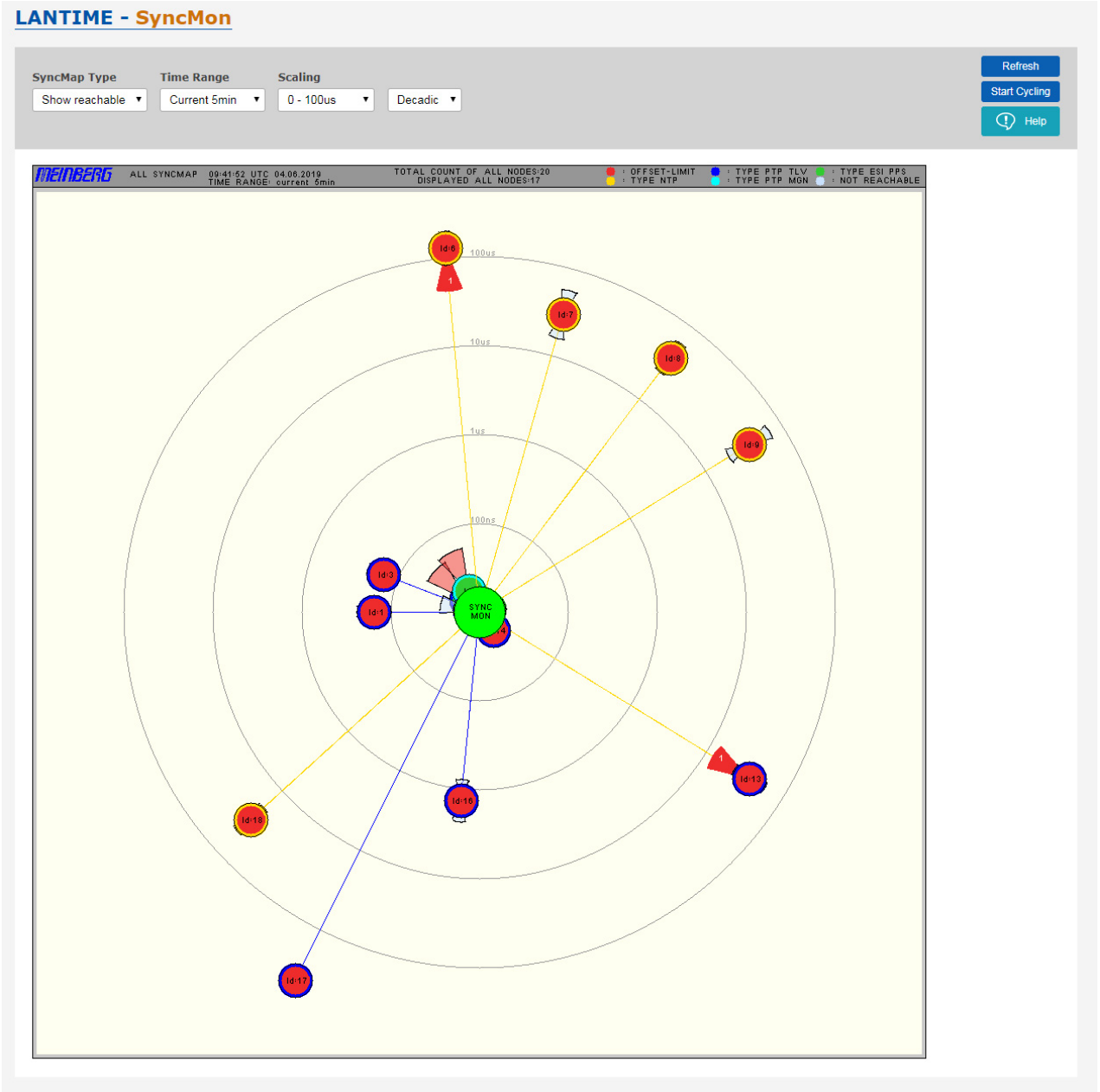


Abbildung: Die SyncMap als grafische Darstellung der überwachten Knoten in einem Netzwerk, visualisiert als Polardiagramm. Es kann Knoten anzeigen, die folgende Protokolle oder Signale unterstützen: NTP, PTP (IEEE 1588v2) oder PPS.

Jeder überwachte Knoten wird als Kreis mit unterschiedlichen statistischen Informationen angezeigt.

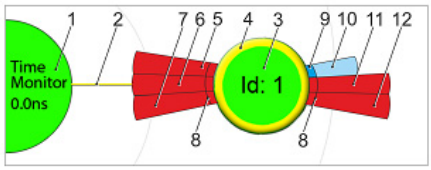


Abbildung: Eine Knoten-Darstellung in der Sync-Map. Die Bedeutung der verschiedenen Farbcodes und Bereiche, die zu einem Knoten gehören, werden nachfolgend im Text erläutert.

In der Mitte befindet sich die Referenzzeitüberwachung mit ihrer Referenzuhr, die als „Zeitüberwachung“ [1] bezeichnet wird. Es stellt eine Timing-Referenz durch einen gesteuerten Oszillator zur Verfügung (synchronisiert durch GPS, GLN, PZF, Galileo, Beidou oder eine externe Taktung). Der Knoten „Zeitüberwachung“ in der Mitte [1] wird grün dargestellt, wenn der Referenztakt synchron ist. Zusätzlich wird der aktuelle Offset zwischen dem gesteuerten Oszillator und der Referenzzeitquelle als Wert [1] angezeigt.

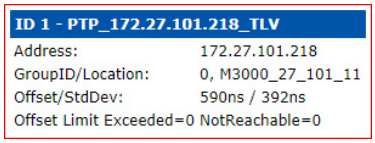
Um das Zentrum herum sind vier konzentrische Kreise gezeichnet, die die Skalierung des Polardiagramms darstellen. Alle Knoten [3] sind konzentrisch durch eine Linie [2] vom zentralen Knoten aus verbunden. Der Abstand von der Mitte zu den Knoten stellt den absoluten durchschnittlichen Zeitversatz zwischen dem Zeitmonitor und jedem einzelnen Knoten dar. Der Mittelwert wird über den gewählten „Zeitraum“ berechnet. Jeder Knoten wird als Kreis mit einer Farbe im Inneren [3] dargestellt, die dem Status entspricht, und einem Außenring [4], der seinem Typ entspricht.

Status:	grün	= Offset < Limit
	rot	= Offset ≥ Begrenzung oder Überschreitung der maximalen Skalierung
Type:	gelb	= NTP
	dunkelblau	= PTP mit TLV
	hellblau	= PTP mit Management-Msgs
	grün	= ESI PPS
	grau	= nicht verfügbar

Zusätzlich die statistischen Werte: Die Standardabweichung [8] wird als Kreissegment dargestellt. Diese Werte stellen den zeitlichen Jitter der Messwerte um den Mittelwert dar. Wenn die Kreissegmentfarbe rot ist, dann ist die Abweichung von der Skalierung abhängig und überschreitet die Hälfte des Bereichs der Dekade → Beispiel: Liegt die mittlere Abweichung im Bereich von 1μs - 10μs und das größte gefundene Maximum > 5μs, dann wird das einzelne Segment rot, sonst blau [10] gezeichnet.

Wenn eines dieser Ereignisse eintritt „Offset-Grenze überschritten“ oder „Nicht erreichbar“, dann wird das Kreissegment dunkelrot und ein Wert (in weiß), der die Anzahl der einzelnen Ereignisse darstellt. Der Kreisabschnitt in der Nähe der Mitte [5,7] stellt die Ereignisse „Nicht erreichbar“ und der äußere Kreisabschnitt [6,7] die Ereignisse „Offset-Limit überschritten“ dar.

Beim Gleiten mit der Maus über einen Knoten in der Sync-Map ohne Anklicken eines entsprechenden Infofensters mit dem Namen werden einige statistische Werte angezeigt:



Durch Auswahl eines bestimmten Knotens in der Sync-Map mit einem linken Mausklick wird das folgende Menü geöffnet:

„Grafik anzeigen“ öffnet das entsprechende grafische Diagramm.

Beispiel für eine vollständige Sync-Map
Das folgende Bild zeigt eine Sync-Map eines Netzwerks mit 250 überwachten NTP-Knoten, die auf einem SyncFire Server laufen. Das ist eine echte Messung unseres Test-Netzwerks für Burn-In-Tests in der LANTIME-Produktion. Die rot markierten Knoten sind DCF77-Empfänger ohne Kompensation der Entfernung zwischen einem Senderstandort und einem Empfänger.

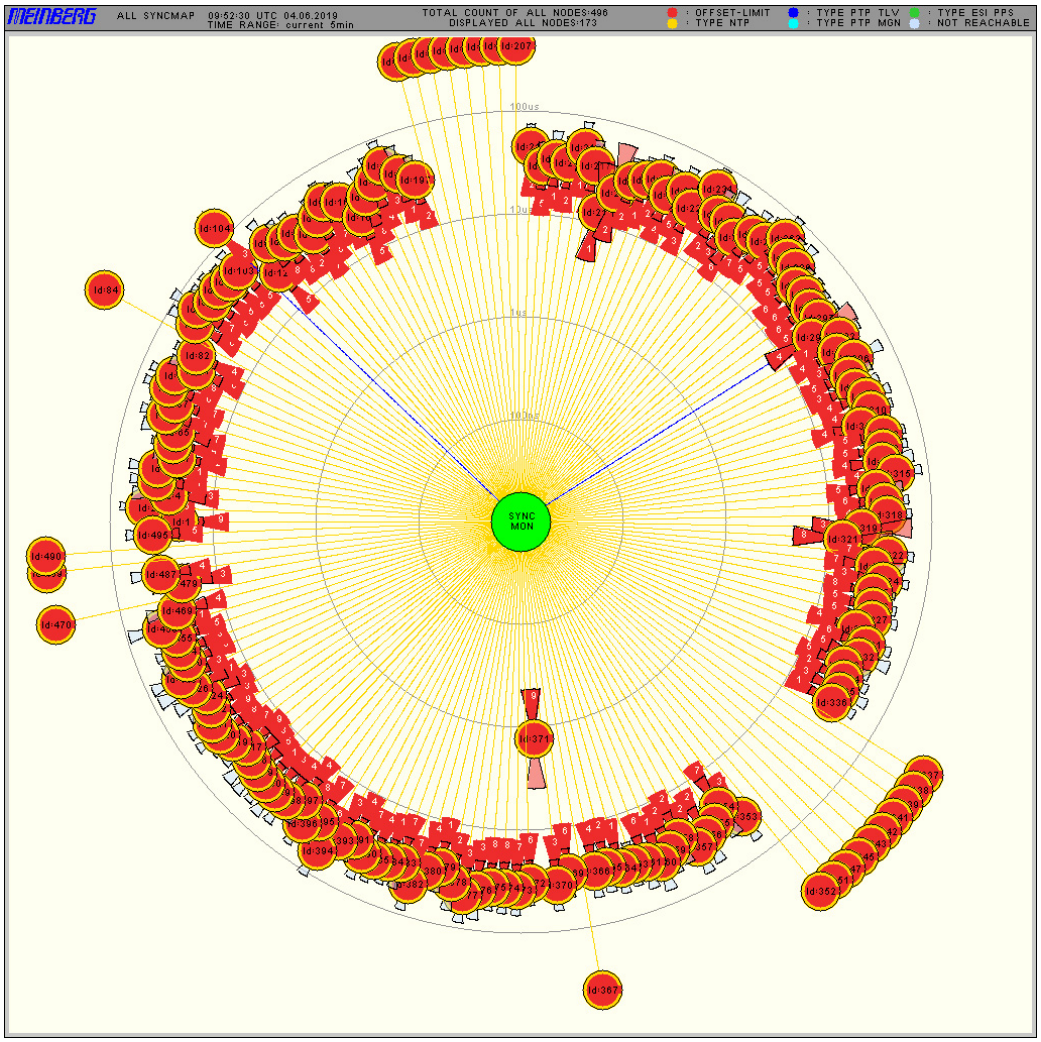


Abbildung: Ein Beispiel für eine Sync-Map mit 250 Knoten.

Sync-Map Typ:

- Erreichbarkeit anzeigen: Aktuell erreichbare Knoten werden in der Sync-Map angezeigt.
- Alle Knoten anzeigen: Alle in der Überwachungsliste konfigurierten Knoten werden in der Sync-Map angezeigt, auch wenn sie nicht erreichbar sind.
- Nur NTP anzeigen: In der Sync-Map werden nur Knoten angezeigt, die über das NTP-Protokoll überwacht werden. Sie werden von einem gelben Ring umgeben.
- Nur PTP anzeigen: Nur Knoten, die über das PTP-Protokoll überwacht werden, werden in der Sync-Map angezeigt. Knoten erscheinen mit einem dunkelblauen Ring, wenn das PTP mit TLV-Protokoll zur Überwachung verwendet wird, oder mit einem hellblauen Ring, wenn das PTP-Protokoll mit Management-Meldungen verwendet wird.

Zeitraum: Die Sync Map kann aus den Überwachungsdaten erzeugt werden, die in den letzten 30 min, 5 min, 24 h oder in einem manuell gewählten Zeitraum aufgenommen wurden. Auch die statistischen Werte werden aus den Daten des gewählten Zeitintervalls berechnet.

Skalierung: Mögliche Skalierungsoptionen: Dekadenschritte oder linear für verschiedene Zeitgenauigkeitsbereiche. Für PTP-Knoten kann es sinnvoll sein, die Skalierung im unteren Mikrosekundenbereich zu verwenden, während für NTP Bereiche von wenigen 100 Mikrosekunden oder Millisekunden gewählt werden können.

Aktualisieren-Button: Aktualisiert sofort die Sync-Map basierend auf den aktuell verfügbaren Statistiken der einzelnen Knoten. Es wird eine neue Sync-Map mit dem gewählten Zeitraum generiert - es ist wie ein Neuladen dieser WEB-Seite mit den neuesten Messungen.

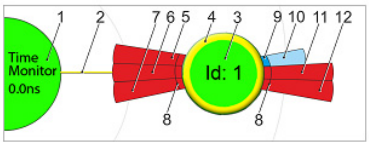
Start Zyklus: aktiviert den Sync-Map-Animationsmodus. In diesem Modus wird jede Minute eine neue Sync-Map mit den neuesten Messungen generiert. Die letzten 60 Sync-Maps werden dann als Animation angezeigt. Eine neue Sequenz beginnt mit einer leeren Sync-Map. Der Statistikzeitbereich wird standardmäßig auf 5 min festgelegt.

Die Anzahl der im RAM gespeicherten PNGs wird im automatischen Aktualisierungsmodus bei einer Q7-CPU oder einem Syncfire auf 1000 gesetzt.

Hilfe-Button: zeigt die Online-Hilfeseite für die Sync-Map-Funktion an.

10.1.8.13 Sync Map - Hilfe

Meinberg SyncMap Help Page



The SyncMap is a graphical representation of Time-Synchronization in a network visualized as a polar diagram.

A short legend:
[1] The Time Monitor node and the current offset measured between its oscillator and the reference time.
[2] Line connecting each node with the SyncMon. Its length represents the absolute average time offset between Reference of SyncMon and the node.
[2] The color defines the sign of the average: yellow=negative blue=positive
[3] A measured node, its color inside corresponds to its status.
[4] Outer ring which corresponds the type of the node.
[5] Event counter for "Node not reachable".
[6] Event counter for "Node Offset Limit exceeded".
[7] If Event counter > 0 then this slide is dark red. If Event counter = 0 the Standard Deviation is light red or light blue.
[8] Standard deviation measurement. If light red, it exceeds the 100 percent of current offset, otherwise is blue.

The Network Sync Manager with its reference clock stands in the middle, labeled as the "SyncMon" [1]. It provides a timing reference with its controlled oscillator (synchronized by GPS, GLN, PZF, Galileo, Beidou or an external clock supply). The Time Monitor node in the center [1] is shown in green color when the reference clock is synchronous.

Around the center 4 concentric circles representing the scaling of the polar diagram are drawn. All nodes [3] are connected concentrically by a line [2] from the central node. The distance from the center to the nodes represents the absolute average time offset between the Time Monitor and each individual node. The average value is calculated over the selected "Time Range". Each node is shown as a circle with a color inside [3] that corresponds the status and an outer ring [4],that corresponds the type.

```
Status: green = Offset < Limit
        red   = Offset >= Limit or outside the maximum scaling
Type:   yellow        = NTP
        dark blue     = PTP with TLV
        light blue    = PTP with Management Msgs
        green         = ESI PPS
        grey          = not available
```

Additionally, the statistical values: the standard deviation [8] respectively is represented as circle segments. This value represent the temporal jitter of the measured values around the mean value. When the circle segment color is red, then the deviation is dependent on the absolute average time offset and it exceeds the double (100%) of the absolute average time offset -> example: if average time offset is 5us and the standard deviation 10us (2001750f the average time offset), then the individual segment is drawn red, otherwise blue [10].

If one of the events occure "Offset Limit Exceeded" or "not reachable" then the circle segment will become dark red and a white value which represents the count of each event. The circle slide near the center [5,7] represent the Event "not reachable" and the outer circle slide [6,7] represent the Event "Offset Limit Exceeded".

Close Window

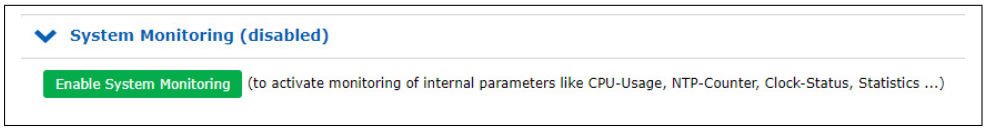
Eine kurze Legende:

1 Der Time Monitor-Knoten und der aktuelle Offset, der zwischen seinem Oszillator und der Referenzzeit gemessen wird.
2 Linie, die jeden Knoten mit dem SyncMon verbindet. Seine Länge stellt den absoluten durchschnittlichen Zeitversatz zwischen Referenz von SyncMon und dem Netzwerk-Knoten dar.
Die Farbe definiert das Vorzeichen des Mittelwertes: gelb=negativ blau=positiv
3 Ein gemessener Knoten, dessen Farbe im Inneren seinem Status entspricht.
4 Äußerer Ring, der dem Typ des Knotens darstellt.
5 Ereigniszähler für „Node not reachable“.
6 Ereigniszähler für „Node Offset Limit exceeded“.
7 Wenn der Ereigniszähler > 0 ist, dann ist diese Folie dunkelrot. Wenn der Ereigniszähler = 0 ist, ist die Standardabweichung entweder hellrot oder hellblau.
8 Standardabweichungsmessung. Wenn die Fläche hellrot ist, überschreitet es die 100-Prozent des aktuellen Offsets, ansonsten ist die Fläche blau.

10.1.8.14 System Monitoring

System Monitoring überwacht interne Signale im LANTIME-System, die nicht zu den überwachten Knoten gehören (z.B. CPU-Auslastung, lokale NTP-, ESI-Eingänge, MRS-Referenzen und Referenzuhrparameter). Die Anzahl und Art der internen Signale hängt von den integrierten Hardwarekomponenten in einem LANTIME-System ab.

Die Systemüberwachung ist eine optionale Funktion und standardmäßig deaktiviert. Sie kann im Menü „Sync-Mon → Systemeinstellungen“ im Dialogfeld Systemparameter aktiviert werden oder direkt über den Reiter „System Monitoring“:

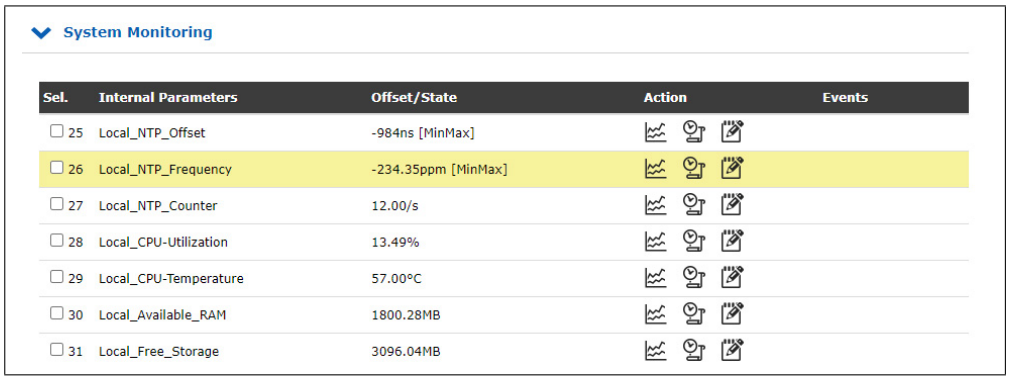


Wenn die Systemüberwachung aktiviert ist, werden alle Signale automatisch gemessen und protokolliert, wie bei der Knotenüberwachung, d.h. der Menüpunkt „Systemüberwachung“ ist sichtbar.

Die Anzahl der MRS-Referenzen (CLK1-GPS-0, CLK1-NTP-1, CLK1-PTP-2 ...) hängt von den aktivierten Quell-Prioritäten für jede Referenzuhr ab - das kann über „MRS-Settings“ im Webinterface-Menü „Clock“ für jede eingesetzte Referenzuhr konfiguriert werden.

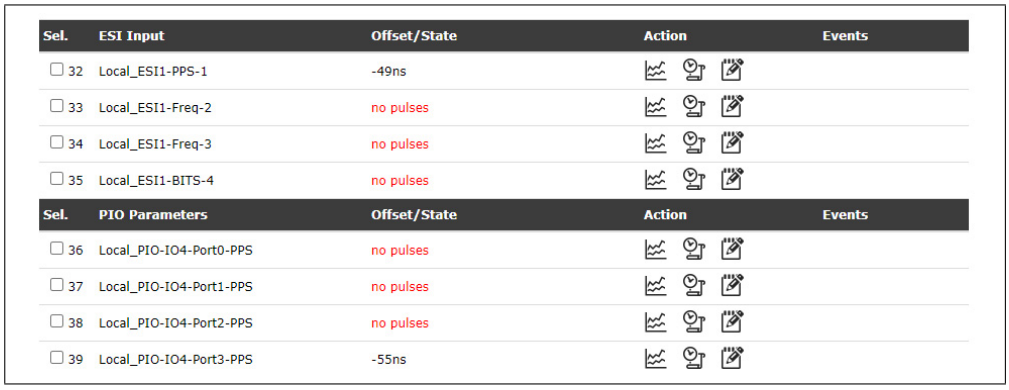
Jeder Knoten aus dem „System Monitoring“ kann selektiert werden und gemeinsam mit Knoten aus dem „Node Monitoring“ in einer Grafik dargestellt werden.

Liste der möglichen Sensoren in SyncMon:



Interne Parameter:

NTP-Offset
NTP-Frequenz
NTP-Counter
Local_CPU-Utilization
Local_CPU-Temperatur
System Free RAM Memory-Status
System Flash Storage-Status

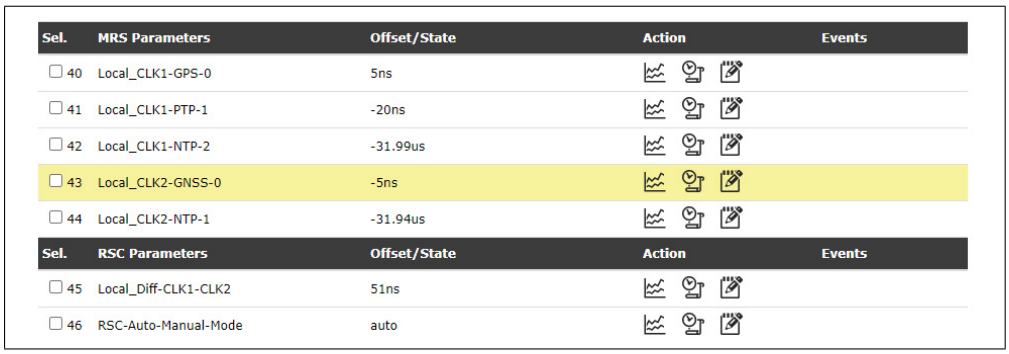


ESI Eingang:

ESI PPS in
ESI Freq in
ESI BITS in

PIO Parameter:

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 Referenzeingänge:

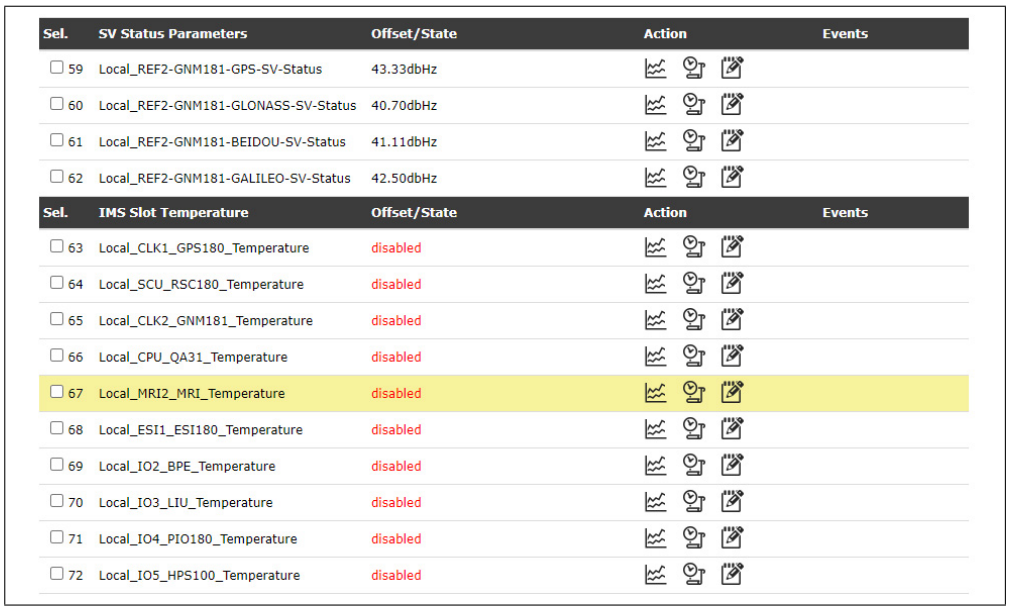
Standard-GPS
10 MHz Eingangsfrequenz
1 PPS Eingangssignal
kombiniertes 10 MHz plus PPS
IRIG Eingang
Network Time Protocol (NTP)
Precision Time Protocol (PTP/IEEE1588)
feste Frequenz
1 PPS zusammen mit Zeittelegramm
variable Eingangssignale über GPIO
DCF77: PZF bietet viel mehr Genauigkeit als ein Standard-LWR
Langwellenempfänger z.B. DCF77 AM, WWVB, MSF, JJY
GNSS Empfänger

RSC Parameter:

Local_Diff-CLK1-CLK2
RSC-Auto-Manual-Mode

Für jede Referenzuhr:

- 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 Parameter:
- GPS-SV-Status
- GLONASS-SV-Status
- BEIDOU-SV-Status
- GALILEO-SV-Status

IMS Slot-Temperatur: CLK, SCU, CPU, MRI, ESI, IO

10.1.8.15 NTP Zugriffsstatistik

Der LANTIME zählt automatisch alle eingehenden Netzwerkpakete am UDP-Port 123 aller verfügbaren Netzwerkschnittstellen. Diese Statistik wird in der Tabelle „System Monitoring“ unter **Local_NTP_Counter** grafisch dargestellt. Die rote Linie zeigt einen Wert der empfangenen NTP-Pakete innerhalb eines ausgewählten Zeitraums an.

10.1.8.16 Error Logs

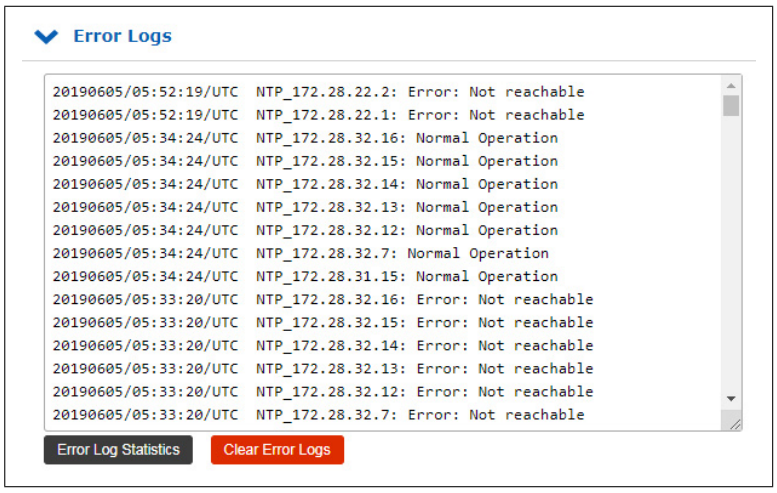


Abbildung: Protokollieren Sie Meldungen von allen überwachten Knoten.

Das globale Fehlerprotokoll bietet die Möglichkeit, alle Fehlerereignisse zu verfolgen.

Fehlerprotokoll-Statistik: Kategorisierung von Fehlerprotokollen für jeden einzelnen Knoten.
Fehlerprotokolle löschen: Löscht die Liste der protokollierten Fehler.

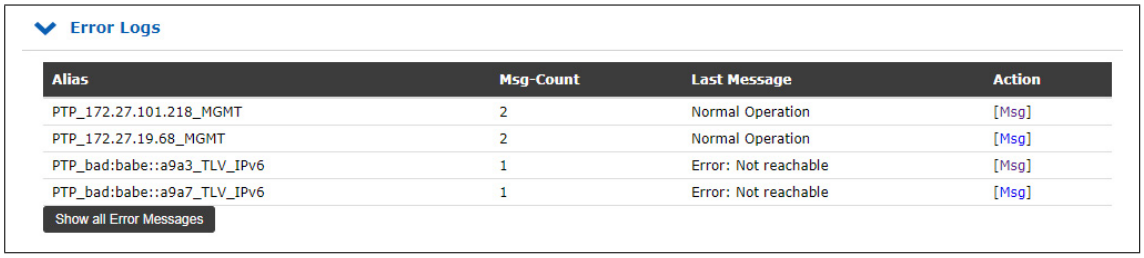


Abbildung: Fehlerprotokoll-Statistik.

10.1.8.17 Systemeinstellungen

Das Menü „Systemeinstellungen“ zeigt den aktuell verfügbaren Speicherplatz auf der Flash-Disk an und berechnet die Anzahl der Tage, die gespeichert werden können, abhängig von der Anzahl der überwachten Knoten und dem Protokollintervall.

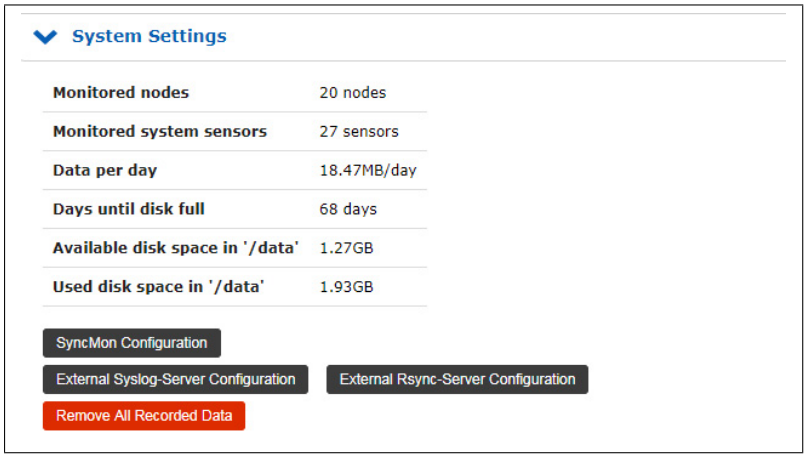


Abbildung: Status der Speicherkarte, verfügbarer Speicherplatz und Archivierungsoptionen für Protokolldateien.

Es ist ein Indikator implementiert, der über den verfügbaren Flash-Speicherplatz „Verfügbarer Platz auf dem Flash-Speicher“ und die Anzahl der verbleibenden Tage für die Überwachung des aktuellen Sync-Knoten-Setups informiert. Die aktuellen Daten werden auf der Flash-Karte gespeichert.

Mit der Schaltfläche „Alle erfassten Daten entfernen“ werden alle Dateien auf dem zu Sync-Mon gehörenden Flash-Speicher ohne Backup entfernt.

10.1.8.18 Überwachungsdaten als Backup an externen SYSLOG-Server senden

Im SyncMon-Menü im Web-Interface-Menü „Systemeinstellungen → Externe Syslog-Server-Konfiguration“ können Sie bis zu 3 externe Server konfigurieren, auf denen die Messdaten in jedem Protokollintervall über das SYSLOG-Protokoll gesendet werden. Auf dem externen Server muss ein Dienst wie ein Standard Syslog-Server laufen.

Um die Überwachungsdaten zu sichern und für die spätere analytische Verarbeitung zu speichern, können Sie das automatische Senden der Daten über das SYSLOG-Protokoll an bis zu 3 externe Datenbankserver ermöglichen. In diesem Fall wird jede in einem Protokollintervall verarbeitete Knotenmessung an einen bestimmten Server gesendet.

Im folgenden Dialog können Sie die Zielserver konfigurieren, auf denen Sie Ihre Daten speichern möchten.

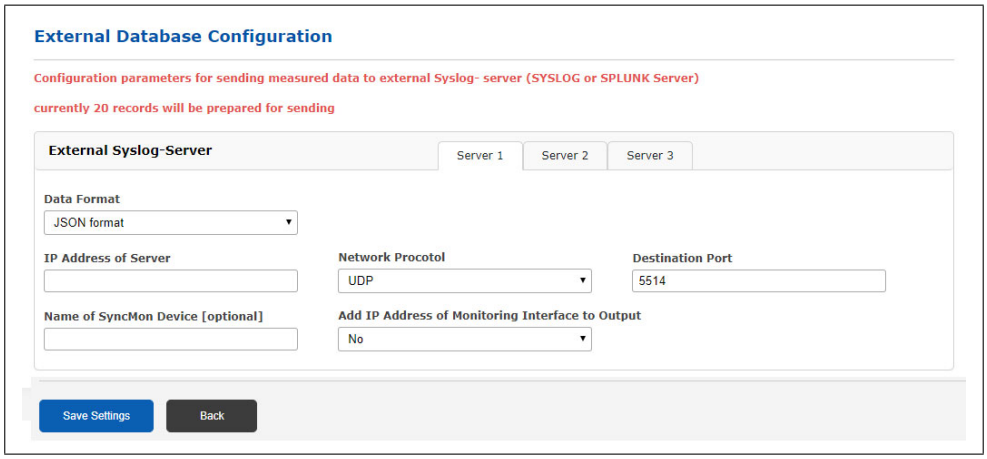


Abbildung: Konfigurationsoptionen für externe Datenbankserver, auf denen die Überwachungsdaten gespeichert werden können.

Für jeden dieser externen Server können die folgenden Parameter eingestellt werden:

- Netzwerkprotokoll: UDP oder TCP
  - Konfiguration des Ausgabeformats:
  - Meinberg Standardformat
  - Key-Value-Paare (SPLUNK-kompatibel)
  - JSON-Format
- eine Portnummer (Standard ist 514 für Standard-SYSLOG)
- ein Gerätename
- optional kann die IP-Adresse des für die Messung verwendeten Netzwerkports aktiviert werden.

Als Netzwerkprotokoll-Optionen können Sie zwischen dem UDP- oder TCP/IP-Protokoll wählen, das standardmäßig auf einem Port:514 läuft.

Name dieses SyncMon-Gerätes: Sie können Ihr Netzwerk durch verschiedene Sync-Monitoring-Geräte überwachen. Sie können ihnen eindeutige Namen geben, um sie auf dem Datenbankserver, von dem die Daten stammen, leicht zu erkennen.

Das Meinberg Standard-Format entspricht dem SyncMon-Datenformat, das in einem Dateisystem auf einem LANTIME gespeichert ist. Dieses wird später für den SyncMon-Manager verwendet. Der SyncMon-Manager befindet sich derzeit in der Entwicklung und kann die auf einem externen Server gespeicherten Daten visualisieren und Berichte erstellen.

Ein Auszug aus dem SyncMon-Format „Meinberg Standard“, das per Syslog-Protokoll gesendet wird:

```
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
```

Für weitere Details zu den SyncMon-Formaten siehe Kapitel „Technischer Anhang → SyncMon Formate“.

10.1.8.19 Überwachungsdaten auf externen Server über RSYNC als Backup kopieren

Im Web-Interface-Menü „SyncMon → Systemeinstellungen → Externe Rsync-Server Konfiguration“ können Sie bis zu 3 externe Server konfigurieren, auf die die Messdaten stündlich oder einmal um 00:00 UTC über das RSYNC-Protokoll kopiert werden. Auf dem externen Server muss ein Dienst wie ein Standard-RSYNC-Server laufen.

Im folgenden Dialog können Sie die Zielserver konfigurieren, auf denen Sie Ihre Daten speichern möchten:

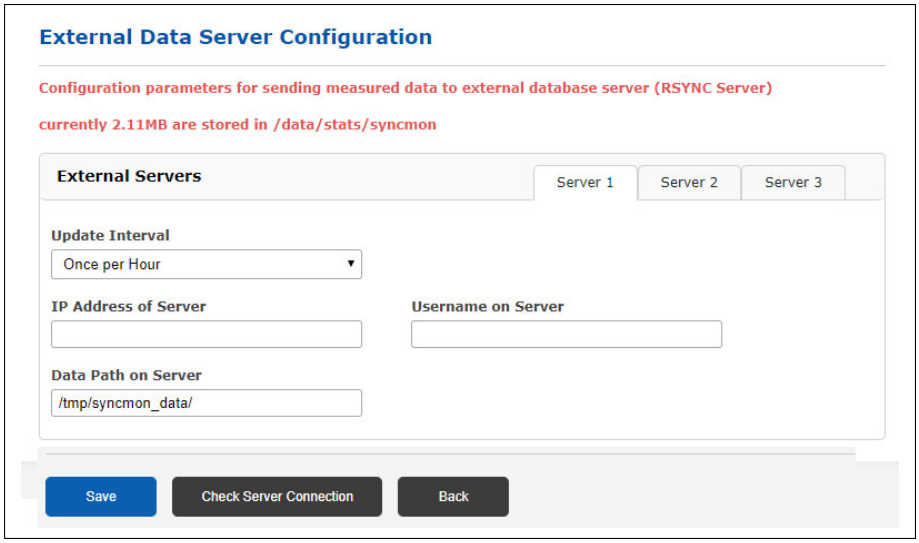


Abbildung: Externe Syslog- oder Splunk-Server-Konfiguration

Um Daten stündlich oder einmal täglich automatisch über **‘rsync‘** zu versenden, müssen Sie den ssh-Key für den externen RSYNC-Server vorbereiten:

- Anmeldung über SSH beim LANTIME
- Überprüfen Sie, ob Identitäten in */root/.ssh/id_rsa.pub* verfügbar sind.
- Wenn nicht, dann erstellen Sie eine Identität mit **‘ssh-keygen -t rsa‘**.
- Speichern Sie diese Identität für den dauerhaften Gebrauch mit: **‘saveconfig @‘**.
- Kopieren Sie die Identität des LANTIME auf den externen RSYNC-Server mit: **‘ssh-copy-id ip-adresse-of-RSYNC-server‘**.

10.1.8.20 SyncMon Konfiguration

Mit der Schaltfläche „SyncMon Konfiguration“ können einige Systemkonfigurationsparameter eingestellt werden:

- Quellport der ausgehenden NTP-Pakete: Standard ist 33000.
- Basispfad für Logdateien für die Historie der Tage. Der Standardpfad ist die interne Compact-Flash mit /data. Das kann z.B. durch Verwendung eines USB-Memorysticks in /mnt/usb-storage geändert werden.
- Aktivieren Sie die Überwachung der systeminternen Parameter.

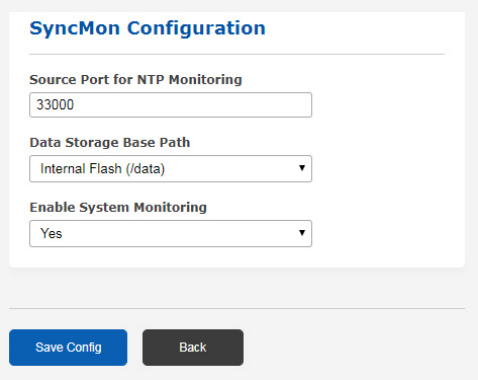


Abbildung: Systemparameter-Einstellungen innerhalb der SyncMon-Funktion. Hier können Sie den aktuellen Pfad einstellen, in dem die Daten gespeichert werden. Beachten Sie, wenn die Speicherkarte voll ist, werden die ältesten Daten überschrieben.

Systemüberwachung aktivieren: Die Überwachung von internen Signalen wie CPU-Auslastung, lokale NTP-, ESI-Eingänge, MRS-Referenzen und Referenzuhrparameter, abhängig von der integrierten Hardware des Systems, wird aktiviert. Standardmäßig ist die Überwachung des Systems deaktiviert.

Die Messdaten der überwachten Knoten werden in separaten Verzeichnissen auf einer Flash-Disk gespeichert. Der Basispfad der gespeicherten Datendateien kann vom Benutzer konfiguriert werden, daher ist es auch möglich, eine externe Flash-Disk (z.B. USB-Stick) zu verwenden. Die Daten werden für jeden Tag und jeden überwachten Knoten separat gespeichert.

```
/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
    |         |         |              |       ...
```

Abbildung: Beispiel für die Standardpfadstruktur der Historie der Tagesdatendateien auf der Flash-Karte.

Das Format der Datendatei:

1. MJD: Modifiziertes julianisches Datum - ist die kontinuierliche Anzahl der Tage seit Beginn der Julianischen Periode (begonnen um 1858 Nov 17 - 0:00 Uhr).
2. Zeit nach Mitternacht in Sekunden
3. Zeitstempel (ISO von MJD und Zeit nach Mitternacht)
4. gemessener Taktversatz roh (Wenn das Anforderungsintervall kleiner als das Aufzeichnungsintervall ist, dann wird der Mittelwert der gemessenen Offsets im Anforderungsintervall gespeichert).
5. bei NTP: Clock Offset Median (Median der 5 zuletzt gemessenen Offsets auf Anfrage)
   im Falle von PTP: gemeldeter Offset
6. Pfadverzögerung in Sekunden
7. NTP-Schicht oder PTP-Status
8. 'R' (optionales Kennzeichen für Min/Max-Werte von Rohdaten: wenn das Anforderungsintervall kleiner als das Protokollintervall ist, dann werden automatisch die Min- und Max-Werte der Rohdaten in den nächsten 2 Zeilen gespeichert.
9. siehe 8. (optional)
10. siehe 8. (optional)
11. 'M' (optionaler Indikator für Min/Max-Werte von MTie-Werten (Maximum Time interval error) von PTP-Knoten, der diese Option unterstützt: Wenn der PTP-Knoten MTie-Funktion mit erweiterten TLVs unterstützt, werden die Min- und Max-Werte in den nächsten 2 Zeilen gespeichert.
12. siehe 11. (optional)
13. siehe 11. (optional)

Auszüge von Überwachungsdaten, die in der Historie der Tagesdateien gespeichert sind:

Beispiel für NTP-Datendateien:

```
# 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
```

Beispiel für NTP-Datendateien mit Anfrageintervall kleiner als Protokollintervall:

```
# 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
```

Beispiel für PTP-Datendateien:

```
# 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
```

Beispiel für PTP-Datendateien mit Unterstützung der Mtie-Funktionalität:

```
# 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
```

10.1.8.21 Systemnutzung

Mit der neuesten SyncMon-Version ist es möglich, bis zu 1000 Knoten zur Überwachung zu konfigurieren. Das Anforderungs- und Protokollierungsintervall kann auf 1s eingestellt werden. Beachten Sie, dass die System-CPU bei hohen Knotenzahlen und niedrigen Anforderungs- und Protokollintervallen stark belastet wird. Dies kann auch die Leistung des NTP-Servers beeinträchtigen.

Beispiele:

- 10 Überwachungsknoten mit Log-Intervall = 1s speichern 70MBytes (69194kBytes) pro Tag - die Standardgröße des für die SyncMon-Protokollierung verwendeten Flash beträgt etwa 400MB - also können 5 Tage auf der internen Flash-Disk gespeichert werden.
- 100 Überwachungsknoten mit Log-Intervall = 1s speichern 700 MB pro Tag - dann stoppt die Datenaufzeichnung, wenn der Flash-Speicher voll ist - die Log-Rotation für SyncMon wird um 00:00 UTC gestartet und löscht Dateien, die älter als 2 Tage sind. Die CPU-Auslastung wird um ca. 10% steigen.
- 100 Überwachungsknoten mit Anforderungsintervall = 1s und log-interval = 64s speichern ca. 12MBytes pro Tag - so können ca. 40 Tage auf der internen Flash-Disk gespeichert werden. Die CPU-Auslastung wird um ca. 7% steigen.
- 900 Überwachungsknoten mit Anforderungsintervall = 1s und log-interval = 64s speichern ca. 100MBytes pro Tag - so können ca. 4 Tage auf der internen Flash-Disk gespeichert werden. Die CPU-Auslastung wird um 45% steigen.
  - this is critical for the NTP server performance of the device.

The size of a data file per day depends on the logging interval and has a size of about 110kB if log-interval is 64s.

10.1.8.22 Sync Monitor Status-Datei über CLI

Der aktuelle Status der überwachten Knoten, wie er im Web-GUI angezeigt wird, wird in einer ASCII-Datei */var/lo /syncmon_node_status* gespeichert. Diese Datei wird nach jedem vollständigen Scan der konfigurierten Knoten aktualisiert und ist über CLI zugänglich.

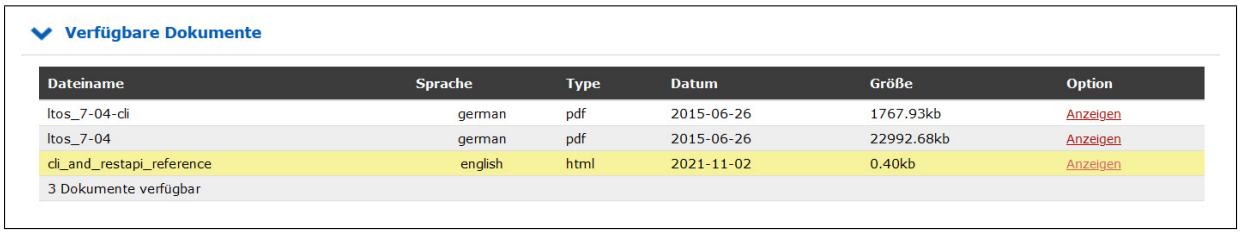
```
#   Net Sync Monitoring Status with total 15 Nodes (updated  at  ...)

#   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
```

Abbildung: Die Statusinformationstabelle, auf die über ein CLI zugegriffen werden kann.

Konfiguration über CLI
Die Konfigurationsdatei kann mit einem Texteditor direkt in der Kommandozeile (CLI) des Systems bearbeitet oder durch eine externe vorbereitete Datei ersetzt werden. Weitere Informationen finden Sie in der LANTIME CLI-Referenz.

10.1.9 Dokumentation und Support

Diese Seite bietet Ihnen Zugriff auf einige Dokumente, die auf Ihrem LANTIME-System gespeichert sind, insbesondere die aktuellsten Firmware-Handbücher. Die Liste enthält Dateiname, Sprache, Dateityp, Datum und Größe der Dokumente.



LT_CLI-Help
Zusätzlich steht auch noch ein Link zur LT_CLI-Onlinehilfe zur Verfügung. Diese Onlinehilfe ist bei allen IMS LANTIME-Geräten und bei allen SyncFire-Systemen mit einem Arbeitsspeicher (RAM) $\geq$ 512 MB auf dem System verfügbar und kann über den Link geöffnet werden.

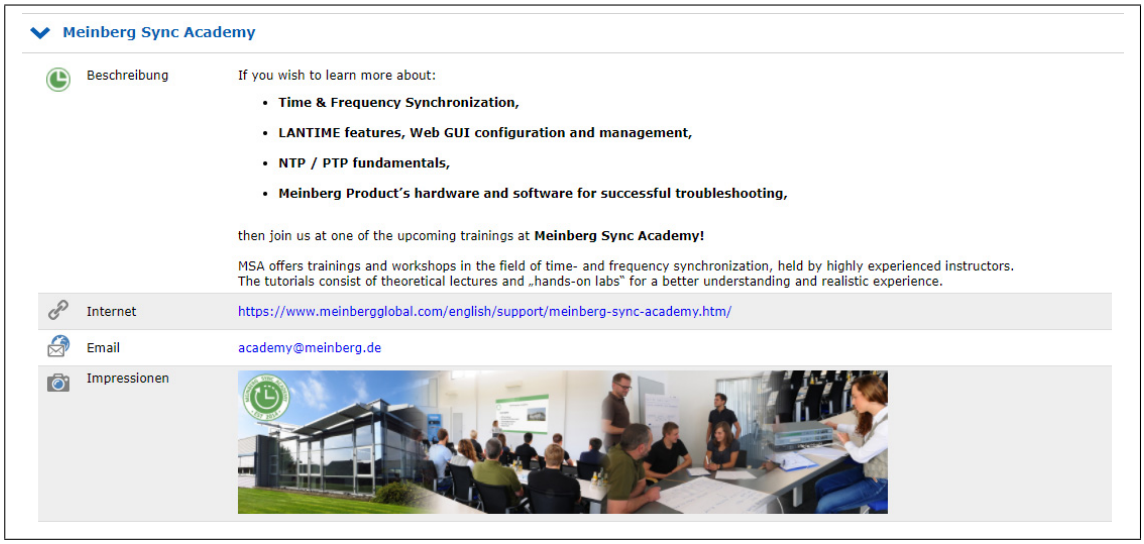
Für Benutzer, die nicht über ein solches System verfügen, haben wir eine Online-Hilfe auf unserem Public-Webserver hinterlegt: http://demo.meinberg.de/lt_cli/

Darüber hinaus kann diese CLI-Hilfe auch als ZIP-Archiv heruntergeladen werden:
http://demo.meinberg.de/lt_cli/firmware-7.04.008-x86-clihelp.zip

Sie müssen diese Datei nach dem Download in Ihr eigenes Dateisystem, in Ihrer Netzwerkumgebung oder auf Ihrem PC, entpacken. Danach kann die Hilfe wie eine normale Webseite verwendet werden.

Im Submenü „Support-Informationen“ finden Sie alle notwendigen Informationen, wie Sie den technischen Support kontaktieren können. Darüber hinaus finden Sie hier einen Link zum Firmwareportal von Meinberg.

Die Registerkarte „Docs & Support“ enthält auch einige wichtige Weblinks. Darüber hinaus erhalten Sie Informationen über die Meinberg Sync Academy (MSA).



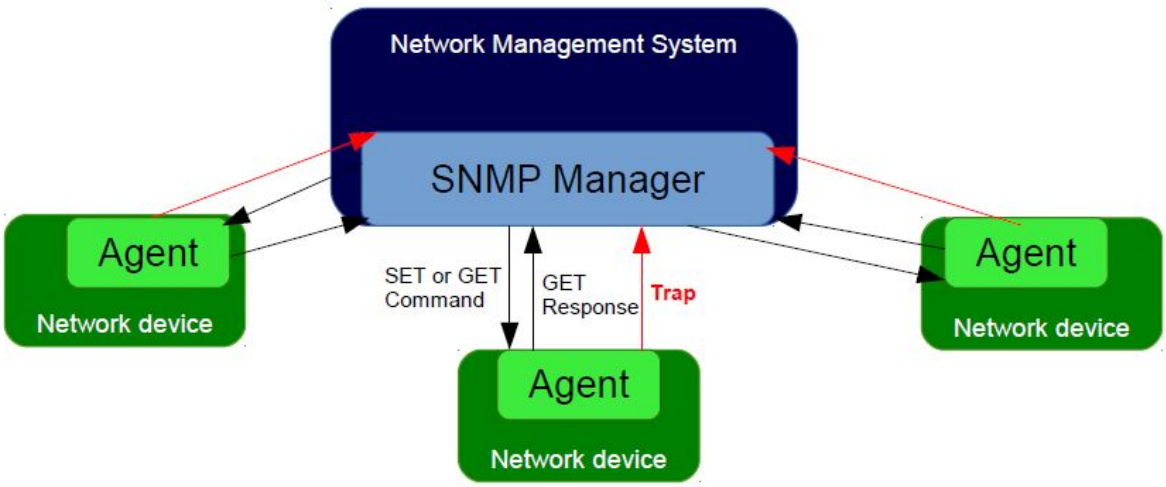
Die Meinberg Sync-Academy bietet und entwickelt Tutorials im Bereich der Zeit- und Frequenzsynchronisation, wie NTP, PTP IEEE-1588 und viele mehr. Dieser Teil der LANTIME-Registerkarte „Dokumentation & Support“ enthält grundlegende Informationen über die Sync-Academy, gefolgt von einigen Links zu hilfreichen Informationen auf: https://www.meinberg.de/german/support/meinberg-sync-academy.htm

10.2 Monitoring über SNMP

10.2.1 Das Simple Network Managment Protocol

Die meisten vernetzten Geräte unterstützen eine Reihe von Verwaltungsoptionen, darunter das Simple Network Management Protocol (SNMP). SNMP ist ein Netzwerkprotokoll, das es einem einzelnen Netzwerkmanagementsystem ermöglicht, eine große Anzahl von Geräten im Netzwerk zu überwachen.

Die Funktionsweise ist, dass jedes Netzwerkelement einen „Agent“ hat, der mit dem Manager über SNMP kommuniziert. Jeder Agent verfügt über eine entsprechende „Management Information Base“, kurz MIB. Die MIBs organisieren Datenelemente in einer Baumstruktur. Es ist in einer standardisierten und strukturierten Sprache geschrieben, so dass die MIBs aller Geräte im Netzwerk im selben Manager vereint werden können.



MIB-Elemente werden als „Object Identifiers“ oder OIDs bezeichnet. Sie bestehen aus Konfigurationsvariablen, Statusvariablen, Baumstrukturbezeichnungen und Benachrichtigungen. Die OIDs können mit den Befehlen SNMP SET und GET gelesen oder geändert werden. Es gibt auch rekursive Befehle, mit denen der Manager nach allen OIDs in einem Zweig (Teilbaum) oder sogar dem gesamten Baum fragen kann. Dieser Prozess wird als „Walking the MIB“ bezeichnet. Ereignisbenachrichtigungen, allgemein als Traps bezeichnet, sind eine spezielle Art von OID. Ein Trap kann so konfiguriert werden, dass beim Statuswechsel des Geräts sofort eine Nachricht vom Agent an den Manager gesendet wird.

10.2.2 MIB Objekte eines LANTIME

Ein LTOS-Betriebssystem, das auf einem LANTIME-Servern läuft, unterstützt alle SNMP-Versionen (v1, v2c und v3) mit voller Funktionalität. Die properitären LANTIME-OIDs sind in Teilbäume gegliedert, die eine bestimmte Systemkomponente oder eine Betriebsart definieren. Der Hauptteilbaum mit den OIDs, die sich auf den LANTIME-Status verschiedener Modi beziehen, heißt „LantimeNGStatus“, NG steht für „Neue Generation der LANTIME-Features“ in der LANTIME-Firmware. Der „LantimeNGStatus“ besteht aus acht Teilbäumen, in denen Refclock, NTP, PTP, SystemHardware, Cluster und Misc die am wichtigsten zu überwachenden Teilbäume sind.

10.2.2.1 Refclock Subtree

Hier ist eine kurze Liste von OIDs aus dem Teilbaum NGStatus mit entsprechenden Beschreibungen:

mbgLtNgRefclockState
Diese OID beschreibt einen aktuellen Zustand einer LANTIME refclock (Hardware-Uhrenmodul), der sich auf GNSS oder ein anderes Zeitquellensignal im MRS (Multi Reference Source) Modell bezieht.

Status	Beschreibung
0:	*refclock is not available:* Siehe mögliche Fehlerbehebung: 1. Das Refclock-Modul kann nicht aufgerufen werden. 2. Überprüfen Sie, ob es beschädigt ist und ersetzen Sie es gegebenenfalls.
1:	*synchronized:* Die Referenzuhr Ihres Systems ist korrekt mit der ausgewählten Zeitquelle (GNSS oder MRS) synchronisiert. In einem MRS-System kann eine Refclock mit einer Referenzzeitquelle aus der Prioritätenliste synchronisiert werden. Siehe das Beispiel in der nächsten Abbildung. Das obige MRS-System synchronisiert sich zuerst mit GPS, aber wenn das GPS-Signal nicht verfügbar ist, wechselt die Referenzuhr zur nächsten Zeitquelle aus der Prioritätenliste (in unserem Fall PTP). Der Wechsel erfolgt erst nachdem eine „Trust-Time“ der nicht verfügbaren Zeitquelle (GPS-Signal) abgelaufen ist. Das soll verhindern, dass in zu kurzen Zeitperioden von einer Zeitquelle zur anderen gewechselt wird. Sobald GPS wieder verfügbar ist, schaltet die Uhr wieder auf GPS um, ohne auf den Ablauf der PTP-Trust-Tiem zu warten, weil die GPS-Referenz eine höhere Genauigkeit als PTP hat.
2:	*not synchronized:* Offensichtlich ist die refclock nicht mit ihrer Zeitquelle synchronisiert. Hier ist die mögliche Fehlerbehebung: A) Überprüfen Sie, ob die GPS-Antenne angeschlossen ist und die Referenzzeit empfangen wird. Mehr darüber, wie die Meinberg GPS-Antenne richtig zu montieren und zu positionieren ist, erfahren Sie hier. B) Wenn GPS die aktuelle Zeitquelle ist, überprüfen Sie die Anzahl der empfangenen Satelliten. Es sollte mindestens vier sein, um Synchronisationsinformationen bereitzustellen. C) Starten Sie „warm boot“, um die aktuelle Satellitenposition zu ermitteln. Dies ist besonders notwendig, wenn die physische Position Ihres LANTIME um mehr als 100 km von seiner Position verschoben wurde. Der vorherige Standort und die damit veralteten Satellitendaten werden weiterhin im System gespeichert. D) Starten Sie „cold boot“, um das Satelliten-Almanach zu aktualisieren. E) Wenn diese Maßnahmen nicht helfen, muss das GPS-Uhrenmodul ausgetauscht werden.

```
Es wird empfohlen, Ihre Netzwerkmanagement-Software so zu konfigurieren,
dass sie diesen Status regelmäßig, wenn möglich alle 60 Sekunden,
überprüft.
```

mbgLtNgRefclockLeapSecondDate
Diese OID übermittelt Informationen über das nächste Schaltsekundendatum. Wenn das bevorstehende Schaltsekundendatum noch nicht bekannt gegeben wurde, enthält die OID Informationen über das vorherige Schaltsekundenereignis.

Hier ist eine kurze Zusammenfassung der Schaltsekunden. Es gibt zwei verschiedene Zeitskalen, über die wir normalerweise in der Synchronisierungsumgebung sprechen: GPS - steht für Global Positioning System Time und UTC - steht für Universal Time Coordinated. UTC war früher bekannt als GMT (Greenwich Mean Time). Diese Zeitskalen unterscheiden sich voneinander durch die Anzahl der Schaltsekunden, die seit Beginn der GPS-Zeit am 6. Januar 1980 eingeführt wurden. Im Moment des Schreibens liegt das UTC 16 Sekunden hinter der GPS-Zeit. Das ist auf die ungleichmäßige Rotation der Erde zurückzuführen.

```
Da die Einführung einer neuen Schaltsekunde die Zeit im gesamten zu
synchronisierenden System beeinflusst, empfehlen wir, diesen Status
regelmäßig zu überprüfen, z.B. einmal pro Stunde.
```

Die nächsten in einer Reihe von OIDs sind diejenigen, die sich auf den NTP-Status beziehen. Sie befinden sich im Teilbaum „mbgLtNgNtp“.

10.2.2.2 NTP subtree

Hier ist eine kurze Liste von OIDs aus dem Teilbaum NGStatus mit entsprechenden Beschreibungen:

mbgLtNgNtpCurrentState
Eine der wichtigsten OIDs in diesem Teilbaum, die regelmäßig überprüft werden muss. Diese OID informiert über den NTP-Dienst Ihres LANTIME. Es sind drei Zustände möglich:

Status	Beschreibung

0: *not available:* Siehe die mögliche Fehlerbehebung:

A) Überprüfen Sie, ob der NTP-Dienst an einer bestimmten LAN-Schnittstelle tatsächlich aktiviert ist.

Um das zu überprüfen, melden Sie sich über das Webinterface an. Werkseitig voreingestellte Anmeldeinformationen: „root/timeserver“. Gehen Sie zum Menü: „Netzwerk → Netzwerkdienste“ und aktivieren Sie den Service der entsprechenden Schnittstelle (siehe Abbildung 3).

B) Überprüfen Sie, ob die Schnittstelle bzw. der Anschluss beschädigt ist und ersetzen Sie diesen gegebenenfalls.

1: *not synchronized:* Im Falle von „nicht synchronisiert“ ist der NTP-Dienst noch nicht auf einen Referenztakt synchronisiert. Mögliche Ursachen für diesen Zustand sind die folgenden:

A) Der NTP-Daemon befindet sich noch in der Initialisierungsphase, für die er ca. 3-5 Minuten benötigt. Warten Sie daher eine Weile, um zu sehen, ob sich hier der Status ändert.

B) Wenn eine Referenzuhr nicht synchronisiert wird, wird das im NTP-Status angezeigt. In diesem Fall wird der NTP-Daemon auf seine lokale Uhr synchronisiert und sein Stratumwert ändert sich auf 12. Bitte überprüfen Sie die mögliche Fehlerbehebung für einen Refclock-Status wie oben beschrieben.

2. *synchronized* : Der NTP-Dienst befindet sich im Normalbetrieb. Der LANTIME funktioniert nun einwandfrei.

```
Es wird empfohlen, den NTP-Status regelmäßig zu überprüfen,
jedoch nicht öfter als alle 64 s.
```

10.2.2.3 Hardware subtree

mbgLtNgSysPsStatus
Wenn ein LANTIME über ein redundantes Netzteil (RPS) verfügt, ist es wichtig, den Status beider RPS-Module regelmäßig zu überprüfen. Diese PowerSupplyStatus-OID befindet sich im Teilbaum System-Hardware. Die folgenden Zustände sind verfügbar:

Status	Beschreibung
0:	*notAvailable:* Das abgefragte Netzteil wird von einem System nicht erkannt. Überprüfen Sie, ob es beschädigt ist, und ersetzen Sie das Netzteil gegebenenfalls.
1:	*down:* Das abgefragte Netzteil ist nicht in Betrieb. Überprüfen Sie, ob es beschädigt ist, und ersetzen Sie das Netzteil gegebenenfalls.
2:	*up:* Das abgefragte Stromversorgungsmodul ist in Betrieb.

```
Es wird empfohlen, diese OID alle 60 s zu überprüfen.
```

10.2.2.4 Misc subtree

mbgLtNgEthPortLinkState
Im Teilbaum mbgLtNgMisc befindet sich eine „EthPortLinkState OID", die den Status jedes physikalischen Ethernet-Ports eines LANTIME identifiziert. Verfügbare Werte sind:

Status	Beschreibung
0:	*notAvailable:* Der abgefragte Port ist ausgefallen, überprüfen Sie die Link-LED. Bei einem Defekt ersetzen Sie die Netzwerkkarte.
1:	*up:* Der abgefragte Port befindet sich im Normalbetrieb.

```
Es wird empfohlen, diese OID alle 60 s zu überprüfen.
```

10.2.2.5 PTP subtree

Wenn Ihr LANTIME über eine IEEE 1588 PTPv2-Funktionalität verfügt, finden Sie die entsprechenden PTP-OIDs im Teilbaum „mbgLtNgPtp“. Hier sind die wichtigsten zu überwachenden OIDs:

mbgLtNgPtpPortState
Die folgenden PTP-Portzustände sind möglich:

Status	Beschreibung
0:	*uninitialized:* Der Port bootet, der Software-Daemon ist noch nicht gestartet, die IP-Adresse ist noch nicht vergeben.
1:	*initializing:* In diesem Zustand initialisiert der Port seine Datensätze, Hardware und Kommunikationseinrichtungen.
2:	*faulty:* Nicht in einem LANTIME definiert.
3:	*disabled:* Der PTP-Dienst wurde an diesem Port deaktiviert, entweder durch Benutzerkonfiguration oder weil sich das Modul im Standby-Modus befindet.
4:	*listening:* Der Port wartet darauf, dass der „announceReceiptTimeout“ abläuft oder dass er eine Announce-Nachricht von einem Master erhält.
5:	*preMaster:* Ein kurzer Übergangszustand, während der Port zum Master wird.
6:	*master:* Der Port ist ein aktueller Master.
7:	*passive:* Der Port befindet sich im passiven Modus, d.h. es ist eine weiterer Masterclock in der PTP-Domäne aktiv. Der Port kann in den Masterstatus wechseln, wenn er den BMCA aufgrund eines Ausfalls/Dienstabfalls des aktuellen Masters gewinnt.
8:	*uncalibrated:* Ein oder mehrere Master-Ports wurden in der Domäne erkannt.
9:	*slave:* Der Port hat sich erfolgreich bei einem Master angemeldet und empfängt alle erwarteten Nachrichten. Es wurde auch erfolgreich die Pfadverzögerung (Path Delay) mit Hilfe von „Delay Request Messages“ gemessen.

```
Es wird empfohlen, die PtpPortState OID alle 3 s zu überwachen.
```

10.2.3 SNMP Traps

SNMP Trap Name:	mbgLtNgTrapNTPNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.1
Schweregrad:	Warnung oder kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn NTP nicht synchron ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → NTP-Nachrichten → NTP Not Sync
Aufgehoben durch:	mbgLtNgTrapNTPSync

SNMP Trap Name:	mbgLtNgTrapNTPStopped
OID:	.1.3.6.1.4.1.5597.30.3.0.2
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn gestoppt ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → NTP-Nachrichten → NTP Stopped
Aufgehoben durch:	MbgLtNgTrapNTPSync or mbgLtNgTrapNTPNotSync

SNMP Trap Name:	mbgLtNgTrapServerBoot
OID:	.1.3.6.1.4.1.5597.30.3.0.3
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Zeitserver die Boot-Sequenz beendet hat
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapReceiverNotResponding
OID:	.1.3.6.1.4.1.5597.30.3.0.4
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der Empfänger nicht antwortet.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Rsponding
Aufgehoben durch:	MbgLtNgTrapReceiverNotSync or mbgLtNgTrapReceiverSync

SNMP Trap Name:	mbgLtNgTrapReceiverNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.5
Schweregrad:	Fehler
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der Empfänger nicht synchronisiert ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Sync
Aufgehoben durch:	mbgLtNgTrapReceiverSync

SNMP Trap Name:	mbgLtNgTrapAntennaFaulty
OID:	.1.3.6.1.4.1.5597.30.3.0.6
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, die gesendet werden soll, wenn die Verbindung zur Antenne unterbrochen ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Antenna Faulty
Aufgehoben durch:	mbgLtNgTrapAntennaReconnect

SNMP Trap Name:	mbgLtNgTrapAntennaReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.7
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn die Antenne wieder angeschlossen ist
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapConfigChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.8
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Zeitserver seine Konfiguration neu geladen hat.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapLeapSecondAnnounced
OID:	.1.3.6.1.4.1.5597.30.3.0.9
Schweregrad:	Info-Warnung
Kurzbeschreibung:	trap to be sent when a leap second has been announced
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Leap Second Announced Managm./Mon. → NTP → Leap Second Handling
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitError
OID:	.1.3.6.1.4.1.5597.30.3.0.10
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der bei Überschreitung des SHS-Zeitlimits gesendet wird
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → SHS Time Limit Warning Managm./Mon. → Webinterface → Einleitung LTOS 6 Managm./Mon. → Webinterface → Sicherheit → SHS Modus LTOS 6 Managm./Mon. → Webinterface → Sicherheit → SHS Time Limit
Aufgehoben durch:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotSync
OID:	.1.3.6.1.4.1.5597.30.3.0.11
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der sekundäre Empfänger nicht synchronisiert ist
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Sync
Aufgehoben durch:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapPowerSupplyFailure
OID:	.1.3.6.1.4.1.5597.30.3.0.12
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn eine der redundanten Stromversorgungen ausfällt.
Referenz zu anderen Kapitel:	Wichtige Sicherheitshinweise → Sicherheit bei der Installation Wichtige Sicherheitshinweise → Sicherheit im laufenden Betrieb
Aufgehoben durch:	mbgLtNgTrapPowerSupplyUp

SNMP Trap Name:	mbgLtNgTrapAntennaShortCircuit
OID:	.1.3.6.1.4.1.5597.30.3.0.13
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn eine angeschlossene Antenne aufgrund eines Kurzschlusses ausfällt.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Antenna Short Circuit
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapReceiverSync
OID:	.1.3.6.1.4.1.5597.30.3.0.14
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der bei synchronisiertem Empfänger gesendet wird
Referenz zu anderen Kapitel:	Antennen- und Empfängerinformationen → Referenzzeitquellen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPClientAlarm
OID:	.1.3.6.1.4.1.5597.30.3.0.15
Schweregrad:	Error
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein NTP Client Monitoring Alarm auftritt, z.B. wenn ein überwachter Client nicht erreichbar ist.
Referenz zu anderen Kapitel:	Überprüfen Sie die Netzwerkkonfiguration unter Managm./Mon. → Netzwerk
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPowerSupplyUp
OID:	.1.3.6.1.4.1.5597.30.3.0.16
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Netzteil wieder in einen korrekten Zustand versetzt wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNetworkDown
OID:	.1.3.6.1.4.1.5597.30.3.0.17
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn ein überwachter Netzwerk-Port ausgefallen ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Netzwerk-Nachrichten → Network Link Down
Aufgehoben durch:	mbgLtNgTrapNetworkUp

SNMP Trap Name:	mbgLtNgTrapNetworkUp
OID:	.1.3.6.1.4.1.5597.30.3.0.18
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn ein überwachtes Netzwerk-Port aktiv ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSecondaryRecNotRespp
OID:	.1.3.6.1.4.1.5597.30.3.0.19
Schweregrad:	Warnung oder kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn der sekundäre Empfänger nicht antwortet.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → CLK Not Responding
Aufgehoben durch:	mbgLtNgTrapSecondaryRecSync

SNMP Trap Name:	mbgLtNgTrapMrsLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.30
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Referenzoffset den konfigurierten Grenzwert überschreitet.
Referenz zu anderen Kapitel:	LTOS 6 Managm./Mon. → Webinterface → Clock → MRS Settings Troubleshooting und Alarmierungen → Referenzuhr → MRS Limit Exceed
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapMrsRefDisconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.31
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Referenzsignal verloren gegangen ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → MRS Reference Disconnected
Aufgehoben durch:	mbgLtNgTrapMRSRefReconnect

SNMP Trap Name:	mbgLtNgTrapMRSRefReconnect
OID:	.1.3.6.1.4.1.5597.30.3.0.32
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein Referenzsignal wiederhergestellt wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapFdmError
OID:	.1.3.6.1.4.1.5597.30.3.0.33
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein FDM-Modul einen Alarm erzeugt.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → FDM → FDM Konfiguration
Aufgehoben durch:	mbgLtNgTrapFDMOk

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitWarning
OID:	.1.3.6.1.4.1.5597.30.3.0.34
Schweregrad:	Warnung, kritisch
Kurzbeschreibung:	Trap, der bei Überschreitung der SHS-Warngrenze gesendet wird.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Einleitung Managm./Mon. → Webinterface → Security → SHS Konfiguration Managm./Mon. → Webinterface → Security → SHS Modus Troubleshooting und Alarmierungen → Referenzuhr → SHS Time Limit Warning
Aufgehoben durch:	mbgLtNgTrapSHSTimeLimitOk

SNMP Trap Name:	mbgLtNgTrapSecondaryRecSync
OID:	.1.3.6.1.4.1.5597.30.3.0.35
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der sekundäre Empfänger synchronisiert ist.
Referenz zu anderen Kapitel:	Antennen- und Empfänger-Information → Referenzzeitquellen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPSync
OID:	.1.3.6.1.4.1.5597.30.3.0.36
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn NTP synchronisiert wird
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPtpPortDisconnected
OID:	.1.3.6.1.4.1.5597.30.3.0.37
Schweregrad:	Warnung oder kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn der PTP-Netzwerkanschluss getrennt wurde.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → PTP → PTP Globaler Status
Aufgehoben durch:	mbgLtNgTrapPtpPortConnected

SNMP Trap Name:	mbgLtNgTrapPtpPortConnected
OID:	.1.3.6.1.4.1.5597.30.3.0.38
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der PTP-Netzwerkanschluss verbunden wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPtpStateChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.39
Schweregrad:	Info-Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn sich der PTP-Zustand geändert hat (z.B. von „passiv“ auf „Master“).
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → PTP → PTP Globaler Status
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPtpError
OID:	.1.3.6.1.4.1.5597.30.3.0.40
Schweregrad:	Warnung, kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn PTP einen Fehler ausgelöst hat.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → PTP → PTP Globaler Status
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapLowSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.41
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System mit geringen Ressourcen läuft.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapSufficientSystemResources

SNMP Trap Name:	mbgLtNgTrapFanDown
OID:	.1.3.6.1.4.1.5597.30.3.0.45
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Lüfter ausfällt.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Sonstige Meldungen → Fan Failure
Aufgehoben durch:	mbgLtNgTrapFanUp

SNMP Trap Name:	mbgLtNgTrapFanUp
OID:	.1.3.6.1.4.1.5597.30.3.0.46
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Lüfter hochfährt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapCertificateExpired
OID:	.1.3.6.1.4.1.5597.30.3.0.47
Schweregrad:	Info oder Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn das HTTPS-Zertifikat abläuft oder ablaufen wird.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Sicherheit → HTTPS-Zertifikat
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSufficientSystemResources
OID:	.1.3.6.1.4.1.5597.30.3.0.48
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System wieder genügend Ressourcen erhalten hat.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.49
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Oszillator aufgewärmt ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapOscillatorNotWarmedUp
OID:	.1.3.6.1.4.1.5597.30.3.0.50
Schweregrad:	Information
Kurzbeschreibung:	Trap, der gesendet werden soll, wenn der Oszillator nicht aufgewärmt ist.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Referenzuhr → Oscillator not Adjusted
Aufgehoben durch:	mbgLtNgTrapOscillatorWarmedUp

SNMP Trap Name:	mbgLtNgTrapMRSRefChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.51
Schweregrad:	Info-Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn die MRS-Referenzquelle geändert wurde.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapClusterMasterChanged
OID:	.1.3.6.1.4.1.5597.30.3.0.52
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn der Cluster-Modus aktiv ist und der Cluster geändert wurde.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Netzwerk → Netzwerkschnittstellen → Cluster
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerDetected
OID:	.1.3.6.1.4.1.5597.30.3.0.53
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der bei aktivem Cluster-Modus gesendet werden soll, und ein Cluster-Mitglied wird als Falseticker erkannt.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Netzwerk → Netzwerkschnittstellen - Cluster
Aufgehoben durch:	mbgLtNgTrapClusterFalsetickerCleared

SNMP Trap Name:	mbgLtNgTrapClusterFalsetickerCleared
OID:	.1.3.6.1.4.1.5597.30.3.0.54
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der bei aktivem Cluster-Modus gesendet werden soll, und ein Clustermitglied ist kein Falseticker mehr.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapSHSTimeLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.55
Schweregrad:	Information
Kurzbeschreibung:	Trap, der gesendet wird, wenn der SHS-Zeitlimitfehler bestätigt wurde. oder die Zeitdifferenz fällt unter den Warngrenzwert.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → Einleitung
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapIMSError
OID:	.1.3.6.1.4.1.5597.30.3.0.56
Schweregrad:	Kritisch
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein IMS-Modul nicht mehr reagiert - hat Temperaturprobleme, etc.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → Sonstige Meldungen → IMS Error
Aufgehoben durch:	mbgLtNgTrapIMSOk

SNMP Trap Name:	mbgLtNgTrapIMSOk
OID:	.1.3.6.1.4.1.5597.30.3.0.57
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein IMS-Modul in einen normalen Zustand zurückkehrt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapFDMOk
OID:	.1.3.6.1.4.1.5597.30.3.0.58
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn ein FDM-Modul in einen normalen Zustand zurückkehrt.
Referenz zu anderen Kapitel:	Managm./Mon. → Webinterface → FDM → FDM Konfiguration
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.59
Schweregrad:	Error
Kurzbeschreibung:	Trap, der bei der Überwachung eines NTP-Clients und seiner Umgebung gesendet wird. Offset-Grenze wird überschritten.
Referenz zu anderen Kapitel:	Troubleshooting und Alarmierungen → NTP-Nachrichten → NTP Offset Limit Exceeded
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNTPOffsetLimitOk
OID:	.1.3.6.1.4.1.5597.30.3.0.60
Schweregrad:	Info
Kurzbeschreibung:	Trap, der bei der Überwachung eines NTP-Clients und seiner Umgebung gesendet wird. Offset-Grenze ist wieder in einem gültigen Bereich.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapNTPOffsetLimitExceeded

SNMP Trap Name:	mbgLtNgTrapXheRubOk
OID:	.1.3.6.1.4.1.5597.30.3.0.61
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn externes Rubidium OK meldet.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapXheRubError
OID:	.1.3.6.1.4.1.5597.30.3.0.62
Schweregrad:	Error
Kurzbeschreibung:	Trap, der gesendet wird, wenn externes Rubidium einen Fehler meldet.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapXheRubOk

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionExceeded
OID:	.1.3.6.1.4.1.5597.30.3.0.63
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System zu viel Strom verbraucht.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapPowerConsumptionOk

SNMP Trap Name:	mbgLtNgTrapPowerConsumptionOk
OID:	.1.3.6.1.4.1.5597.30.3.0.64
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System über ausreichend Strom verfügt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyNotAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.65
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn kein Backup der Stromversorgung verfügbar ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapPowerRedundancyAvail

SNMP Trap Name:	mbgLtNgTrapPowerRedundancyAvail
OID:	.1.3.6.1.4.1.5597.30.3.0.66
Schweregrad:	Info
Kurzbeschreibung:	Trap, der gesendet wird, wenn mindestens eine Stromnetzteil als Backup vorhanden ist.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapTrustedSourceError
OID:	.1.3.6.1.4.1.5597.30.3.0.67
Schweregrad:	Warnung
Kurzbeschreibung:	Trap, der gesendet wird, wenn die Zeitabweichung einer MRS-Quelle die konfigurierte Grenze überschreitet.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	mbgLtNgTrapTrustedSourceOk

SNMP Trap Name:	mbgLtNgTrapTrustedSourceOk
OID:	.1.3.6.1.4.1.5597.30.3.0.68
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn die Zeitabweichung einer MRS-Quelle zu ihrer konfigurierten Grenze zurückkehrt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapNormalOperation
OID:	.1.3.6.1.4.1.5597.30.3.0.77
Schweregrad:	Clearing-Ereignis
Kurzbeschreibung:	Trap, der gesendet wird, wenn das System in den Normalbetrieb zurückkehrt.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapHeartbeat
OID:	.1.3.6.1.4.1.5597.30.3.0.88
Schweregrad:	Information
Kurzbeschreibung:	Trap, der regelmäßig gesendet wird, um anzuzeigen, dass der Zeitserver noch arbeitet.
Referenz zu anderen Kapitel:	Managm./Mon. → Benachrichtigung → Verschiedenes - Heartbeat aktivieren
Aufgehoben durch:	-

SNMP Trap Name:	mbgLtNgTrapTestNotification
OID:	.1.3.6.1.4.1.5597.30.3.0.99
Schweregrad:	Information
Kurzbeschreibung:	Trap, der gesendet wird, wenn eine Testbenachrichtigung angefordert wird.
Referenz zu anderen Kapitel:	keine weiteren Informationen
Aufgehoben durch:	-

11 Troubleshooting und Alarmierungen

11.1 NTP-Nachrichten

Fehler- und Systemmeldung / Beschreibung	Troubleshooting / Zusatzinformationen
NTP Not Sync / Der NTP-Dienst eines LANTIME ist nicht synchronisiert.	• Für LANTIMEs mit eingebauter Referenzuhr überprüfen Sie bitte den Status der Uhr auf der Startseite im Webinterface. Wenn der Referenztakt nicht synchronisiert ist, lesen Sie bitte die Fehlerbehebungsinformationen für „CLK Not Sync“. • Bei LANTIMEs, die von externen NTP-Servern synchronisiert werden sollen, ist darauf zu achten, dass die externen NTP-Server erreichbar sind. • Überprüfen Sie für MRS-Geräte, ob MRS-Referenzzeitquellen im Web-Interface konfiguriert sind („Das Webinterface → Uhr → MRS-Einstellungen) und entsprechende Signale verfügbar sind (“Das Webinterface → Uhr → MRS-Status)". • Wenden Sie sich an Ihren Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.
NTP Stopped / Der NTP-Dienst wurde angehalten	• Hinweis: Nach jeder für den NTP relevanten Konfigurationsänderung wird der NTP-Dienst gestoppt und neu gestartet. In diesem Fall wird eine Meldung ‘NTP Stopped‘ in das Systemprotokoll des LANTIME geschrieben. • Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn „NTP Stopped“ dauerhaft als NTP-Status auf der Frontplatte oder im Webinterface angezeigt wird.

NTP Offset Limit Exceeded
LANTIMEs erzeugen diese Meldung, wenn der interne Zeitversatz zwischen LANTIME-Systemzeit und Referenztakt größer als der konfigurierte Schwellenwert ist.

- Überprüfen Sie den konfigurierten Schwellenwert im Web Interface: „NTP → Spezielle Einstellungen → Max. Interner Offset (ms.)“.
- Hinweis: Nach dem Neustart des LANTIME dauert es je nach Referenzzeitquelle mehrere Minuten, bis der interne Offset $< \pm 1$ ms ist.
- Wenden Sie sich an Ihren Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

11.2 Referenzuhr-Nachrichten

Fehler- und Systemmeldung / Beschreibung	Fehlerbehebung / Zusatzinformationen
CLK Not Responding / Der LANTIME kann nicht mehr mit seiner internen Referenzuhr kommunizieren.	• Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.
CLK Not Sync / Leistungs- und Systemressourcen-problem des NTP	LANTIME mit GNSS-Referenzuhr (GPS/GLN/GNS): • Überprüfen Sie die Antennenposition: • Wenn der GPS-Referenztaktgeber an einen GPS-Antennenverteiler GPSAV4 (https://www.meinberg.de/german/products/gps-antennenverteiler.htm) angeschlossen ist, stellen Sie sicher, dass der Port „Clock 1“ des GPSAV4 angeschlossen ist, da der GPSAV4 und die Antenne über diesen Port mit Strom versorgt werden. LANTIME mit Langwellenempfänger (DCF77-PZF/WWVB/MSF/JJY): • Überprüfen Sie die Antennenposition LANTIME mit TCR-Referenztakt (IRIG): • Überprüfen Sie, ob der Timecode-Eingangsport auf der Rückseite des LANTIME korrekt mit einer IRIG-Quelle verbunden ist. Überprüfen Sie im Webinterface, ob der richtige IRIG-Eingabecode konfiguriert ist (Menü „Uhr → IRIG-Einstellungen → Timecode-Eingang“). Der Eingangs-Zeitcode ist der IRIG-Code, der dem LANTIME von der IRIG-Quelle zur Verfügung gestellt wird. • Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Antenna Faulty /
GNSS-Referenzuhr (GPS/GLN/GNS):
Die Antenne wurde nicht erkannt.

- Überprüfen Sie die Verbindungen zwischen der Antenne und einem LANTIME.
- Überprüfen Sie die Ausgangsspannung am LANTIME-Antennenanschluss.
- Trennen Sie dazu das Antennenkabel vom LANTIME-Antennenanschluss. Der folgende Spannungswert sollte
- zwischen Innen- und Außenleiter gemessen werden:
  - GPS-Empfänger → 15-18 V DC
  - GLN-Empfänger → 5 V DC
  - GNS-Empfänger → 5 V DC
- Wenn die Spannung 0 V DC beträgt, wenden Sie sich bitte an den Technischen Support von Meinberg.
- Wenn die gemessene Spannung am Antennenanschluss des LANTIME korrekt ist, schließen Sie das Antennenkabel wieder an und überprüfen Sie die Spannung am anderen Ende des Kabels.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Langwellenempfänger (DCF77-PZF/WWVB/MSF/JJY):
Entweder die Antenne oder ein anderes Eingangssignal wurde nicht erkannt.

- Überprüfen Sie die Verbindungen zwischen der Antenne und einem LANTIME.
- Überprüfen Sie den Status des empfangenen Antennensignals auf der Hauptseite im Webinterface. Der angezeigte Feldstärkewert sollte > 40 sein. Ist das nicht der Fall, überprüfen Sie bitte, wie die Antenne positioniert ist.
- Überprüfen Sie die Ausgangsspannung am LANTIME-Antennenanschluss.
- Trennen Sie dazu das Antennenkabel vom LANTIME-Antennenanschluss. Der folgende Spannungswert sollte zwischen Innen- und Außenleiter gemessen werden: Langwellenempfänger →] 5 V DC.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Antenna Short Circuit
Kurzschluss an der Antennenleitung.

- Trennen Sie das Antennenkabel vom LANTIME-Antennenanschluss.
- Durchführen eines Neustarts des Systems
- Wenn der LANTIME nach der Inbetriebnahme die Fehlermeldung nicht anzeigt, schließen Sie die Antenne wieder an. Andernfalls wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.

GPS Warm Boot
Im Warm-Boot-Modus führt die GPS-Referenzuhr die Positionsbestimmung durch. Um diesen Prozess erfolgreich abzuschließen, sollten mindestens 4 Satelliten empfangen werden. Nach erfolgreicher Positionsbestimmung wird die Position im batteriegepufferten Speicher der Uhr gesichert. Damit soll die Positionsbestimmung nach einem Neustart nicht erneut durchgeführt werden müssen.

- Wenn der LANTIME den GPS-Warmstartvorgang nicht abschließen kann, überprüfen Sie die Anzahl der „Guten Satelliten“, die im Webinterface angezeigt werden: „Menü Uhr → GPS (GNSS-Uhr) → Empfängerinformationen → Anzahl der guten Satelliten“.
- Wenn die Anzahl der guten Satelliten dauerhaft unter 4 liegt und der LANTIME die Positionsbestimmung nicht abschließen kann, dann lesen Sie den Fehlerbehebungsfall für „CLK Not Sync“.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

GPS Cold Boot
Im GPS Cold Boot-Modus versucht die GPS-Referenzuhr, das GPS-Almanach herunterzuladen, welches die Satellitenbahndaten für alle Satelliten enthält. Um diesen Prozess abzuschließen, sollte mindestens ein Satellit empfangen werden. Der Prozess dauert mindestens 12 Minuten. Nachdem der Kaltstart abgeschlossen ist, schaltet die Uhr automatisch auf den GPS-Warm-Boot um, um die Position zu bestimmen.

Das GPS-Almanach wird im batteriegepufferten Speicher der Uhr gesichert.

- Wenn der LANTIME den GPS Cold Boot-Betrieb nach mehr als 30 Minuten nicht abschließen kann, überprüfen Sie die Anzahl der „guten Satelliten“ im Webinterface-Menü: „Uhr → GPS (GNSS-Uhr → Empfängerinformationen → Anzahl der guten Satelliten“.
- Wenn die Anzahl der guten Satelliten 0 ist, lesen Sie bitte den Fehlerbehebungsfall für „CLK Not Sync“.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

SHS Time Limit Warning
LANTIME-Systeme mit zwei eingebauten Referenzuhren senden diese Meldung, sobald die Zeitdifferenz zwischen beiden Uhren die vorkonfigurierte Einstellung „Time Limit Warning Level“ überschreitet.

- Überprüfen Sie die aktuelle Zeitdifferenz zwischen den beiden Referenzuhren im Hauptmenü des Webinterfaces.
- Überprüfen Sie Ihre SHS-Konfiguration unter „Sicherheit → SHS-Konfiguration“. Sind die konfigurierten Schwellenwerte möglicherweise zu streng eingestellt?
- Überprüfen Sie den Status der beiden Referenzuhren im Hauptmenü des Webinterfaces. Wenn eine der beiden Uhren nicht synchronisiert ist, lesen Sie bitte den Fehlerbehebungsfall für „CLK Not Sync“.
- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Oscillator not Adjusted
Der interne Oszillator ist (noch) nicht vollständig diszipliniert. Sobald dieser Vorgang abgeschlossen ist, sendet der LANTIME eine Logmeldung „Oscillator Adjusted“. Die Zeit, die benötigt wird, um einen Oszillator zu disziplinieren, hängt von der Qualität des eingehenden Signals, der Alterung und den Umwelteinflüssen auf den Oszillator ab.

- Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Leap Second Announced
LANTIME-Server mit GNSS-Referenztaktgeber (GPS / GLN / GNS) oder Langwellenempfänger (DCF77-PZF / WWVB / MSF / JJY) senden die Schaltsekunden-Benachrichtigungsmeldung „Leap Second Announced“, sobald sie die Durchsage durch das Referenzsignal erhalten haben. Die GPS-Satelliten kündigen die bevorstehende Schaltsekunde in der Regel etwa ein halbes Jahr im Voraus an. Langwellensender senden die Ansage in der Regel 1 Stunde im Voraus.

- Dies ist nur eine Info-Benachrichtigung, daher ist keine weitere Aktion erforderlich.

XMR Limit Exceed
LANTIME erzeugt diese Meldung, wenn der gemessene Zeitversatz einer MRS-Zeitquelle den konfigurierten Schwellenwert überschritten hat.

- Überprüfen Sie den aktuellen MRS-Zeitquellenstatus im Web-Interface unter „Uhr → GNSS-Uhr → MRS-Status".
- Überprüfen Sie die MRS-Konfiguration im Web-Interface unter „Uhr → GNSS-Uhr → MRS-Einstellungen". Sind die konfigurierten Schwellenwerte (Spalte „Limit" ankreuzen) möglicherweise zu streng konfiguriert?
- Wenden Sie sich an Ihren Meinberg TechSupport und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

XMR Reference Disconnected
LANTIME erzeugt diese Meldung, wenn die konfigurierte MRS-Zeitquelle nicht mehr verfügbar ist.

- Wenden Sie sich an Ihren Meinberg TechSupport und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

11.3 Netzwerk-Meldungen

Fehler- und Systemmeldung / Beschreibung	Troubleshooting / Zusatzinformationen
Network Link Down / Es wurde keine Verbindung an einer Netzwerkschnittstellen des LANTIME erkannt.	• Überprüfen Sie, welche Ports physisch verbunden sind und ob der Link verfügbar sein sollte. • Überprüfen Sie, ob die Netzwerkeinstellungen am Switch und am LANTIME kompatibel sind. • Überprüfen Sie die Einstellungen zur Linküberwachung über das Web-Interface: „Netzwerk → Physikalische Netzwerkkonfiguration → Zeige Linkstatus an Front LED". – Der LANTIME überwacht einen Verbindungsstatus für die Ports, bei denen die Option „Zeige Linkstatus an Front LED" aktiviert ist. • Wenden Sie sich an den Technischen Support von Meinberg und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

11.4 Sonstige Meldungen

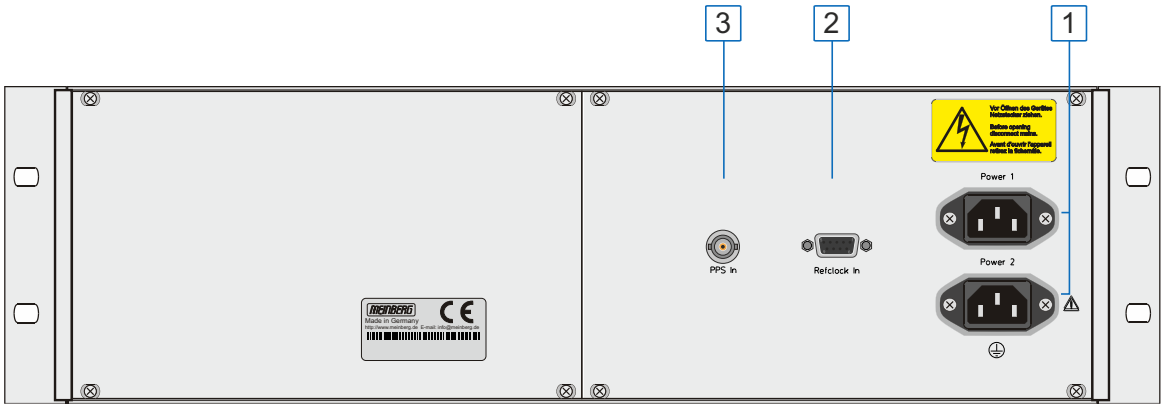
Fehler- und Systemmeldung / Beschreibung>	Troubleshooting / Zusatzinformationen
Fan Failure / Der LANTIME hat einen Fehler an einem Lüftermodul erkannt oder ein Lüftermodul wurde während des Systembetriebs entfernt.	• Wenn das Lüftermodul nicht bewusst entfernt wurde, wenden Sie sich an den Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.
IMS Error / Entweder hat der LANTIME einen Fehler an einem IMS-Modul erkannt oder ein IMS-Modul wurde während des Betriebs aus dem LANTIME IMS-System entfernt.	**Troubleshooting / Zusatzinformationen** • Wenn das IMS-Modul nicht bewusst entfernt wurde, wenden Sie sich an den Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung.
CPU No Response (Diese Fehlermeldung kann nur auf einem Display erscheinen) / Das Display erhält keine Informationen von der installierten LANTIME CPU-Einheit.	**Troubleshooting / Zusatzinformationen** • Überprüfen Sie, ob der LANTIME noch über das Netzwerk erreichbar ist (Ping, SSH, HTTP / HTTPS). • Löst ein System-Neustart dieses Problem (kurz von der Spannungszufuhr trennen)? • Wenn der LANTIME noch über HTTP / HTTPS erreichbar ist, laden Sie bitte eine Diagnosedatei über das Webinterface herunter und senden Sie diese an den Technischen Support von Meinberg. Wenn keine Verbindung zum LANTIME möglich ist, wenden Sie sich an unseren Support mit der Seriennummer Ihres LANTIME.
Certificate Expired / Ein LANTIME erzeugt diese Warnung 60 Tage, 30 Tage und 15 Tage vor dem Ende der Laufzeit des installierten SSL-Zertifikats für den HTTPS-Dienst.	**Troubleshooting / Zusatzinformationen** • Überprüfen Sie die Gültigkeit des installierten SSL-Zertifikats über das Web-Interface: „Sicherheit → HTTPS-Zertifikat → SSL-Zertifikat anzeigen“. • Laden Sie ein neues SSL-Zertifikat über das LANTIME Webinterface im Dialogfeld „Sicherheit → HTTPS Zertifikat → Upload SSL-Zertifikat“ hoch. • Wenden Sie sich an Ihren Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

Low System Resource /
Ein LANTIME erzeugt diese Warnung:
Verzeichnis „/var“ <] 1MB frei
Verzeichnis „/var“ >] 90% Nutzung
RAM Speicher frei < 6MB

Troubleshooting / Additional information

- Wenden Sie sich an Ihren Meinberg-Support und stellen Sie eine LANTIME-Diagnosedatei zur Verfügung, wenn Sie weitere Hilfe bei der Problemlösung benötigen.

12 Anhang: Technische Daten



ENGLISH

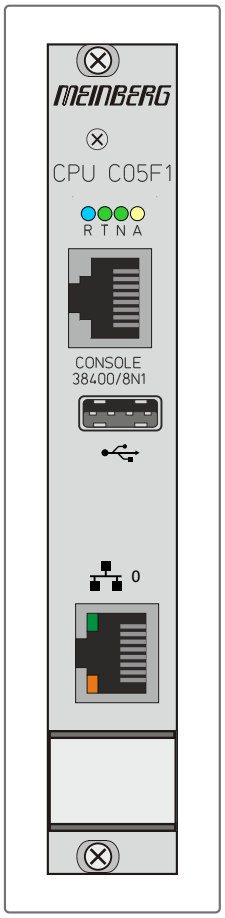
1. Power supply connector
2. Refclock Input, DSUB-9 conncetor
3. PPS Input, BNC female

DEUTSCH

1. Spannungsversorgung
2. Refclock Eingang, DSUB-9 Anschluss
3. PPS Eingang, BNC Buchse

12.1 LAN-CPU Zeitserver-Modul

Die Baugruppe LAN-CPU ist ein kompletter Einplatinenrechner mit LINUX Betriebssystem und vorinstalliertem NTP Server. Die Baugruppe kann in verschiedene GNSS-, DCF77, WWVB, MSF oder IRIG-Systeme von Meinberg integriert werden, um diese zu einem NTP Stratum 1 Server zu erweitern.

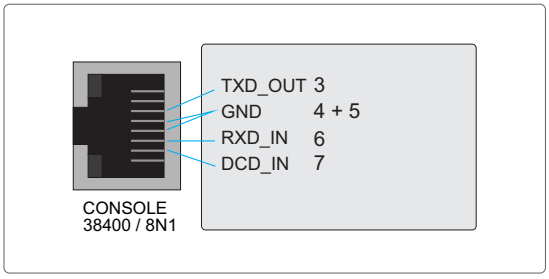


Das System lässt vielfältige Management- und Konfigurationsmethoden zu, die aus Gründen der Sicherheit einzeln aktiviert/deaktiviert werden können: Web-Oberfläche (HTTP/HTTPS), textbasierendes Setupprogramm (TELNET/SSH) und SNMP. Firmware-Updates können bequem über das Web-Interface durchgeführt werden.

Technische Daten LAN CPU

CPU Modul-Typ:	C05F1
Prozessor:	Geode™ LX800 mit 500 MHz
Hauptspeicher:	256 MB
Cachespeicher:	16 KB 2nd Level Cache
Flashdisk:	1 GB
Signal:	100BASE-T
Datenübertragungs-rate:	10/100 Mbit/s
Verbindungstyp:	8P8C (RJ45)
Kabel:	Kupfer Twisted Pair, z.B. CAT 5.0
Duplex Modi:	Half/Full/Autonegotiaton

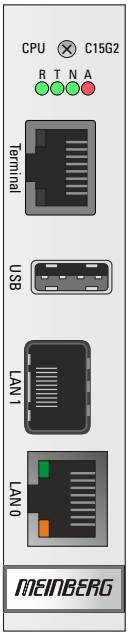
RJ45 Schnittstelle zum Anschluss eines seriellen Terminals. Diese Schnittstelle dient zur Konfiguration von einem CAB-CONSOLE-RJ45 Kabel angeschlossenen PC mittels eines Terminal Programmes. Die Einstellungen für die Schnittstelle auf dem PC müssen auf 38400 Baud, 8 Datenbits, keine Parität und ein Stopbit (8N1) eingestellt werden. Die Terminal Emulation muss auf VT100 gesetzt werden. Nach dem Herstellen der Verbindung sollte die Eingabeaufforderung für die Benutzerkennung angezeigt werden (evtl. noch einmal RETURN drücken:



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

12.2 Technische Daten - IMS CPU-C15G2

Als zentrales Management- und Bedienelement ist das CPU-Modul in einem LANTIME-System für Management, Überwachung, Konfiguration und Alarmmeldungen zuständig. Es bietet zusätzlich NTP- und SNTP-Dienste auf seinen Netzwerkschnittstellen. Das CPU-Modell C15G2 ist mit zwei integrierten Netzwerk-Schnittstellen ausgerüstet, zusätzliche Netzwerk-Ports können durch die Installation von LNE-Modulen hinzugefügt werden.



Prozessor: Intel® Atom™ Processor E Series
(2 Cores, 1.33GHz, TDP 3W)

Hauptspeicher: onboard 2 GB

Cache-Speicher: 1MB 2nd Level Cache

Flashdisk: 4 GB

Netzwerk-anbindung:
1 x 10/100/1000 Base-T mit RJ45-Anschluss
1 x 1000Base-T mit SFP-Anschluss

Serielle Schnittstelle:
RJ45 Anschluss
Konsole: 38400 / 8N1,
Anschluss über CAB-CONSOLE Kabel

USB Port:
Aufspielen von Firmware-Updates
Backup und Sichern von Konfigurationsdateien
Kopieren von Sicherheitsschlüsseln
Sperren / Entsperren von Funktionstastatur

Betriebssystem: GNU/Linux 4.x

Statusanzeige:

LAN 0 Interface
LED - Connect, Activity und Speed der Netzwerkverbindung

LAN-CPU
R - Reference Time
T - Time Service
N - Network
A - Alarm

Unterstützte Protokolle:

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)

Umgebung:

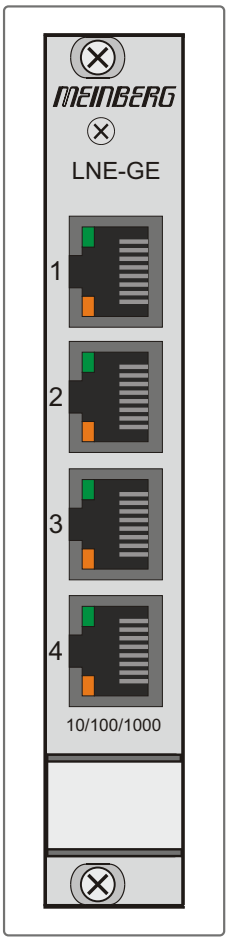
Umgebungstemperatur:	0 ... 50°C
Luftfeuchtigkeit:	Max. 85%

12.3 LNE-GbE: Zusätzliche Ethernet-Schnittstellen

LANTIME Netzwerk Erweiterung LNE, zusätzliche Netzwerkschnittstellen für LANTIME Zeitserver mit Gigabit Unterstützung.

Systembeschreibung

Die Baugruppe LNE-GbE dient zur Erweiterung des LANTIME NTP-Servers um vier zusätzliche Netzwerkverbindungen. Somit stehen die Standardfunktionen des LANTIME weiteren autarken Netzwerken zur Verfügung.



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

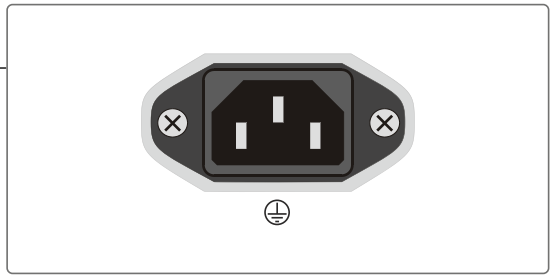
Ausgangssignal	1000BASE-T
Datenübertragungsrate	10/100/1000 Mbit/s
Anschlusstyp:	8P8C (RJ45)
Kabel:	Kupfer Twisted Pair, z.B. CAT 5.0

Es stehen 7 Modis zur Verfügung:
- Autosensing
- 10 MBit/Halb-Duplex
- 100 MBit/Halb-Duplex
- 1000 MBit/Halb-Duplex (Gigabit Support)
- 10 MBit/Voll-Duplex
- 100 MBit/Voll-Duplex
- 1000 MBit/Voll-Duplex (Gigabit Support)

Die Konfiguration kann über das Display-Menü und/oder über das Web-Interface durchgeführt werden.

12.4 Anschluss Spannungsversorgung

Verbindungstyp: Kaltgerätestecker



Eingangsparameter

Nennspannungsbereich:	U_N	=	100-240 V~
	U_N	=	100-200 V ⎓
Max. Spannungsbereich:	U_{max}	=	90-265 V~
	U_{max}	=	90-250 V ⎓
Nennstrom:	I_N	=	0,5 A
Nennfrequenzbereich:	f_N	=	50-60 Hz
Max. Frequenzbereich:	f_{max}	=	47-63 Hz

Ausgangsparameter

Max. Leistung:	P_{max}	=	50 W
Max. Wärmeabgabe:	E_{therm}	=	180,00 kJ/h (170,61 BTU/h)

WARNUNG!
Dieses Gerät wird an einer gefährlichen Spannung betrieben.

Lebensgefahr durch elektrischen Schlag!

- Nur Fachpersonal (Elektriker) darf das Gerät anschließen.
- Arbeiten an geöffneten Klemmen und Steckern dürfen niemals bei anliegender Spannung durchgeführt werden.
- Alle Steckverbinder müssen mit einem geeigneten Steckergehäuse gegen Berührung spannungsführender Teile geschützt werden!

- Hinweis: Achten Sie immer auf eine sichere Verdrahtung!

- Wichtig: Das Gerät muss an eine ordnungsgemäße Erdung (PE) angeschlossen werden

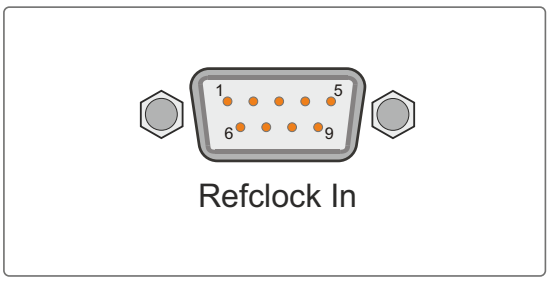
12.5 Refclock In

Signal: Referenz, RS-232

Verbindungstyp: D-SUB Stecker 9pol.

Kabel: Datenkabel (geschirmt)

Belegung:
Pin 1: PPS (optional)
Pin 2: RxD
Pin 5: GND

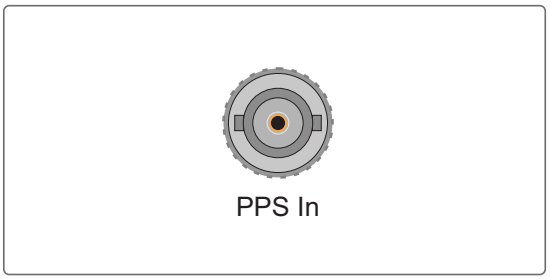


12.6 PPS In

Kabel: Koaxialkabel, geschirmt

Impulslänge: >= 5μs, active high

Verbindungstyp: BNC-Buchse



13 Appendix

13.1 Zeittelegramme

13.1.1 Format des Meinberg Standard Telegramms

Das Meinberg Standard Telegramm besteht aus einer Folge von 32 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Das Format ist:

<STX>D:*tt.mm.jj;T:w;U:hh.mm.ss;uvxy*<ETX>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-Of-Text, ASCII Code 02h wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet

tt.mm.jj	das Datum:		
	tt	Monatstag	(01..31)
	mm	Monat	(01..12)
	jj	Jahr ohne Jahrhundert	(00..99)
w	der Wochentag		(1..7, 1 = Montag)
hh.mm.ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)

uv Status der Funkuhr: (abhängig vom Funkuhrentyp)

u:	'#'	GPS: Uhr läuft frei (ohne genaue Zeitsynchronisation) PZF: Zeitraster nicht synchronisiert DCF77: Uhr hat seit dem Einschalten nicht synchr.
	"	(Leerzeichen, 20h) GPS: Uhr läuft GPS synchron (Grundgenauig. erreicht) PZF: Zeitraster synchronisiert DCF77: Synchr. nach letztem Einschalten erfolgt
v:	'*'	GPS: Empfänger hat die Position noch nicht überprüft PZF/DCF77: Uhr läuft im Moment auf Quarzbasis
	' '	(Leerzeichen, 20h) GPS: Empfänger hat seine Position bestimmt PZF/DCF77: Uhr wird vom Sender geführt

x Kennzeichen der Zeitzone:

'U'	UTC	Universal Time Coordinated, früher GMT
' '	MEZ	Mitteleuropäische Standardzeit
'S'	MESZ	Mitteleuropäische Sommerzeit

y Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:

'!'	Ankündigung Beginn oder Ende der Sommerzeit
'A'	Ankündigung einer Schaltsekunde
' '	(Leerzeichen, 20h) kein Zeitsprung angekündigt

<ETX> End-Of-Text, ASCII Code 03h

13.1.2 Format des Meinberg GPS Zeittelegramms

Das Meinberg GPS Zeittelegramm besteht aus einer Folge von 36 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Es enthält im Gegensatz zum Meinberg Standard Telegramm keine lokale Zeitzone oder UTC sondern die GPS-Zeit ohne Umrechnung auf UTC. Das Format ist:

<STX>D:*tt.mm.jj;T:w;U:hh.mm.ss;uvGy;lll*<ETX>

Die *kursiv* gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Startzeichen Start-Of-Text, (ASCII Code 02h)

tt.mm.jj das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr ohne Jahrhundert	(00..99)

w der Wochentag (1..7, 1 = Montag)

hh.mm.ss die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)

uv Status der GPS Funkuhr:

u:	'#'	Uhr läuft frei (ohne genaue Zeitsynchronisation)
	"	(Leerzeichen, 20h)
		Uhr läuft GPS synchron (Grundgenauig. erreicht)
v:	'*'	Empfänger hat die Position noch nicht überprüft
	' '	(Leerzeichen, 20h)
		Empfänger hat seine Position bestimmt

G Kennzeichen der Zeitzone „GPS-Zeit"

y Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:

'A'	Ankündigung einer Schaltsekunde
' '	(Leerzeichen, 20h) kein Zeitsprung angekündigt

lll Anzahl der Schaltsekunden zwischen GPS-Zeit und UTC
(UTC = GPS-Zeit + Anzahl Schaltsekunden)

<ETX> End-Of-Text (ASCII Code 03h)

13.1.3 Format des Meinberg Capture Telegramms

Das Meinberg Capture Telegramm besteht aus einer Folge von 31 ASCII-Zeichen, abgeschlossen durch eine CR/LF (Carriage Return/Line Feed) Sequenz. Das Format ist:

CH*x_tt.mm.jj_hh:mm:ss.fffffff*<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

x	0 oder 1, Nummer des Eingangs
_	ASCII space 20h

tt.mm.jj das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr ohne Jahrhundert	(00..99)

hh:mm:ss.fffffff die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
fffffff	Bruchteile der Sekunden, 7 Stellen	

<CR> Carriage Return, ASCII Code 0Dh

<LF> Line Feed, ASCII Code 0Ah

13.1.4 Format des SAT Telegramms

Das SAT Telegramm besteht aus einer Folge von 29 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Das Format ist:

<STX>*tt.mm.jj*/*w*/*hh:mm:ss*xxxxu*v*<CR><LF><ETX>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX>	Start-Of-Text, ASCII Code 02h wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
tt.mm.jj	das Datum:		
	tt	Monatstag	(01..31)
	mm	Monat	(01..12)
	jj	Jahr ohne Jahrhundert	(00..99)
	w	der Wochentag	(1..7, 1 = Montag)
hh:mm:ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
xxxx	Kennzeichen der Zeitzone:		
	UTC	Universal Time Coordinated, früher GMT	
	MEZ	Mitteleuropäische Standardzeit	
	MESZ	Mitteleuropäische Sommerzeit	
u	Status der Funkuhr:		
	'*'	GPS-Empfänger hat seine Position noch nicht überprüft	
	' '	(Leerzeichen, 20h) GPS-Empfänger hat seine Position bestimmt	
v	Ankündigung eines Zeitsprungs während der letzten Stunde vor dem Ereignis:		
	'!'	Ankündigung Beginn oder Ende der Sommerzeit	
	' '	(Leerzeichen, 20h) kein Zeitsprung angekündigt	
<CR>	Carriage Return, ASCII Code 0Dh		
<LF>	Line Feed, ASCII Code 0Ah		
<ETX>	End-Of-Text, ASCII Code 03h		

13.1.5 Format des Telegramms Uni Erlangen (NTP)

Das Zeitelegramm Uni Erlangen (NTP) einer GPS-Funkuhr besteht aus einer Folge von 66 ASCII-Zeichen, eingeleitet durch das Zeichen STX (Start-of-Text) und abgeschlossen durch das Zeichen ETX (End-of-Text). Das Format ist:

<STX>*tt.mm.jj; w; hh:mm:ss; voo:oo; acdfg i;bbb.bbbbn lll.llle hhhhm*<ETX>

Die kursiv gedruckten Zeichen werden durch Ziffern oder Buchstaben ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<STX> Start-Of-Text, ASCII Code 02h
wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet

tt.mm.jj das Datum:

tt	Monatstag	(01..31)
mm	Monat	(01..12)
jj	Jahr ohne Jahrhundert	(00..99)
w	der Wochentag	(1..7, 1 = Montag)

hh:mm:ss die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)

v Vorzeichen des Offsets der lokalen Zeitzone zu UTC

oo:oo Offset der lokalen Zeitzone zu UTC in Stunden und Minuten

ac Status der Funkuhr:

a:	'#'	Uhr hat seit dem Einschalten nicht synchronisiert
	' '	(Leerzeichen, 20h) Uhr hat bereits einmal synchronisiert
c:	'*'	GPS-Empfänger hat seine Position noch nicht überprüft
	' '	(Leerzeichen, 20h) Empfänger hat seine Position bestimmt

d Kennzeichen der Zeitzone:

'S'	MESZ	Mitteleuropäische Sommerzeit
' '	MEZ	Mitteleuropäische Standardzeit

f Ankündigung Beginn oder Ende der Sommerzeit
während der letzten Stunde vor dem Ereignis:

'!'	Ankündigung Beginn oder Ende der Sommerzeit
' '	(Leerzeichen, 20h) kein Zeitsprung angekündigt

g Ankündigung einer Schaltsekunde während der letzten Stunde vor dem Ereignis:

'A'	Ankündigung einer Schaltsekunde
' '	(Leerzeichen, 20h) kein Zeitsprung angekündigt

i Schaltsekunde

'L'	Schaltsekunde wird momentan eingefügt (nur in 60. sec aktiv)
' '	(Leerzeichen, 20h) Schaltsekunde nicht aktiv

bbb.bbbb Geographische Breite der Empfängerposition in Grad
führende Stellen werden mit Leerzeichen (20h) aufgefüllt

n Geographische Breite, mögliche Zeichen sind:

'N'	nördlich d. Äquators
'S'	südlich d. Äquators

lll.llll	Geographische Länge der Empfängerposition in Grad führende Stellen werden mit Leerzeichen (20h) aufgefüllt
e	Geographische Länge, mögliche Zeichen sind: 'E' östlich Greenwich 'W' westlich Greenwich
hhhh	Höhe der Empfängerposition über WGS84 Ellipsoid in Metern führende Stellen werden mit Leerzeichen (20h) aufgefüllt
<ETX>	End-Of-Text, ASCII Code 03h

13.1.6 Format des NMEA 0183 Telegramms (RMC)

Das NMEA Telegramm besteht aus einer Folge von 65 ASCII-Zeichen, eingeleitet durch das Zeichen '$GPRMC' und abgeschlossen durch die Zeichen CR (Carriage Return) und LF (Line Feed). Das Format ist:

$GPRMC,*hhmmss.ss,A,bbbb.bb,n,lllll.ll,e,0.0,0.0,ddmmyy,0.0,a*hh*<CR><LF>

Die kursiv gedruckten Zeichen werden durch Ziffern oder Buchstaben ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

$ — Start character, ASCII Code 24h
wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet

hhmmss.ss — die Zeit:

hh	Stunden	(00..23)
mm	Minuten	(00..59)
ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
ss	Sekunden	(1/10 ; 1/100)

A — Status (A = Zeitdaten gültig, V = Zeitdaten ungültig)

bbbb.bb — Geographische Breite der Empfängerposition in Grad
führende Stellen werden mit Leerzeichen (20h) aufgefüllt

n — Geographische Breite, mögliche Zeichen sind:

'N'	nördlich d. Äquators
'S'	südlich d. Äquators

lllll.ll — Geographische Länge der Empfängerposition in Grad
führende Stellen werden mit Leerzeichen (20h) aufgefüllt

e — Geographische Länge, mögliche Zeichen sind:

'E'	östlich Greenwich
'W'	westlich Greenwich

0.0,0.0 — Geschwindigkeit in Knoten und die Richtung in Grad
Bei einer Meinberg GPS-Uhr sind diese Werte immer 0.0,
bei einer GNS-Uhr werden die Werte bei mobilen Anwendungen berechnet

ddmmyy — das Datum:

dd	Monatstag	(01..31)
mm	Monat	(01..12)
yy	Jahr ohne Jahrhundert	(00..99)

a — magnetische Variation E/W

hh — Prüfsumme (XOR über alle Zeichen außer '$' und '*')

<CR> — Carriage Return, ASCII Code 0Dh

<LF> — Line Feed, ASCII Code 0Ah

13.1.7 Format des NMEA 0183 Telegramms (GGA)

Das NMEA (GGA) Telegramm besteht aus einer Zeichenfolge, die durch das Zeichen '$GPGGA' eingeleitet wird und abgeschlossen durch die Zeichen CR (Carriage Return) und LF (Line Feed). Das Format ist:

$GPGGA,*hhmmss.ss,bbbb.bbbbb,n,lllll.ll,e,A,vv,hhh.h,aaa.a,M,ggg.g,M,,0*cs*<CR><LF>

Die kursiv gedruckten Zeichen werden durch Ziffern oder Buchstaben ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

$	Start character, ASCII Code 24h wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
hhmmss.ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
	ss	Sekunden	(1/10 ; 1/100)
bbbb.bbbbb	Geographische Breite der Empfängerposition in Grad führende Stellen werden mit Leerzeichen (20h) aufgefüllt		
n	Geographische Breite, mögliche Zeichen sind:		
	'N'	nördlich d. Äquators	
	'S'	südlich d. Äquators	
lllll.lllll	Geographische Länge der Empfängerposition in Grad führende Stellen werden mit Leerzeichen (20h) aufgefüllt		
e	Geographische Länge, mögliche Zeichen sind:		
	'E'	östlich Greenwich	
	'W'	westlich Greenwich	
A	Position bestimmt (1 = ja, 0 = nein)		
vv	Anzahl der verwendeten Satelliten		
hhh.h	HDOP (Horizontal Dilution of Precision)		
aaa.h	Mittlere Meereshöhe (MSL = WGS84 Höhe - Geoid Separation)		
M	Einheit Meter (fester Wert)		
ggg.g	Geoid Separation (WGS84 Höhe - MSL Höhe)		
M	Einheit Meter (fester Wert)		
cs	Prüfsumme (XOR über alle Zeichen außer '$' und '*')		
<CR>	Carriage Return, ASCII Code 0Dh		
<LF>	Line Feed, ASCII Code 0Ah		

13.1.8 Format des NMEA 0183 Telegramms (ZDA)

Das NMEA ZDA Telegramm besteht aus einer Folge von 38 ASCII-Zeichen, eingeleitet durch das Zeichen **'$GPZDA'** und abgeschlossen durch die Zeichen **CR** (Carriage Return) und LF (Line Feed). Das Format ist:

$GPZDA,*hhmmss.ss,dd,mm,yyyy,HH,II*cs*<CR><LF>
ZDA - Zeit und Datum: UTC, Tag, Monat, Jahr und lokale Zeitzone

Die kursiv gedruckten Zeichen werden durch Ziffern oder Buchstaben ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

$	Start character, ASCII Code 24h wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
hhmmss.ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
HH,II	die lokale Zeitzone (Offset zu UTC):		
	HH	Stunden	(00..±13)
	II	Minuten	(00..59)
dd,mm,yy	das Datum:		
	dd	Monatstag	(01..31)
	mm	Monat	(01..12)
	yyyy	Jahr	(0000..9999)
cs	Prüfsumme (XOR über alle Zeichen außer '$' und '*')		
<CR>	Carriage Return, ASCII Code 0Dh		
<LF>	Line Feed, ASCII Code 0Ah		

13.1.9 Format des ABB SPA Telegramms

Das ABB-SPA-Zeittelegramm besteht aus einer Folge von 32 ASCII-Zeichen, eingeleitet durch die Zeichenfolge **„>900WD:“** und abgeschlossen durch das Zeichen **<CR>** (Carriage Return). Das Format ist:

>900WD:*jj-mm-tt_hh.mm;ss.fff:cc*<CR>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

jj-mm-tt	das Datum:		
	jj	Jahr ohne Jahrhundert	(00..99)
	mm	Monat	(01..12)
	tt	Monatstag	(01..31)
	_	Leerzeichen (ASCII-code 20h)	
hh.mm;ss.fff	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
	fff	Millisekunden	(000..999)
cc	Prüfsumme. Die Berechnung erfolgt durch Exklusiv-Oder-Verknüpfung der vorhergehenden Zeichen, dargestellt wird der resultierende Byte-Wert im Hex-Format (2 ASCII-Zeichen ‘0‘ bis ‘9‘ oder ‘A‘ bis ‘F‘)		
<CR>	Carriage Return, ASCII Code 0Dh		

13.1.10 Format des Computime Zeittelegramms

Das Computime-Zeittelegramm besteht aus einer Folge von 24 ASCII-Zeichen, eingeleitet durch das Zeichen T und abgeschlossen durch das Zeichen LF (Line-Feed, ASCII-Code 0Ah). Das Format ist:

T:***jj:mm:tt:ww:hh:mm:ss***<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

T	Startzeichen wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
jj:mm:tt	das Datum:		
	jj	Jahr ohne Jahrhundert	(00..99)
	mm	Monat	(01..12)
	tt	Monatstag	(01..31)
	ww	der Wochentag	(01..07, 01 = Montag)
hh:mm:ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
<CR>	Carriage Return, ASCII Code 0Dh		
<LF>	Line Feed, ASCII Code 0Ah		

13.1.11 Format des RACAL Zeittelegramms

Das RACAL Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch das Zeichen X und abgeschlossen durch das Zeichen CR (Carriage Return, ASCII Code 0Dh). Das Format ist:

<X><G><U>***yymmddhhmmss***<CR>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<X>	Startzeichen wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		code 58h
<G>	Kontrollzeichen		code 47h
<U>	Kontrollzeichen		code 55h
jjmmdd	das Datum:		
	jj	Jahr ohne Jahrhundert	(00..99)
	mm	Monat	(01..12)
	dd	Monatstag	(01..31)
hhmmss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
<CR>	Carriage-Return, ASCII-Code 0Dh		

13.1.12 Format des SYSPLEX-1 Zeittelegramms

Das SYSPLEX1 Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch SOH (Start of Header) ASCII Kontrollzeichen und abgeschlossen durch das Zeichen LF (Line Feed, ASCII Code 0Ah).

Bitte beachten:
Damit das Zeittelegramm über ein ausgewähltes Terminalprogramm korrekt ausgegeben und angezeigt werden kann, muss ein „ **C** “ (einmalig, ohne Anführungszeichen) eingegeben werden.

Das Format ist:

<SOH>*ddd:hh:mm:ssq*<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	Start of Header (ASCII Kontrollzeichen) wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
ddd	Jahrestag		(001..366)
hh:mm:ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
	q	Status der Funkuhr:	(space) Time Sync (GPS lock) (?) no Time Sync (GPS fail)
<CR>	Carriage-Return, ASCII-Code 0Dh		
<LF>	Line-Feed, ASCII-Code 0Ah		

13.1.13 Format des ION Zeittelegramms

Das ION Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch SOH (Start of Header) ASCII Kontrollzeichen und abgeschlossen durch das Zeichen LF (Line Feed, ASCII Code 0Ah). Das Format ist:

<SOH>*ddd:hh:mm:ss*q<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	Start of Header (ASCII Kontrollzeichen) wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
ddd	Jahrestag		(001..366)
hh:mm:ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
	q	Status der Funkuhr:	(space) Time Sync (GPS lock) (?) no Time Sync (GPS fail)
<CR>	Carriage-Return, ASCII-Code 0Dh		
<LF>	Line-Feed, ASCII-Code 0Ah		

13.1.14 Format des ION Blanked Zeittelegramms

Das ION Blanked Zeittelegramm besteht aus einer Folge von 16 ASCII-Zeichen, eingeleitet durch SOH (Start of Header) ASCII Kontrollzeichen und abgeschlossen durch das Zeichen LF (Line Feed, ASCII Code 0Ah). Das Format ist:

<SOH>***ddd:hh:mm:ssq***<CR><LF>

Wichtig: Das Blanking Intervall hat eine Länge von 2 Minuten 30 Sekunden und wird alle 5 Minuten eingefügt.

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

<SOH>	Start of Header (ASCII Kontrollzeichen) wird mit der Genauigkeit eines Bits zum Sekundenwechsel gesendet		
ddd	Jahrestag		(001..366)
hh:mm:ss	die Zeit:		
	hh	Stunden	(00..23)
	mm	Minuten	(00..59)
	ss	Sekunden	(00..59, oder 60 wenn Schaltsekunde)
	q	Status der Funkuhr:	(space) Time Sync (GPS lock) (?) no Time Sync (GPS fail)
<CR>	Carriage-Return, ASCII-Code 0Dh		
<LF>	Line-Feed, ASCII-Code 0Ah		

13.1.15 Format des IRIG J Zeittelegramms

Der Zeitcode besteht aus einer Folge von ASCII Zeichen, welche im Format 7O1:

- 1 Startbit
- 7 Datenbit
- 1 Paritätsbit (ungerade)
- 1 Stopbit

gesendet wird.

Die Gültigkeit des Telegramms wird durch die steigenden Flanke des Startbits gekennzeichnet. Das Telegramm umfasst 15 Zeichen und wird sekündlich mit einer Baudrate von 300 oder größer gesendet. Das Format ist:

<SOH>*DDD:HH:MM:SS*<CR><LF>

Die kursiv gedruckten Buchstaben werden durch Ziffern ersetzt, die restlichen Zeichen sind Bestandteil des Zeittelegramms. Die einzelnen Zeichengruppen haben folgende Bedeutung:

SOH	ASCII Code „Start of Heading“ (0x01h)
DDD	Tag des Jahres (1 bis 366)
HH, MM, SS	Zeit des Startbits in Stunde (HH), Minute (MM), Sekunde (SS)
CR	ASCII Code „Carriage Return“ (0x0Dh)
LF	ASCII Code „Line Feed“ (0x0Ah)

13.2 SyncMon Formate

SyncMon-Format für die Verwendung der LANTIME-Firmware:

```
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
```

Schlüssel- und Wert-Paare
Das Format mit Schlüsselwertpaaren kann direkt von einem SPLUNK-Datenbankserver aus aufgerufen werden und hat folgendes 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
Das JSON-Format kann von den meisten Datenbanken direkt verarbeitet werden und hat das folgende 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“
}
```

13.3 Eingesetzte Software von Drittherstellern

Der LANTIME Netzwerk Zeitserver führt eine Reihe von Software aus, die auf der Arbeit von OpenSource Projekten basieren. Sehr viele Personen haben bei der Entwicklung und Realisierung dieser Software mitgearbeitet. Wir bedanken uns ausdrücklich für diese Arbeit.

Die eingesetzte OpenSource-Software unterliegt ihren eigenen Lizenzbedingungen, die wir im Folgenden aufführen. Sollte der Einsatz einer eingesetzten Software deren Lizenzbestimmungen verletzen, werden wir nach Mitteilung unverzüglich dafür sorgen, dass diese Lizenzbestimmungen wieder eingehalten werden.

Ist für eins der eingesetzten Software-Produkte vorgeschrieben, dass der zugrundeliegende Quellcode von der Firma Meinberg zur Verfügung gestellt werden muss, senden wir Ihnen auf Anfrage entweder einen Datenträger oder eine E-Mail zu oder wir stellen Ihnen einen Link zur Verfügungen, unter dem Sie die aktuellste Version des Quellcodes im Internet beziehen können. Bitte beachten Sie, dass wir bei Zusendung eines Datenträgers die dabei anfallenden Kosten in Rechnung stellen müssen.

13.3.1 Betriebssystem GNU/Linux

Die Weitergabe des GNU/Linux Betriebssystems unterliegt der GNU General Public License, die wir weiter unten abdrucken.

Mehr zu GNU/Linux finden Sie auf der GNU-Homepage
www.gnu.org

sowie auf der Homepage von GNU/Linux
www.linux.org

13.3.2 Samba

Die Samba Software Suite ist eine Gruppe von Programmen, die das Server Message Block (abgekürzt SMB) Protokoll für UNIX Systeme implementiert. Durch den Einsatz von Samba ist das Senden von Windows Popup Meldungen sowie die Abfrage der Zeit durch Clients mithilfe des NET TIME Befehls möglich.
Die Weitergabe von Samba unterliegt – wie bei GNU/Linux – der GNU General Public License, siehe Abdruck weiter unten.

Die Website des Samba – Projekts (bzw. einen Mirror) finden Sie unter:
www.samba.org

13.3.3 Network Time Protocol Version 4 (NTP)

Das von David L. Mills geleitete NTP-Projekt ist im Internet unter www.ntp.org erreichbar, dort finden sich eine Fülle von Informationen und Anleitungen zum Einsatz dieses Standard-Softwarepakets. Die Weitergabe und der Einsatz der NTP-Software ist erlaubt, solange der folgende Hinweis in der Dokumentation vorhanden ist:

13.3.4 lighttpd

Für die webbasierende Konfigurationsoberfläche (sowohl HTTP als auch HTTPS) setzen wir die Software lighttpd ein. Lighttpd ist ein freier Webserver, der vom deutschen Entwickler Jan Kneschke stammt und alle wesentlichen
Funktionen eines Webservers beinhalted.

Die Verwendung dieser Software ist durch folgende Lizenz abgedeckt:

13.3.5 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

13.4 Literaturverzeichnis

[**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

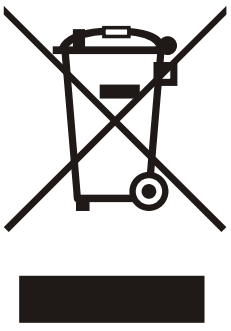
14 RoHS und WEEE

Befolgung der EU Richtlinie 2011/65/EU (RoHS)

Wir erklären hiermit, dass unsere Produkte den Anforderungen der Richtlinie 2011/65/EU und deren deligierten Richtlinie 2015/863/EU genügt und dass somit keine unzulässigen Stoffe im Sinne dieser Richtlinie in unseren Produkten enthalten sind. Wir versichern, dass unsere elektronischen Geräte, die wir in der EU vertreiben, keine Stoffe wie Blei, Kadmium, Quecksilber, sechswertiges Chrom, polybrominatierte Biphenyle (PBBs) und polybrominatierten Diphenyl-Äther (PBDEs), Bis(2-ethylhexyl)phthalat (DEHP), Benzylbutylphthalat (BBP), Dibutylphthalat (DBP), Diisobutylphthalat (DIBP), über den zugelassenen Richtwerten enthalten.

WEEE-Status des Produkts

Dieses Produkt fällt unter die B2B-Kategorie. Zur Entsorgung muss es an den Hersteller übergeben werden. Die Versandkosten für den Rücktransport sind vom Kunden zu tragen, die Entsorgung selbst wird von Meinberg übernommen.



15 Konformitätserklärung

Declaration of Conformity

Doc ID: LCES/NTP/LNE/RPS/BGT-04.02.2022

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

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

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

auf das sich diese Erklärung bezieht, mit den folgenden Normen und Richtlinien übereinstimmt:
to which this declaration relates is in conformity with the following standards and provisions of the directives:

EMV – Richtlinie *EMC Directive* 2014/30/EU	DIN EN 61000-6-2:2019 DIN EN 61000-6-3:2007 + A1:2011 DIN EN 55032:2015 DIN EN 55024:2010 + A1:2015 DIN EN 61000-3-2:2019 DIN EN 61000-3-3:2013 + A1:2019
Niederspannungsrichtlinie *Low-voltage Directive* 2014/35/EU	DIN EN 62368-1:2014 + A11:2017
RoHS – Richtlinie *RoHS Directive* 2011/65/EU + 2015/863/EU	DIN EN IEC 63000:2018

Bad Pyrmont, den 04.02.2022

Stephan Meinberg
Production Manager

LCES_NTP_LNE_RPS_QSG_040222