USER MANUAL

Network Time Server NTS 3/4/5000 Series

NTS-3000
NTS-4000 OCXO
NTS-5000 RUBIDIUM & OCXO
NTS-9000 CESIUM MIL & METROLOGY
with 5071A cesium and HROG-10 direct UTC mode optional support

Updated: February 5th, 2025

SAFETY INSTRUCTIONS

ATTENTION!

These are the important safety instructions that should be followed during the installation and maintenance of the ELPROMA NTS-x000 family of timeservers.

IMPORTANT NOTE!

This equipment contains hazardous AC and DC voltages. Do not handle any metallic part until the power has been disconnected. Do not assemble; disassemble when the power is ON. Making any wiring and touching cables is strongly prohibited when power is ON. Please refer to your RACK'19 safety instruction to learn more about connecting power to server equipment. The NTS-protection system requires the PE line to be connected to RACK'19 din rails.

Elproma safety advises:

1. Safety first! Never work alone under hazardous voltage conditions
2. High short circuit current through conductive materials can cause server burns
3. Check that the power cord(s), plug(s), and sockets are in good conditions
4. Always use qualified service personnel to install permanently wired equipment
5. Do not handle any metallic part before the main power has been disconnected
6. Take care your power lines and rack'19 frame is properly PE grounded

ELPROMA Electronics Poland Sp. z o.o.
Dunska 2A street, 05-152 Czosnow (near Warsaw) POLAND, EU
Phone: +48 227517680
Internet: http://www.elpromaelectronics.com
General info e-mail: info@elpromaelectronics.com
Support e-mail: support@elpromaelectronics.com

ACRONYMS

1PPS	1 Pulse Per Second	**ITU**	International Telecom Union
AIV	Assembly, Integration and Validation	**KPI**	Key Performance Indicator
BIPM	Bureau International des Poids et Mesures	**MCT**	Modular Coherent Transfer
CA	Certificate Authority	**NMI**	National Metrological Institutes
CCTF	Consultative Committee for Time and Frequency	**NTA**	National Time Authority (mostly the same as NMI)
CIF	Core Infrastructure Facilities	**NTP**	Network Time Protocol
COTS	Commercial Off-the-Shelf	**OFT**	Optical Fibber Technology
CV	Common View	**OSC**	Oscillators (OCXO, Rubidium, Cs)
DAB	Digital Audio Broadcasting	**PPP**	Point Precise Positioning
DEMETRA	Demonstrator for EGNSS services based on Time Reference Architecture	**PTP** **PTPv2**	Precise Time Protocol IEEE 1588 (WR –White Rabbit profile of PTP)
DB	Database (mostly SQL)	**QR**	Quality Report
DVB	Digital Video Broadcasting	**RINEX**	Receiver Independent Exchange Format
ETH	Ethernet	**RMO**	Regional Metrological Organization
EBU	European Broadcast Union	**SFN**	Single Frequency Network
EGNOS	European geostationary navigation overlay system	**SIS**	Signal In Space
EGNSS	European GNSS	**SPF**	Service Provision Facility
EURAMET	European Regional Metrological Organisation	**SV** **SVN#**	Satellite Vehicle Satellite Vehicle Number
EWR	Extended White Rabbit	**SVF**	Service Validation Facility
FO	Fibber Optic	**SW**	Software
FR	FREE-RUN mode	**T&F**	Time and(&) Frequency
GCC	Galileo Control Centre	**TAI**	International Atomic Time
FTP	File Transfer Protocol	**TA(PL)**	Polish Atomic Time
GDO	GPS Disciplined Oscillator	**TDMA**	Time Division Multiple Access
GGTO	Galileo GPS Time Offset	**TFL**	Time and Frequency Laboratory
GMT	Greenwich Mean Time	**TLC**	Time Local Clock (the same as UT)
GNSS	Global Navigation Satellite System	**TMC**	Time Master Clock (see TSG)
GPS	Global Positioning System	**TRF**	Time Reference Facility (see TMC)
GPST	GPS Time Scale	**TSA**	Time Stamping Authority
GSA	GNSS Supervising Authority	**TSI**	Time Service Infrastructures
GST	Galileo System Time	**TWSTF**	Two Way Satellite Time and Frequency Transfer
HTTP **HTTPS**	Hypertext Transfer Protocol Hypertext Transfer Protocol Secure	**UT**	User Terminal (see also TLC)
HO	HOLDOVER mode (e.g. operating w/o GNSS)	**UTC**	Universal Time Coordinated
HW	Hardware	**WP**	Work Package
IPR	Intellectual Property Rights	**WR**	White Rabbit (see PTP)
IRIG-B	Time Code (AM or DM)	**WPL**	Work Package Leader

SYNCHRONIZATION TERMS

Accuracy - The degree of conformity of a measured or calculated value to its definition or with respect to a standard reference time. In the meaning of NTP (Network Time Protocol) the accuracy determines how close the PC clock is to UTC reference (GNSS or external atomic clock).

Atomic Time Scale (TA) - a time scale based on atomic or molecular resonance phenomena. Elapsed time is measured by counting cycles of a frequency locked to an atomic or molecular transition. Earlier time scales were based on the rotational rate of the earth.

BEIDOU – (see COMPASS)

Calibration - The process of identifying and measuring time or frequency errors, offsets, or deviations of a clock/oscillator relative to an established standard, such as UTC(NIST).

Clock - a device for maintaining and displaying time.

GOMPASS (BEIDOU)– is Chinese satellite navigation system. It consists of two separate satellite constellations – a limited test system that has been operating since 2000, and a full-scale global navigation system that is currently under construction. The first BeiDou system, officially called the BeiDou Satellite Navigation Experimental System.

Coordinated Universal Time (UTC) - a coordinated time scale, maintained by the Bureau International des Poids et Mesures (BIPM), which forms the basis of a coordinated dissemination of standard frequencies and time signals. A UTC clock has the same rate as a Temps Atomique International (TAI) clock or international atomic time clock but differs by an integral number of seconds called leap seconds. The UTC scale is adjusted by the insertion or deletion of leap seconds to ensure approximate agreement with UT1.

Drift (frequency) - the linear (first-order) component of a systematic change in frequency of an oscillator over time.

Frequency - the rate at which a periodic phenomenon occurs over time. Frequency drift - see drift. Frequency offset - the frequency difference between the measured value and the defined value. Frequency shift - change in frequency from a standard reference. Frequency stability - statistical estimate of the frequency fluctuations of a signal over a given time interval.

Frequency standard - an oscillator such as a rubidium (Rb), cesium (Cs), or hydrogen (H) maser who's output is used as a frequency.

GALILEO – is a global navigation satellite system (GNSS) currently being built by the European Union (EU) and European Space Agency (ESA). One of the aims of Galileo is to provide a high-precision positioning system upon which European nations can rely, independently from the Russian GLONASS, US GPS, and Chinese COMPASS (BEIDOU) which can be disabled in times of war or conflict. Galileo is compatible to US GPS (see GPS).

GLONASS – acronym for **Glo**balnaya **na**vigatsionnaya **s**putnikovaya **s**istema or **Glo**bal **Na**vigation **S**atellite **S**ystem, is a space-based satellite navigation system operated by the Russian Aerospace Defence Forces. It provides an alternative to Global Positioning System (GPS) and is the only alternative navigational system in operation with global coverage and of comparable precision. Glonass use L1-1575.42MHz with additional frequency margin between 1597.50-1609.50Mhz.

GPS (Global Positioning System) - a highly accurate, global satellite navigation system based on a constellation of at 24 satellites orbiting the earth at a very high altitude 20000 km. GPS signals are: L1-1575.42MHz;L2-1227.6MHz;L3-1381.05 MHz

GMT (Greenwich Mean Time) - a 24 Hour system based on mean solar time plus 12 hours at Greenwich, England. Greenwich Mean Time can be considered approximately equivalent to Coordinated Universal Time (UTC), which is broadcast from all standard time and frequency radio stations. However, GMT is now obsolete and has been replaced by UTC.

International Atomic Time (TAI) - an atomic time scale based on data from a worldwide set of atomic clocks. It is the internationally agreed upon time reference conforming to the definition of the second, the fundamental unit of atomic time in the International System of Units (SI). It is defined as the duration of 9 192 631 770 periods of the radiation corresponding to the transition between two hyperfine levels of the ground state of the cesium - 133 atom.

Synchronization - The process of measuring the difference in time of two time scales such as the output signals generated by two clocks. In the context of timing, synchronization means to bring two clocks or data streams into phase so that their difference is 0 (see time scales in synchronism).

Synchronization - Relative adjustment of two frequency sources with the purpose of canceling their frequency difference but not necessarily their phase difference.

Stability (frequency) - statistical estimate of the frequency fluctuations of a signal over a given time interval: Long term stability usually involves measurement averages beyond 100s. Short term stability usually involves measurement averages from a few tenths of a second to 100s.

Stratum - indicates how fare from cesium ref. the clock is in the chain of synchronization.

Time code - a system of symbols (digital or analog) used for identifying specific instants of time. An information format used to convey time information. IRIG-B is example of Time Code.

Time interval - The duration between two instants read on the same time scale.

Time scale - a system of unambiguous ordering of events. A time scale is meant to be stable and homogeneous.

Time standard - a continuously operated device used for the realization of a time scale in accordance with the definition of the second and with an appropriately chosen origin.

Time step - a discontinuity in a time scale at some instant. A step is positive (+) if the time scale reading is increased and negative (-) if the reading is decreased at that instant.

UNDERSTANDING OSCILLATOR HOLDOVER

Customers frequently ask the question, *"How long server can operate holdover w/o GNSS signals."* The answer depends on the built-in oscillator version and requests output NTP/PTP accuracy to UTC. Depending on the server model, Elproma supports the following oscillators:

NTS-3000 std. **QUARTZ**
NTS-4000 **OCXO**
NTS-5000 LITE **OCXO**
NTS-5000 **RUBIDIUM** & OCXO

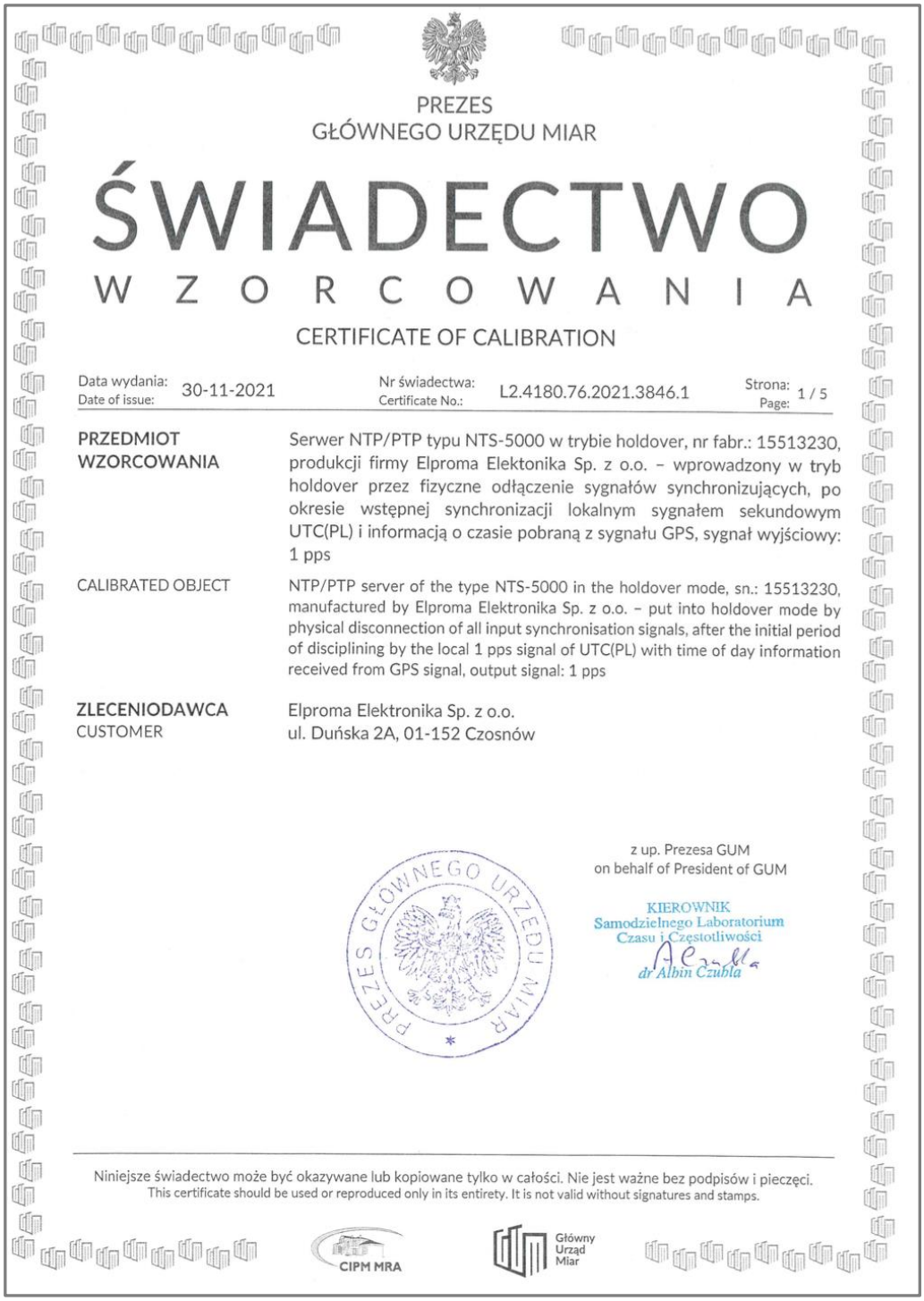
Higher accuracy of synchronization requests concludes with shorter holdover operations for the same version of the oscillator. Independently, each NTS-x000 (NTS-3000, NTS-4000, NTS-50000) product can be extra-ordinary equipped with a TCXO oscillator for chip low-noise clocking. It can be used simultaneously with other versions of oscillators, such as OCXO and RUBIDIUM (Rb).

IMPORTANT NOTE!
Above figures basis on several important assumptions:

- **Server operates in constant temperature**
- **No initial phase and frequency error**
- **Time server device has been powered for one month and locked to GNSS for 72 hours**

Difference between Accuracy and Stability of Synchronization

METROLOGY HOLDOVER CERTIFICATION



PREZES
GŁÓWNEGO URZĘDU MIAR

ŚWIADECTWO
W Z O R C O W A N I A

CERTIFICATE OF CALIBRATION

Data wydania: Date of issue: 30-11-2021 | Nr świadectwa: Certificate No.: L2.4180.76.2021.3846.1 | Strona: Page: 1 / 5

PRZEDMIOT WZORCOWANIA

Serwer NTP/PTP typu NTS-5000 w trybie holdover, nr fabr.: 15513230, produkcji firmy Elproma Elektonika Sp. z o.o. – wprowadzony w tryb holdover przez fizyczne odłączenie sygnałów synchronizujących, po okresie wstępnej synchronizacji lokalnym sygnałem sekundowym UTC(PL) i informacją o czasie pobraną z sygnału GPS, sygnał wyjściowy: 1 pps

CALIBRATED OBJECT

NTP/PTP server of the type NTS-5000 in the holdover mode, sn.: 15513230, manufactured by Elproma Elektronika Sp. z o.o. – put into holdover mode by physical disconnection of all input synchronisation signals, after the initial period of disciplining by the local 1 pps signal of UTC(PL) with time of day information received from GPS signal, output signal: 1 pps

ZLECENIODAWCA
CUSTOMER

Elproma Elektronika Sp. z o.o.
ul. Duńska 2A, 01-152 Czosnów

PREZES GŁÓWNEGO URZĘDU MIAR

z up. Prezesa GUM
on behalf of President of GUM

KIEROWNIK
Samodzielnego Laboratorium
Czasu i Częstotliwości
dr Albin Czubla

Niniejsze świadectwo może być okazywane lub kopiowane tylko w całości. Nie jest ważne bez podpisów i pieczęci.
This certificate should be used or reproduced only in its entirety. It is not valid without signatures and stamps.

CIPM MRA

Główny Urząd Miar

METODA WZORCOWANIA

Porównanie czasu fazowego sygnału wyjściowego 1 pps wzorcowanego serwera PTP/NTP względem sygnału sekundowego UTC(PL) za pomocą częstościomierza-czasomierza kontrolnego - wg instrukcji wzorcowania zegarów, numer systemowy IW6-TF wyd. 8 z 23.04.2021 r.

METHOD OF CALIBRATION

Comparison of phase time of a 1 pps output signal of a server NTP/PTP under tests with reference to the UTC(PL) 1 pps signals using as a control device a time and frequency counter – instruction of clocks calibration, No. IW6-TF, issue 8, April 23, 2021

WARUNKI ŚRODOWISKOWE

Temperatura otoczenia w czasie wykonywania wzorcowania wynosiła: (20,5 ÷ 22,5) °C.

ENVIRONMENTAL CONDITIONS

During calibration ambient temperature amounted to: (20,5 ÷ 22,5) °C

DATA WYKONANIA POMIARÓW DATE OF CALIBRATION

October 8, 2021 – November 9, 2021

SPÓJNOŚĆ POMIAROWA

Wyniki wzorcowania serwera NTP/PTP zostały odniesione do utrzymywanego w GUM państwowego wzorca jednostek miar czasu i częstotliwości przez zastosowanie jako przyrządu kontrolnego: częstościomierza czasomierza typu SR620, nr fabr. 4423, synchronizowanego sygnałem wzorcowym częstotliwości pobieranym z państwowego wzorca jednostek miar czasu i częstotliwości oraz pomiary czasu fazowego względem sygnału UTC(PL)

TRACEABILITY

Calibration results of the NTP/PTP server have been referred to the national time and frequency standard maintained at the Central Office of Measures through application of following control device: SR620 type universal counter, sn 4423, synchronized by standard frequency taken from the national time and frequency standard as well as phase time measurement performed with reference to the UTC(PL).

NIEPEWNOŚĆ POMIARU

Niepewność pomiaru została wyznaczona zgodnie z zaleceniami zawartymi w dokumencie EA-4/02 M: 2013. Podane wartości niepewności stanowią niepewność rozszerzoną przy prawdopodobieństwie rozszerzenia ok. 95 % i współczynniku rozszerzenia k =2

UNCERTAINTY OF MEASUREMENT

The measurement uncertainty has been determined in accordance with EA-4/02 M: 2013 Document. The reported expanded uncertainty is stated as the standard uncertainty multiplied by the coverage factor k =2, which corresponds to a coverage probability of approximately 95 %.

WYNIKI WZORCOWANIA RESULTS OF CALIBRATION

Przedstawione poniżej wyniki wzorcowania odnoszą się wyłącznie do przedmiotu wzorcowania.
Results presented below relate only to the object of calibration.

1. Błąd pomiaru zegara/ serwera NTP/PTP (dla sygnału wyjściowego 1 pps z tyłu urządzenia wynosi) w trybie Rb Holdover:
   a) przed przejściem w tryb Rb Holdover (w trybie synchronizacji sygnałem UTC(PL) i z podłączoną anteną GNSS):

   (0,0 ± 0,1) µs,

   b) w trybie Rb Holdover (w zależności od czasu po odłączeniu sygnału UTC(PL) i anteny GNSS):

Czas pracy bez synchronizacji	1 d	2 d	3 d	4 d	5 d	6 d	7 d
Błąd pomiaru zegara, µs	-0,5 ± 0,1	-1,2 ± 0,1	-1,8 ± 0,1	-2,4 ± 0,1	-2,9 ± 0,1	-3,3 ± 0,1	-3,7 ± 0,1

1. The measurement error of the clock/ NTP/PTP server (for the 1 pps output signal in the back of the device) in Rb Holdover mode amounts to:
   a) before switching into Rb Holdover mode (disciplined by 1 pps of UTC(PL) and with connected GNSS antenna):

   (0,0 ± 0,1) µs,

   b) in Rb Holdover mode (against time after disconnection of the 1 pps of UTC(PL) and GPS antenna):

Time of work with no disciplining	1 d	2 d	3 d	4 d	5 d	6 d	7 d
Measurement error of the clock, µs	-0,5 ± 0,1	-1,2 ± 0,1	-1,8 ± 0,1	-2,4 ± 0,1	-2,9 ± 0,1	-3,3 ± 0,1	-3,7 ± 0,1

Sprawdził(a):
Checked by:
KIEROWNIK
Samodzielnego Laboratorium
Czasu i Częstotliwości
dr Albin Czubla

2. Błąd pomiaru zegara/ serwera NTP/PTP (dla sygnału wyjściowego 1 pps z tyłu urządzenia wynosi) w trybie OCXO Holdover:

   a) przed przejściem w tryb OCXO Holdover
   (w trybie synchronizacji sygnałem UTC(PL) i z podłączoną anteną GNSS):

   (0,0 ± 0,1) µs,

   b) w trybie OCXO Holdover (w zależności od czasu po odłączeniu sygnału UTC(PL) i anteny GNSS):

Czas pracy bez synchronizacji	1 d	2 d	3 d	4 d	5 d	6 d	7 d	14 d
Błąd pomiaru zegara, µs	-0,6 ± 0,1	-2,8 ± 0,1	-7,2 ± 0,1	-13,7 ± 0,1	-22,1 ± 0,1	-32,9 ± 0,1	-45,9 ± 0,1	-184,1 ± 0,1

2. The measurement error of the clock/ NTP/PTP server (for the 1 pps output signal in the back of the device) in OCXO Holdover mode amounts to:

   a) before switching into OCXO Holdover mode (disciplined by 1 pps of UTC(PL) and with connected GNSS antenna):

   (0,0 ± 0,1) µs,

   b) in OCXO Holdover mode (against time after disconnection of the 1 pps of UTC(PL) and GPS antenna):

Time of work with no disciplining	1 d	2 d	3 d	4 d	5 d	6 d	7 d	14 d
Measurement error of the clock, µs	-0,6 ± 0,1	-2,8 ± 0,1	-7,2 ± 0,1	-13,7 ± 0,1	-22,1 ± 0,1	-32,9 ± 0,1	-45,9 ± 0,1	-184,1 ± 0,1

Błąd pomiaru jest różnicą między wskazaniem przyrządu wzorcowanego a wartością (umownie) prawdziwą wielkości mierzonej. Błąd pomiaru zegara odniesiono do momentu pojawienia się zbocza narastającego sygnału wyjściowego 1 pps z wzorcowanego serwera względem sygnału UTC(PL).

Measurement error is a difference between an indication of the device under test and a (conventionally) true value of the measured quantity. Measurement error of the clock was referred to the moment of appearing the rising slopes of 1 pps output signal from the server under test in relation to UTC(PL) signal.

Sprawdził(a):
Checked by:

KIEROWNIK
Samodzielnego Laboratorium
Czasu i Częstotliwości
dr Albin Czubla

ul. Elektoralna 2, 00-139 Warszawa POLAND
tel.: +48 22 581 9156 fax: +48 22 581 9392, e-mail: time@gum.gov.pl

*The **Central Office of Measures (GUM)** fulfils its responsibilities assigned by the Act of 11 of May 2001 – Law on Measures. GUM is the National Metrology Institute (NMI) for the Republic of Poland.*

The Central Office of Measures is responsible for ensuring uniformity of measures and required accuracy of the results of measurements carried out in the Republic of Poland as well as their traceability to the International System of Units (SI).

The Central Office of Measures as the NMI is the source from which the accredited calibration laboratories obtain their measurement traceability. The primary role of the national metrology institute is confirmed in the international document ILAC P10:01/2013, ILAC Policy on the Traceability of Measurement Results and the document DA-06 issued by the Polish Centre for Accreditation entitled "PCA policy on providing traceability for measurement". GUM standards, which are referred to in the results of calibration (information on the traceability posted on the front page of certificate) are linked to the standards of European and worldwide laboratories of National Metrology Institutes through participation in mutual comparisons of standards and / or calibration performed by these laboratories.

GUM calibration laboratories have implemented a quality assurance system based on standard PN-EN ISO/IEC 17025:2018-02 "General requirements for the competence of testing and calibration laboratories".

GUM is a signatory of a Mutual Recognition Arrangement (CIPM MRA) for national measurement standards and for calibration and measurement certificates issued by national metrology institutes.

The information with regard to the Calibration and Measurement Capabilities (CMCs) is specified in Appendix C of the CIPM MRA. This certificate is consistent with the CMCs that are included in Appendix C of the Mutual Recognition Arrangement (MRA) drawn up by the International Committee for Weights and Measures (CIPM). Under the MRA, all participating institutes recognize the validity of each other's calibration and measurement certificates for the quantities, ranges and measurement uncertainties specified in Appendix C (for details see http://www.bipm.org).

ISO 9001 CERTIFICATION

qualityaustria
Succeed with Quality

CERTYFIKAT

Quality Austria - Trainings, Zertifizierungs und Begutachtungs GmbH przyznaje niniejszy **quality**austria certyfikat następującej organizacji:

Niniejszy certyfikat **quality**austria poświadcza stosowanie i dalszy rozwój skutecznego

ELPROMA ELEKTRONIKA

Elproma Elektronika Sp. z o.o.
ul. Duńska 2a, 05-152 Czosnów, Poland

SYSTEMU ZARZĄDZANIA JAKOŚCIĄ
zgodnego z wymogami normy
ISO 9001:2015

Projektowanie, produkcja i sprzedaż systemów elektronicznych ich elementów

Nr rejestracji: Q-11895/1
Data pierwszego wydania: 06 marca 2012 r.
Ważne do: 06 kwietnia 2027 r.

Ważność tego certyfikatu **quality**austria będzie utrzymywana przez coroczne audyty nadzoru i następujące co trzy lata audyty odnawiające.

Wiedeń, 16 kwietnia 2024 r.

Quality Austria - Trainings, Zertifizierungs und Begutachtungs GmbH,
AT-1010 Vienna, Zelinkagasse 10/3

Mag. Christoph Mondl
CEO

Mag. Dr. Werner Paar
CEO

Ing. Christoph Baumgartner, MSc, MBA
Upoważniony sygnatariusz,
Kierownik Customer Service Center

Bieżąca aktualność tego certyfikatu jest udokumentowana wyłącznie na stronie internetowej:
http://www.qualityaustria.com/en/cert

IQNET

Building trust together.

Certificate

Quality Austria
has issued an IQNET recognized certificate that the organization:

Elproma Elektronika Sp. z o.o.

ul. Duńska 2a / 05-152 Czosnów / Poland

for the following scope:

Designing, production and distribution of electronic devices and its components

EAC: 19; 29

has implemented and maintains a

QUALITY MANAGEMENT SYSTEM

which fulfils the requirements of the following standard

ISO 9001:2015

Issued on:	**2024-04-16**
Validity Date:	**2027-04-06**
Quality Austria certified since:	**2012-03-06**

Registration Number: **AT-11895/1**

Alex Stoichitoiu
President of IQNET

Mag. Friedrich Khuen-Belasi
Authorised Representative
of Quality Austria

qualityaustria
Succeed with Quality

This attestation is directly linked to the IQNET Member's original certificate and shall not be used as a stand-alone document

IQNET Members*:
AENOR Spain **AFNOR Certification** France **APCER** Portugal **CCC** Cyprus **CISQ** Italy **CQC** China **CQM** China **CQS** Czech Republic **Cro Cert** Croatia **DQS Holding GmbH** Germany **EAGLE Certification Group** USA **FCAV** Brazil **FONDONORMA** Venezuela **ICONTEC** Colombia **ICS** Bosnia and Herzegovina **INTECO** Costa Rica **IRAM** Argentina **JQA** Japan **KFQ** Korea **LSQA** Uruguay **MIRTEC** Greece **MSZT** Hungary **Nemko AS** Norway **NSAI** Ireland **NYCE** México **PCBC** Poland **Quality Austria** Austria **SII** Israel **SIQ** Slovenia **SIRIM QAS International** Malaysia **SQS** Switzerland **SRAC** Romania **TSE** Türkiye **YUQS** Serbia

* The list of IQNET Members is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

NATO CODIFICATION

WOJSKOWE CENTRUM NORMALIZACJI, JAKOŚCI I KODYFIKACJI
Military Centre for Standardization, Quality and Codification
43 KRAJOWE BIURO KODYFIKACYJNE
43 National Codification Bureau

ZAŚWIADCZENIE
CERTIFICATE

Zaświadcza się, że na podstawie złożonego wniosku podmiot o nazwie:
This is to certify that:

ELPROMA ELEKTRONIKA Sp. z o.o.

z siedzibą w:
located in:

05-152 CZOSNÓW UL. DUŃSKA 2A

otrzymał
was given

Kod NATO Podmiotu Gospodarczego:
***NATO Commercial and Government Entity Code – NCAGE Code*:**

9ATKH

m.p.

DYREKTOR
dr inż. Mariusz SOCZYŃSKI

Warszawa, dnia 21 czerwca 2022 r.

Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji – 43 Krajowe Biuro Kodyfikacyjne
00-909 Warszawa ♦ ul. Nowowiejska 28a ♦ tel. 261845708, fax 261845891 ♦ wcnjk@ron.mil.pl

WOJSKOWE CENTRUM NORMALIZACJI, JAKOŚCI I KODYFIKACJI
00-909 Warszawa, ul. Nowowiejska 28A
(tel. 261 845 700/fax 261 845 891)

Warszawa, 21 czerwca 2022 r.

WOJSKOWE CENTRUM NORMALIZACJI, JAKOŚCI I KODYFIKACJI
Nr 1589/22
22 CZE. 2022
03 00-909 Warszawa 03

Pan Krzysztof BORGULSKI

WICEPREZES ZARZĄDU
ELPROMA ELEKTRONIKA SP. Z O.O.

ul. Duńska 2a
05-152 Czosnów

Nr sprawy: WCNJiK-OKWO.WZ.703.310.2022

Dotyczy: *kodu NATO podmiotu gospodarczego (NCAGE Code – NATO Commercial and Government Entity Code)*

informuję, że na podstawie wniosku z dnia 10.06.2022 r. został przydzielony dla firmy **ELPROMA ELEKTRONIKA SP. Z O.O**. kod NCAGE **9ATKH** – zaświadczenie w załączeniu. Kod identyfikuje firmę w Systemie Kodyfikacyjnym NATO (NCS – NATO Codification System).
Dane firmy zostały wprowadzone do:
– Bazy Podmiotów Gospodarczych prowadzonej przez Wojskowe Centrum Normalizacji, Jakości i Kodyfikacji (WCNJiK),
– Bazy NATO Podmiotów Gospodarczych prowadzonej przez Agencję Wsparcia i Zamówień NATO (NSPA – NATO Support and Procurement Agency),
– Głównego Katalogu NATO Referencji dla Logistyki (NMCRL – NATO Master Catalogue of References for Logistics) prowadzonej przez NSPA,
– Bazy Podmiotów Gospodarczych prowadzonej przez Agencję Logistyki Departamentu Obrony Stanów Zjednoczonych (DLA – Defence Logistics Agency).
Jednocześnie proszę o powiadomienie WCNJiK w przypadku zmiany danych, które zostały podane we wniosku. Dodatkowe informacje o kodzie NCAGE dostępne są na stronie internetowej www.wcnjk.wp.mil.pl w zakładce O Nas> Kodyfikacja>Kod NCAGE.

Załączniki: 1 na 1 str. - tylko adresat

Z upoważnienia
DYREKTORA
WOJSKOWEGO CENTRUM NORMALIZACJI, JAKOŚCI I KODYFIKACJI
ppłk Stanisław HABUDA
Szef Wydziału Zarządzania
Oddziału Kodyfikacji Wyrobów Obronnych

Dorota Mirecka, 261-845-345
21.06.2022 r. T703

Details

Back

9ATKH **ELPROMA ELEKTRONIKA SP. Z O.O.**

CAGE Information

CAGE	9ATKH
UEI	
Status	Active
Type	Non-US Manufacturer
Established	06/15/2022
CAGE Update Date	06/15/2022
CAGE Expiration	
SAM Expiration	

Contact Information

POC	
Phone	
Fax	48 227517681
International	48 227517680
Address	DUNSKA 2A
P.O. Box	
City	CZOSNOW
County	
State/Province	MAZOWIECKIE
Country	POLAND
Zip/Postal	05-152
Corporate URL	WWW.ELPROMAELECTRONICS.COM

Ownership of Offeror Information

Highest Level Owner

Information not Available

Immediate Level Owner

Information not Available

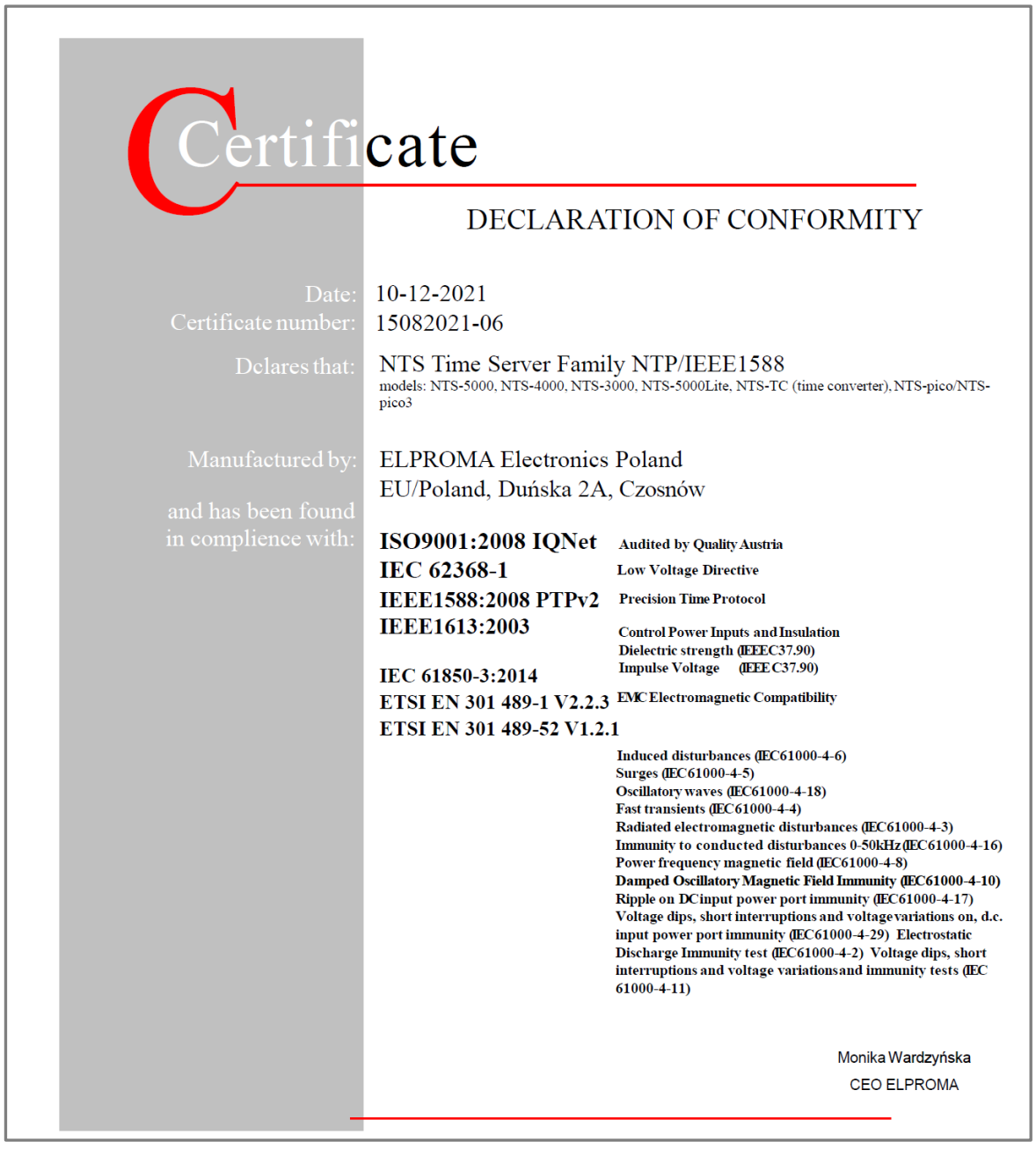
List of Offerors (0)

Information not Available

Additional Information

CAO-PAY

CE CERTIFICATION



Certificate

DECLARATION OF CONFORMITY

Date: 10-12-2021
Certificate number: 15082021-06

Delares that: NTS Time Server Family NTP/IEEE1588
models: NTS-5000, NTS-4000, NTS-3000, NTS-5000Lite, NTS-TC (time converter), NTS-pico/NTS-pico3

Manufactured by: ELPROMA Electronics Poland
EU/Poland, Duńska 2A, Czosnów

and has been found in complience with:

ISO9001:2008 IQNet Audited by Quality Austria
IEC 62368-1 Low Voltage Directive
IEEE1588:2008 PTPv2 Precision Time Protocol
IEEE1613:2003 Control Power Inputs and Insulation Dielectric strength (IEEEC37.90) Impulse Voltage (IEEE C37.90)
IEC 61850-3:2014
ETSI EN 301 489-1 V2.2.3 EMC Electromagnetic Compatibility
ETSI EN 301 489-52 V1.2.1

Induced disturbances (IEC61000-4-6)
Surges (IEC61000-4-5)
Oscillatory waves (IEC61000-4-18)
Fast transients (IEC61000-4-4)
Radiated electromagnetic disturbances (IEC61000-4-3)
Immunity to conducted disturbances 0-50kHz (IEC61000-4-16)
Power frequency magnetic field (IEC61000-4-8)
Damped Oscillatory Magnetic Field Immunity (IEC61000-4-10)
Ripple on DC input power port immunity (IEC61000-4-17)
Voltage dips, short interruptions and voltage variations on, d.c. input power port immunity (IEC61000-4-29) Electrostatic Discharge Immunity test (IEC61000-4-2) Voltage dips, short interruptions and voltage variations and immunity tests (IEC 61000-4-11)

Monika Wardzyńska
CEO ELPROMA

Configure In 5 Minutes

1. QUICK INFO – About

Thank you for choosing ELPROMA. Here are a few important steps to get started with your ELPROMA NTS-3000, 4000, or 5000 timeserver (referred to as the NTS-x000 in this manual).

Company Website
Visit our main website at https://elpromaelectronics.com for general information and resource

General Inquiries
For general information, you can reach us at info@elpromaelectronics.com.

Sales Department
Contact our sales team at sales@elpromaelectronics.com for purchasing and product details.

Technical Support
For technical support, please reach out to support@elpromaelectronics.com and include your server model and serial number to help us assist you efficiently. You can also visit support.elpromaelectronics.com for further support resources

Firmware Updates
Download the latest firmware updates from our repository at cloud.elpromaelectronics.com/index.php/s/NTS-Firmware

Newsletter
Stay updated on new firmware releases, software patches, and company news by subscribing to our newsletter at newsletter.elpromaelectronics.com

2. QUICK INFO – Introduction to NTS series

This manual cover ELPROMA time servers (shortly **NTS-x000**): **NTS-3000, NTS-4000, NTS-5000, NTS-5000LITE, NTS-9000), NTS-TC** time converter**.**

All servers are STRATUM-1 NTP time servers. The support all versions of NTP, SNTP including NTPv4 NTPv3. They automatically increase STRATUM level to STRATUM-2, STRATUM-3… when to synchronised to another NTS-server. All servers are simultaneously a PTP IEEE1588 GrandMasters and they can operate Sub-Master or Slave (Client). Servers supports both IPv4 and IPv6.

Both protocols NTP and/or PTP IEEE1588 are served parallelly. They are synchronized to STRATUM0 sources of UTC. The default ref. source of time is GNSS L1 carrier supporting GPS + GLONASS. Other satellite systems as BEIDOU* or GALILEO* are optional.

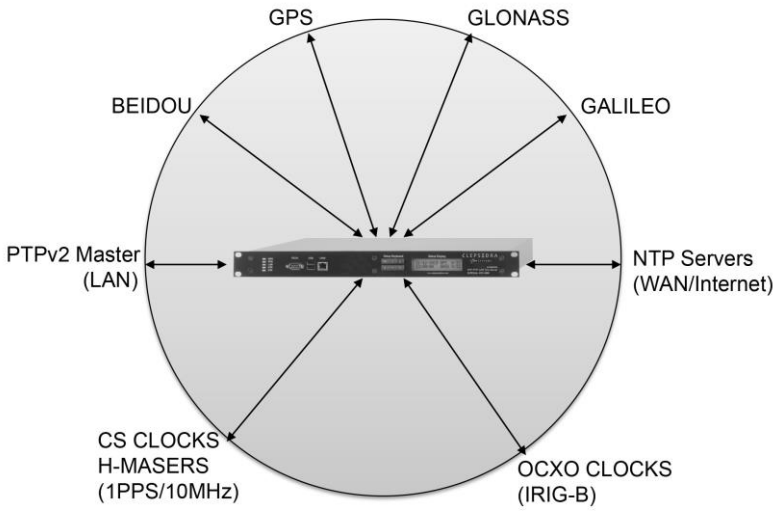
Servers can be also synchronized to any other local or remote UTC ref. clocks using additional I/O interfaces: 1PPS (PPM*, PPH*), 10MHz, IRIG-B AM or DCLS, IBM SYSPLEX. Other not std. interfaces are available on request too.

The main difference between models is a built-in ***holdover*** (HO) ***oscillator*** (OSC) type. Oscillator ensures synchronization continuum when timeserver cannot receive GNSS satellite signals. To operate in HO mode, the OSC must be synchronized to GNSS first. Please ref. to begin of this manual to understand holdover operation.

Server model **NTS5000/NTS5000LITE** optionally supports additional **Expander 1-4** Network Interface Card. Each Expander NIC supports 2x GE Ethernet with low level hardware timestamping. Cards are 100% information isolated from each other. Expander nr. 1 (NIC) is very special one. It can operate in Slave mode for synchronization to other PTP IEEE1588 devices. The hardware PHY timestamping ensures ultra-high accuracy of synchronization represented in level of tens of nanoseconds [ns].

All Elproma servers support simultaneously I/O inputs providing ref. sources of UTC time. However, only one reference is taken in time following user-definable PRIORITY TABLE and other stays ready for backup. There is a special priority management system in the WEB SETUP that is letting you maintain all resources and its priorities. Time ref. sources can be defined into 3 groups of ref. time:

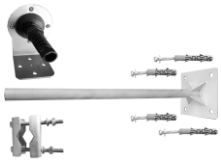
1) **GNSS** using sub-systems*: GPS, GLONASS, GALIELO*, BEIDOU**
2) **NETWORK** using protocols: *NTP, PTP IEEE1588*
3) **LOCAL CLOCKS** using signals: *PPS, RS-232, RS-485, IRIG-B*



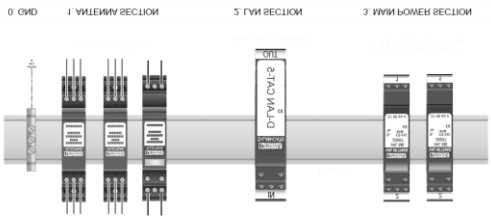
Elproma Time Servers are unique – they take ref. time simultaneously from all available I/O sources

3. QUICK INFO – Product at arrival

Standard product pack includes:

1.	NTS-x000 Network Time Server	1pcs.	
2.	NTS-antenna w/ built-in GNSS receiver	1pcs.	
3.	Roof Mounting Kit Incl. mast H=0,5m, Set of screws, handlers etc.	1set	
5.	Ethernet patch cord UTP cat. 5 (2m)	2pcs.	
6.	Power cable (1.5m)	1pcs.	

Extra options* (need to be ordered separately):

a.	2nd NTS-antenna	extra 1pcs.	*(see above table)*
b.	2nd Roof Mounting Kit	extra 1set.	*(see above table)*
c.	NTS-protect surge/overvoltage arresters	1 set.	
d.	FO-01 Converter electric-2-fibber	2pcs. (1set)	

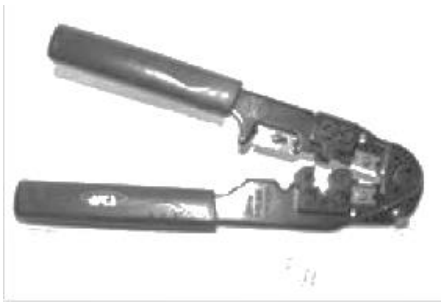
Important Notes!

The antenna cable is not included to product and should be purchased locally (min UTP or STP cat 5).
Manual and software need to be downloaded from web page www.elpromaelectronics.com.

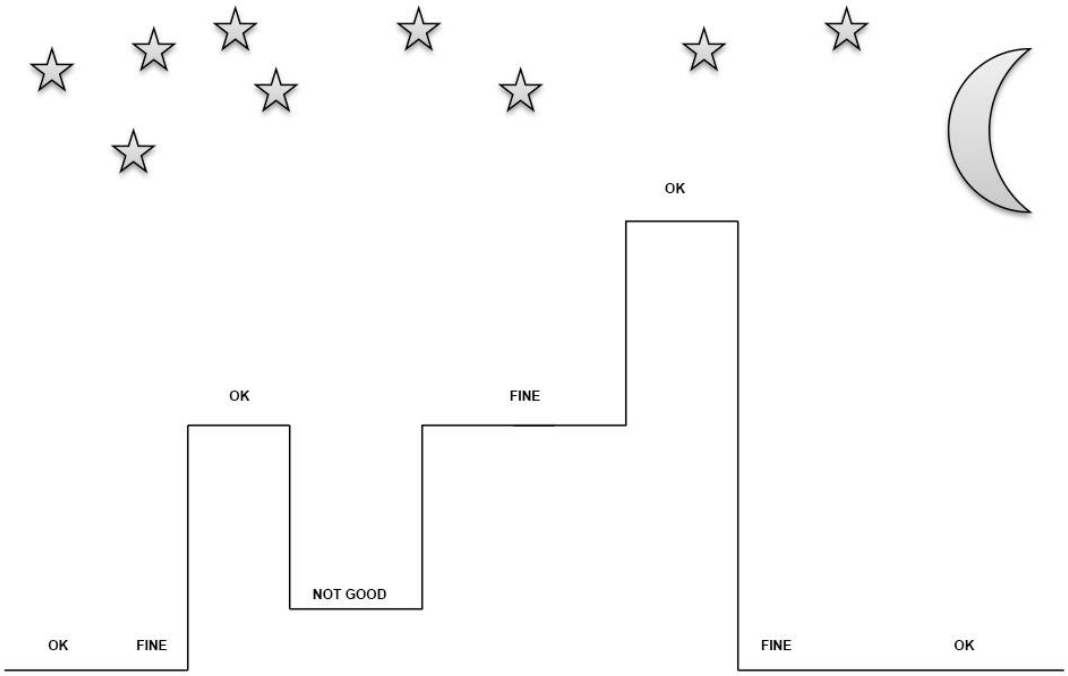
4. QUICK INFO – Installing hardware

Quick unpacking/mounting steps:

1. Remove all parts from shipped box. Prepare additional tools: (1) RJ45 connectors (pcs.2), (2) UTC/STP cable cat.5 or above (not included to shipment), (3) Ethernet crimping tool, (4) screwdriver & scissors.



2. Always mount GNSS receiver (NTS-antenna) on the top point of the roof of building. Antenna should access possible a 360^{o} sky view (unobstructed view of the sky) to receive all available, not reflected satellite signals. Do not mount GNSS receiver: on the building wall, on chimney, near electric engines (e.g. air-condition). Always avoid reflections from any other structures. The minimum recommended distance from other antennas is at least 2 meters.



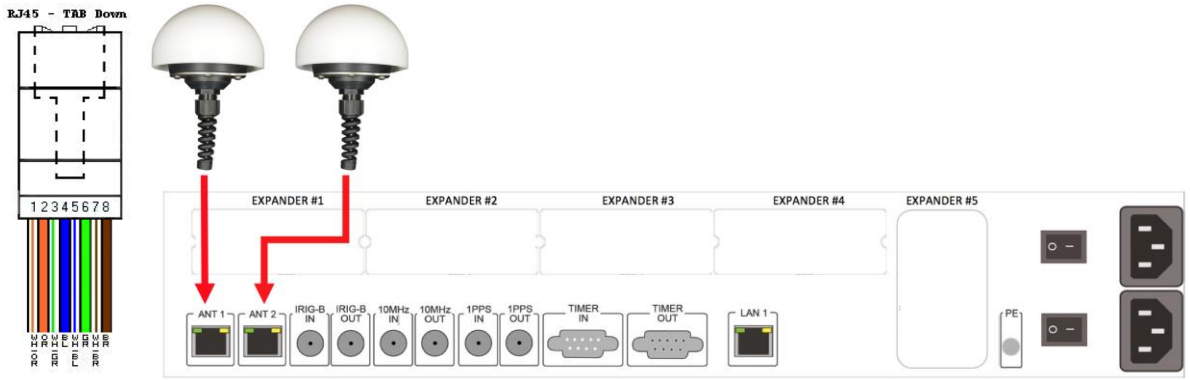
3. Lunch UTP (STP) antenna cable down to datacenter room. Measure and note a total length of used a cable for future signal delay compensation (4ns/m to be set at server www setup-level). Cables should not be located in direct neighborhood to any power line. Well done cable installation should be tested for connectivity and resistance before using. Ensure that building fire regulations do not volatile. Always consider using overvoltage protection and surge arresters.

4. Mount NTS-surge protection on the back of rack'19 shell. Ensure, it is properly grounded to PE line (yellow-green marked). Ask, certified authority to assist you at this step, especially if you are not qualified for electric installations. Always read all safety instructions first!

5. Crimp RJ45 connectors to terminate antenna cables at time-server side and test connections.

6. Locate Time Server in rack”19 shell. Please keep min. 1U space to neighborhood other products that can unexpectedly hit your NTS-x000 timeserver from top and bottom surface.

7. The default setting assumes there are 2x antennas connected to NTS-server. If you use one antenna, please disable the 2nd antenna from device setup level.



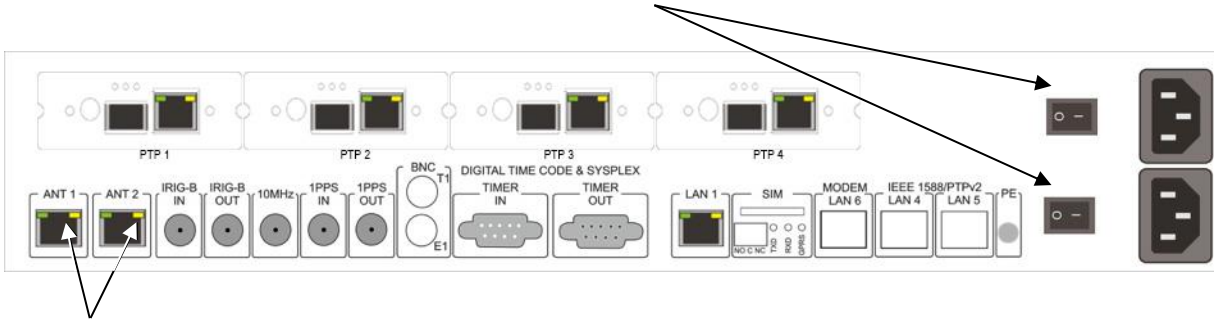
ANT-1/ANT-2 RJ45 (pin)	Signals	Std. UTP cable color
1	PPS+	White/Orange
2	PPS-	Orange
3	ToD+ (TR+)	White/Green
4	JAM/SPF- (or DCF-)	Blue
5	JAM/SPF+ (or DCF+)	White/Blue
6	ToD- (TR-)	Green
7	+VCC (+24VDC)	White/Brown
8	0V	Brown
GND	GND	Not used

ANT-1/ANT-2 interfaces can be configured individually from setup level

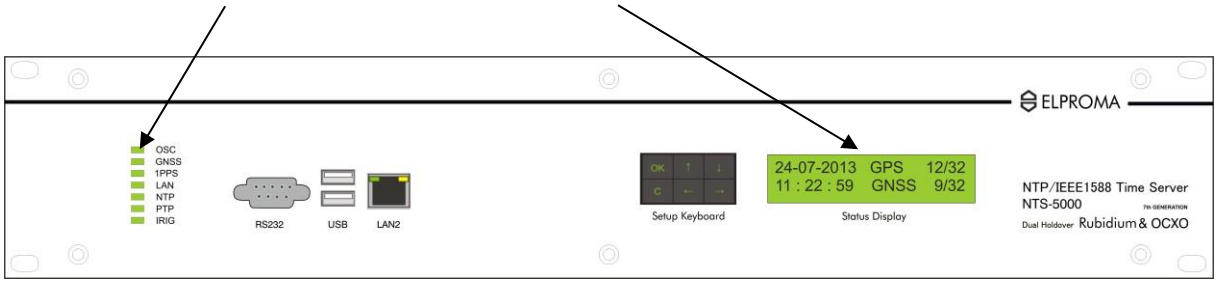
- **INPUT** supplying ref. time to NTS antenna from GNSS and/or DCF
- **OUTPUT** emulating NMEA183 to another server
- **OFF** - port is disabled

5. QUICK INFO – Powering Server OFF/ON

Turn ON the power switch located on the back panel of NTS-x000 server. In case of redundant power each power supply has own ON-OFF separate **switch**.



The ANT1/ANT2 RJ45 YELLO LED starts pulse (PPS) max. 1 minute after switching power ON. Typical firmware start-up time duration takes 1 minute, but this can take longer too. Firmware BOOT progress can be **traced on front panel 6x LED** and **2x20 LCD display** of front panel.

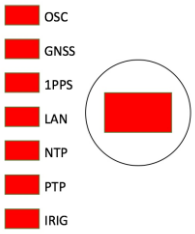
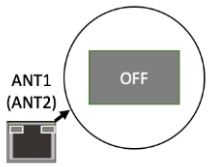
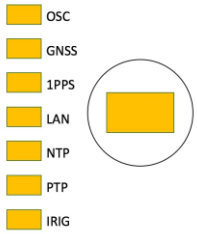
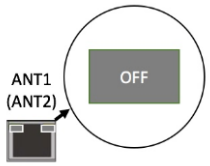
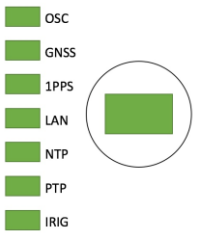
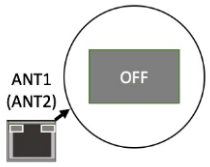
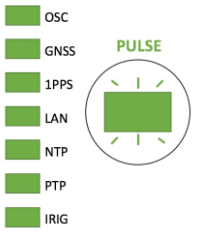
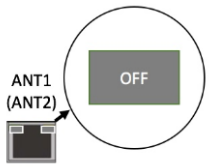
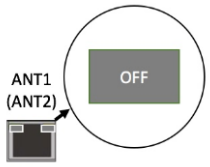
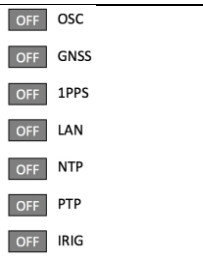
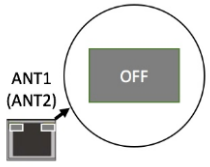


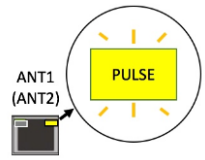
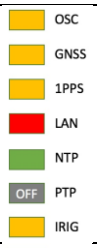
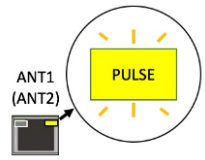
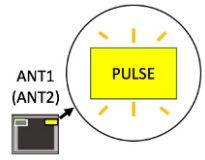
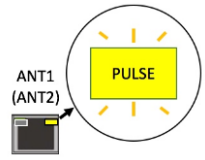
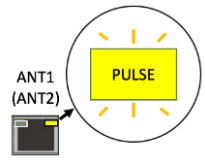
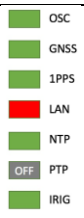
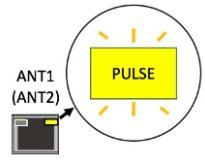
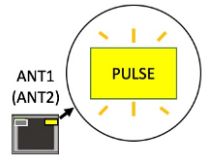
Observe LCD and LED during BOOT process. Ensure GNSS synchronization is indicated by OK status (LCD) and green color LED too.

Use front panel KEYBOARD and SETUP device by entering LAN1-2 basic IPv4 configuration.

6. QUICK INFO – LED Indicators On Booting

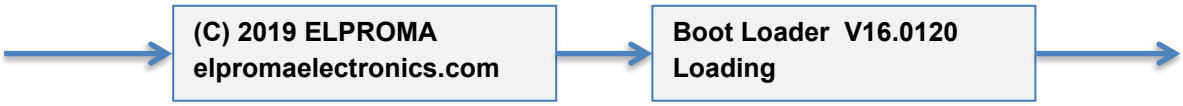
Following **boot sequence** can be observed:

#Lp	*Process*	*Time duration*	*6x LED (Front Panel - left)*	*LCD display (Front Panel right side)*	*ANT1/ANT2 (Back Panel)*
1	OFF-ON	1s		**(C) ELPROMA** **elpromaelectronics.com**	 Yellow LED is OFF
2	HW INIT	1s		**(C) ELPROMA** **elpromaelectronics.com**	 Yellow LED is OFF
3	SW INIT	1s		**Boot Loader V16.0120** **Loading**	 Yellow LED is OFF
4	BOOT LOADER	<1min (60s)		**Loading NTS-5000** **.....**	 Yellow LED is OFF
5	OS INIT	<5s		**Press & hold [OK]** **to enter setup**	 Yellow LED is OFF
6	OS READY	<2s		**Press & hold [OK] [C]** **to reset to defaults**	 Yellow LED is OFF

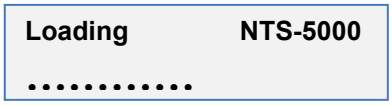
7	NET INIT	<2s		**15-06-2019 OK** **17:17:37 SAT A=0/0** GNSS RECEIVEING IF YELLO LED PULSE 1PPS	 Yellow LED pulse
8	NTP READY LAN Link (-)	+1min (+60s)		**15-06-2019 INIT** **17:17:37 SAT A=0/0**	 Yellow LED pulse
9	GNSS READY	+6min (+360s) max		**15-06-2019 OK** **17:17:37 SAT A=17/30** *ToD millisecond accuracy of synchronization has been started*	 Yellow LED pulse
10	1PPS READY	+6min (+360s) max		**15-06-2019 OK** **17:18:47 SAT A=19/30** *Microsecond [us] to nanosecond [ns] high accuracy of 1 PPS synchronization has started now*	 Yellow LED pulse
11	IRIG READY	+2min (+180s) max		**15-06-2019 OK** **17:18:47 SAT A=19/30**	 Yellow LED pulse
12	OSC READY	+10min (+600s) max		**15-06-2019 OK** **17:18:47 SAT A=19/30**	 Yellow LED pulse
13	ETH Link (+) LAN1 or LAN2			**15-06-2019 OK** **17:18:47 SAT A=19/30**	 Yellow LED pulse

7. QUICK INFO – Panel Keyboard SETUP

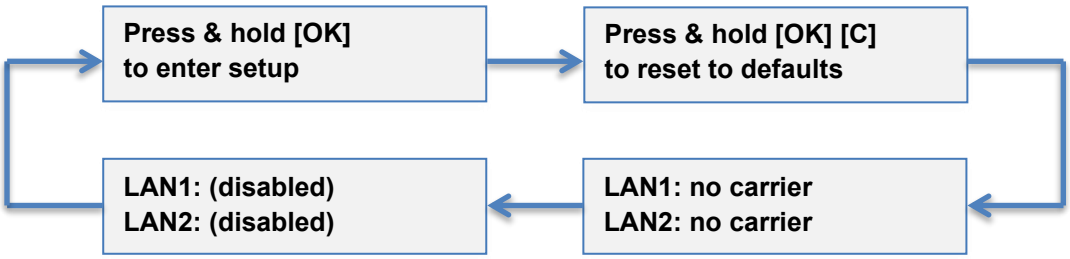
After **switching ON** power the following screen sequence will appear on LCD display:



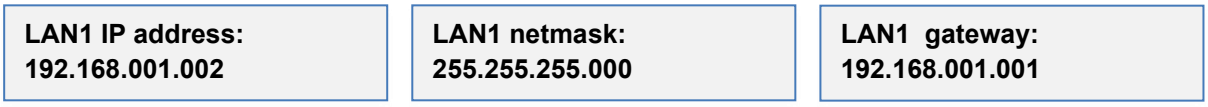
When booting, the following message will be displayed while dots indicates booting progress:



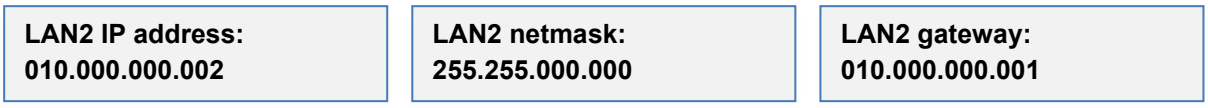
You are able to configure the IPv4 address only for LAN1 and LAN2 using the front panel keyboard. Any additional LAN interfaces available on different models, can be configured through the web interface or via WWW or SSH.



Press & hold [OK] for min. 5s. The **LAN1** IP address will appear on LCD. Use arrow keys **[←→]** to select IPv4 position, and **[↑↓]** to assign requested value 0-9.



Press **[OK]** to switch to next screen or ***press & hold*** **[OK]** for 5s to save configuration. You can always interrupt and quit SETUP w/o saving at any moment by ***pressing & holding*** **[C].** Repeat above steps to configure LAN2 IP address:



Once IPv4 address is set, the following screen request is displayed to save setting:

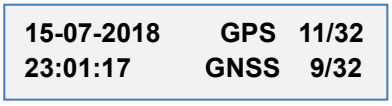
Now NTS-x000 timeserver is ready to communicate via LAN1 (LAN2). Unless you like to provide more advances setting, the above simple IPv4 configuration is the minimum required to start working server.

If the GNSS receiver remains not synchronized the following INIT information will be displayed on LCD:

Once more than 3 satellites are in view, the GNSS receiver is ready and synchronization is pending:

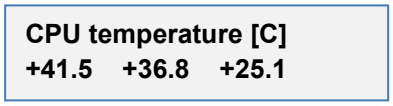
If you use 2 redundant GNSS receivers (Ant1 & Ant2), additional information will be displayed too for B:

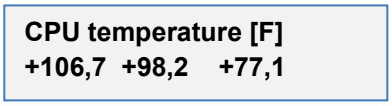
It is frequently that both GNSS receivers can show a different volume of visible satellites.

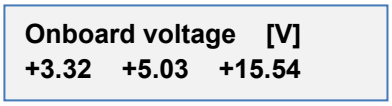


Following additional information can be provided any time:

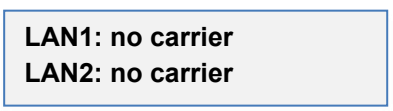
Environmental DATA is provided periodically:

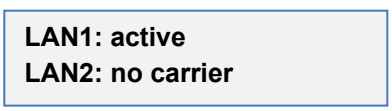






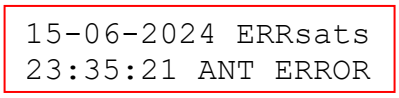
Plugging Ethernet cable to LAN1 will trigger Link(+) and following message will be displayed on LCD:





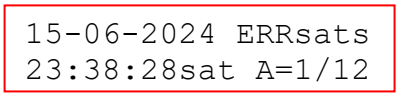
8. QUICK INFO – LCD Messages

If there is **no antenna** connected to server, the following error screen is displayed on LCD front panel:



Error: no antenna detected, antenna error or cable connection is broken

Time server is requiring min. 3 satellites in order to set localization and time from GNSS. If it receives less than 3 satellites or quality of satellite signals is not good enough, server will display ERRsats with specific number of visible satellites at receiver A or B:



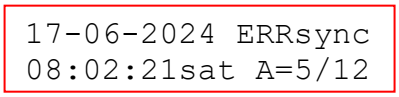
Error: missing GNSS satellites or bad GNSS geometry (should be min 5-sat visible)

Nevertheless, in both above cases the NTS-x000 automatically switch to HOLDOVER mode. In HOLDOVER mode, a time is not provided from GNSS but from built-in oscillator OSC (OCXO or RUBIDIUM – if supported). The Rubidium (Rb) is available for NTS-5000 only. NTS-4000 supports OCXO. Standard version of NTS-3000 does not include any oscillator and therefore it does not support HOLDOVER mode.

To provide accurate time in HOLDOVER mode, oscillators (OCXO and Rubidium) must be synchronized to GNSS first. If server has never reached synchronization to GNSS, the oscillators reminds FREE-RUN mode and they cannot be use. The NTS-x000 state machine never use oscillators when previously not synchronized to GNSS. However, if HOLDOVER mode is overdue, the oscillator can drift providing growing large error to UTC. In some cases, the time overdue is also called a FREE-RUN mode.

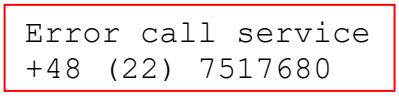
The LCD shows only a status of the GNSS antennas. It does not show status of the other time sources like 1PPS, IRIG, SYSPLEX etc. However, all other time ref. UTC sources can be traced remotely using built-in software (**ntpq).** The **ntpq** is built-in to NTS server and can be accessed by SSH/TELNET setup.

Another kind of “ERR sync” message is possible, if a quality of received satellite signals is not fine enough. This problem might happen when GNSS signal is noisy, reflected or jammed/spoofed.



Error: GNSS not in sync mode

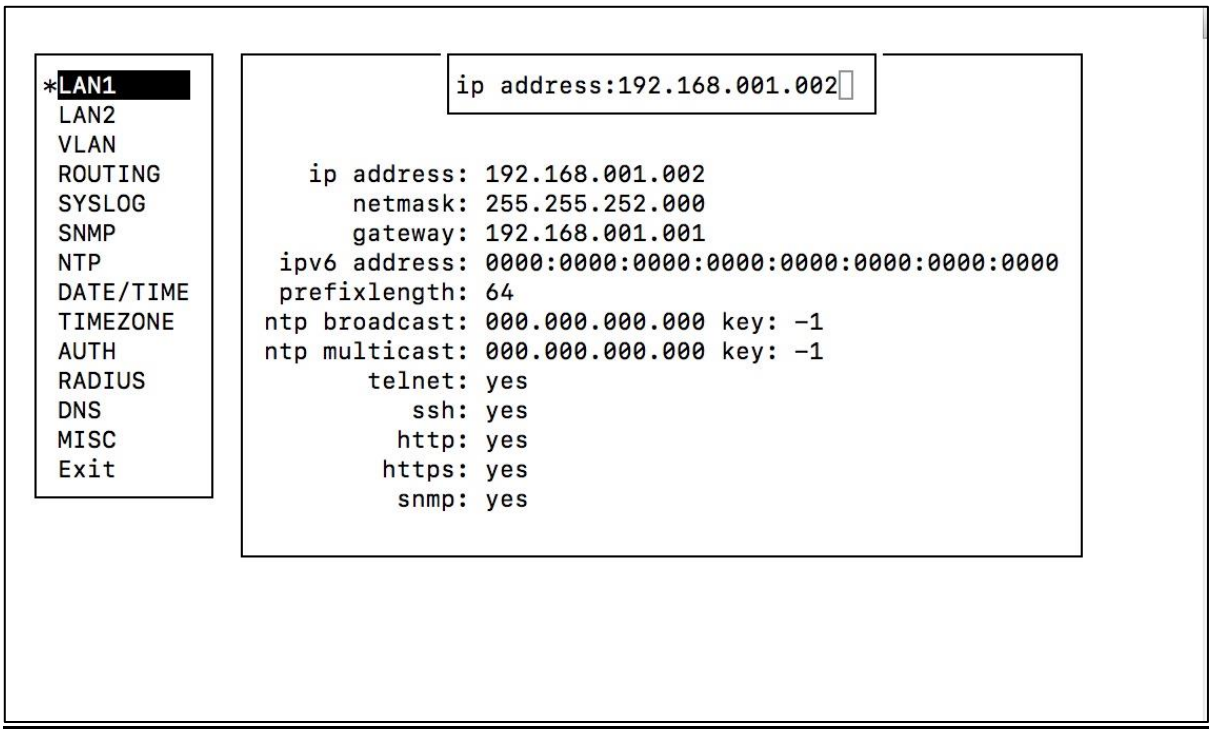
The last, but not least is critical error message - **“Error call service”**. It highlights device is not operating.



Error: Device out of order

9.QUICK INFO – Software Setup LAN (SSH)

NTS-x000 configuration can be done using **LAN1** or **LAN2** network interface**.** This also including the configuration of LAN3-LAN10 (Expander1-4) interfaces of NTS-5000/TC models. We recommend to use SSH protocol. The factory defaults for software SETUP are: *Username* -> ***admin***; *Password* -> ***12345***



Since, PTP LAN3-LAN10 expanders (only for platform 0) interfaces are physically isolated from each other, the Expander 1-4 configuration goes in special protected mode and via LAN1-LAN2. To configure PTP LAN3-LAN10 please select PTP:

The new setup (different color) screen appears after selecting PTP item from main setup menu. Different color indicates fact that you have entered the security zone of NTS-5000/TC. New menu style includes automatically recognized Expander 1-4 NIC cards. Cards are numbered: PTP1 (Expander 1), PTP2 (Expander 2), PTP3 (Expander 3), PTP4 (Expander 4). Only cards that are recognized by NTS system are displayed.

You will need to configure each 1-4 Expander NIC card separately. Each card includes 2 independent network interfaces: 1x electric (RJ45) and 1x SFP – that can be set to operate fiber-optic or electric Ethernet signals. The Expander 1-4 NIC are numbered:

Expander #1 supported by: NTS-5000, NTS-TC
LAN3: RJ45 electric GE interface
LAN4: SFP fiber or electric GE interface

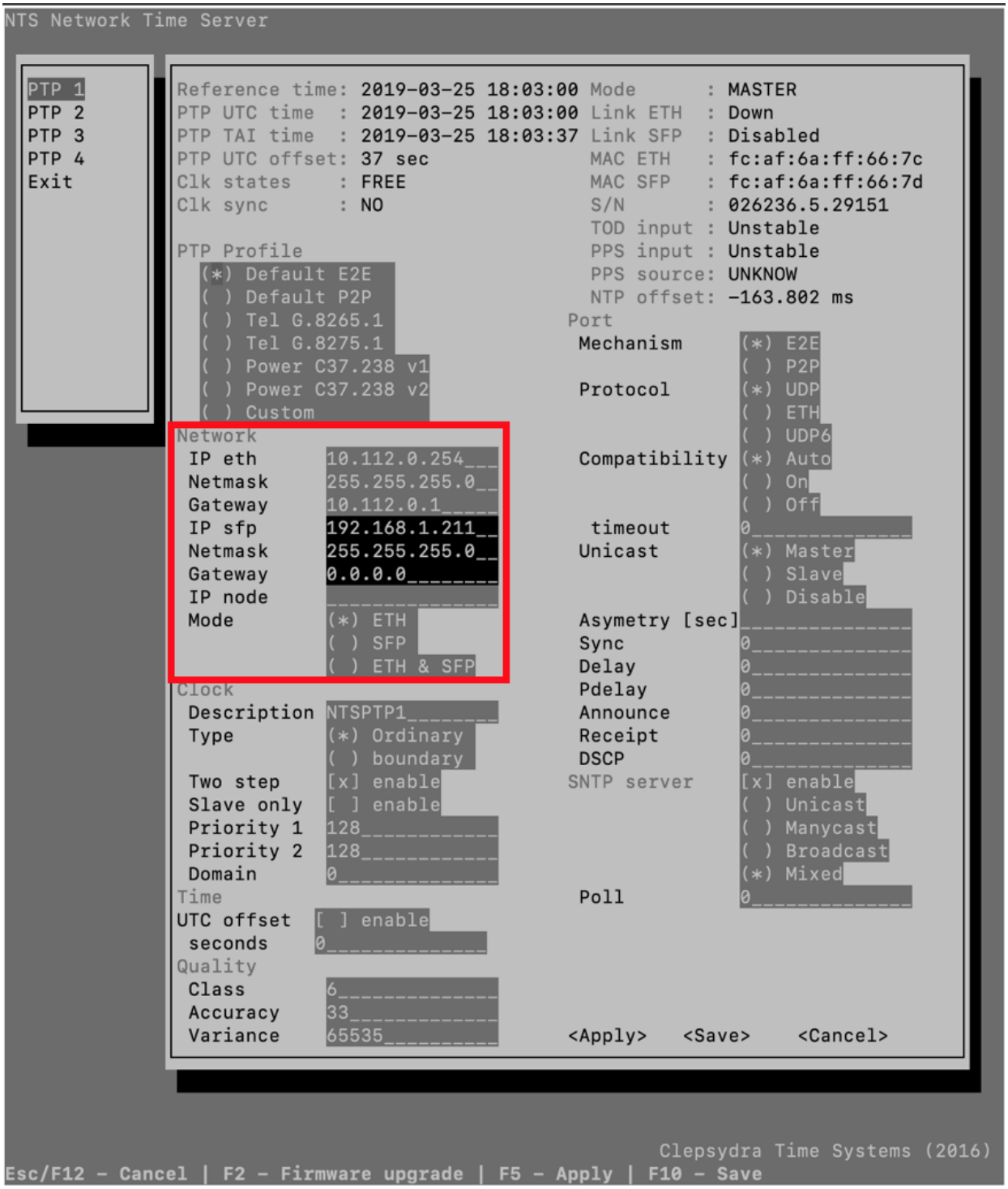
Expander #2 supported by: NTS-5000, NTS-TC
LAN5: RJ45 electric GE interface
LAN6: SFP fiber or electric GE interface

Expander #3 supported by: NTS-5000 only
LAN3: RJ45 electric GE interface
LAN4: SFP fiber or electric GE interface

Expander #4 supported by: NTS-5000 only
LAN5: RJ45 electric GE interface
LAN6: SFP fiber or electric GE interface

Each of LAN3-LAN10 (Expander 1-4) network interface supports own: IP, MASK and GATEWAY. If GENTEWAY is not used please keep field empty (filled by zero). Each of Expander 1-4 NIC is independent microprocessor MASTER with own CPU, RAM, IP-stack and PTP-stack.

Example IP configuration of Expander #1 (LAN3-LAN4).
The LAN3 is labeled ETH
The LAN4 is labeled SFP

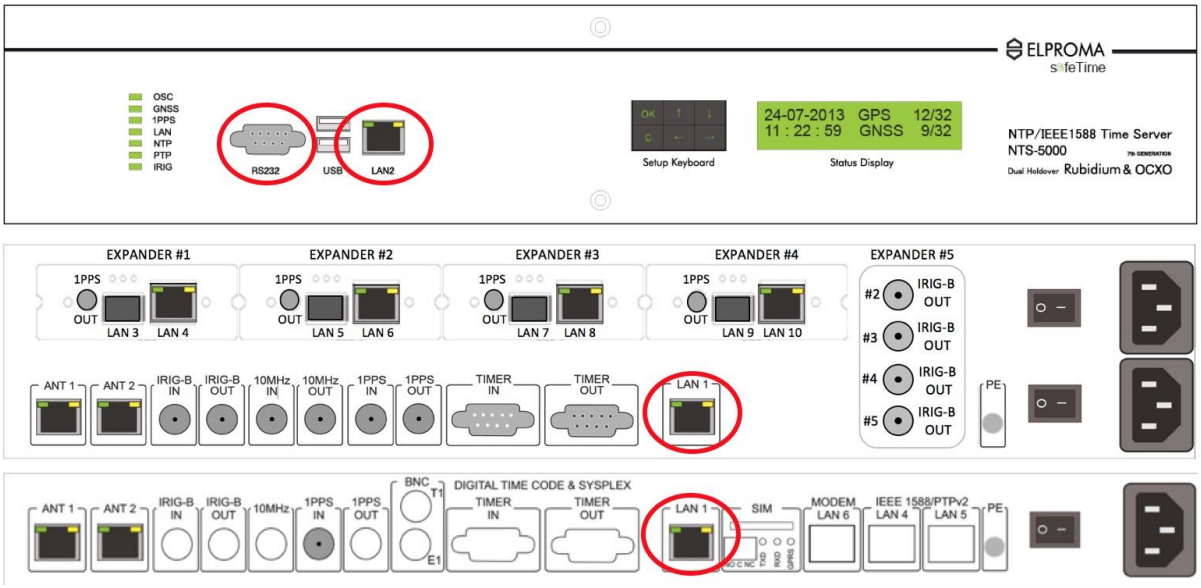


Expander #1 configuration view (SSH setup via LAN1 or LAN2)

10. QUICK INFO – Troubleshooting

Problems with PC communication to server.

If any problem with LAN1 or LAN2, the software SETUP can be executed via **RS232** *(front panel)*
Always keep note, only one interface (LAN1, LAN2, rs232) can be exclusively used for SETUP in time.



Only front panel RS232 & LAN2 or back panel LAN1 can be used for text mode terminal SETUP configuration.

For RS232 terminal communication, please use cross serial cable and connect it to DSUB-9 front panel connector. Please use on PC following serial configuration set to: **9600, 8, 1, N**.

WARNING! You cannot access SETUP using PTP LAN3 - LAN10 (NTS-5000 and LITE only. Expander 1-4).

Note! *For Microsoft Windows operating system you might like to choose PUTTY software available FREE to download from: http://www.putty.org . To ensure displaying correct character set, please choose in configuration Category->Window->Translation->Remote Character Set the correct setting to your region. In case e.g. of Central European the correct options will be Win1250 (Central European)*

The factory default setting is:

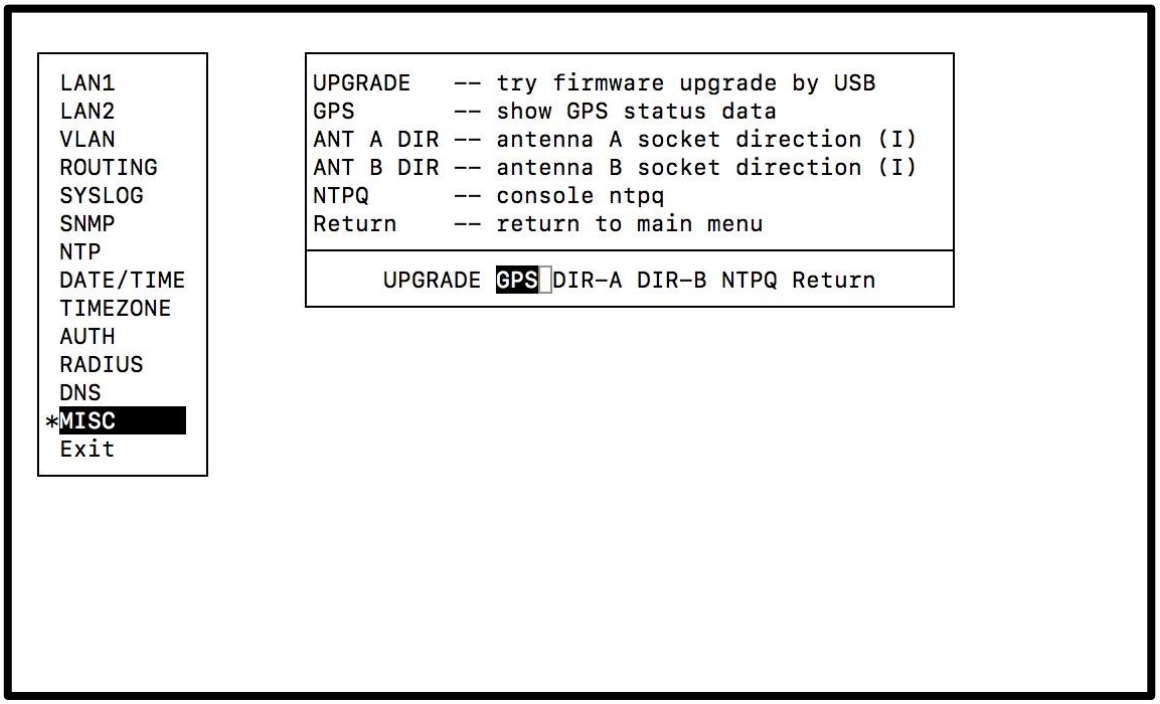
Username: **admin**
Password: **12345**

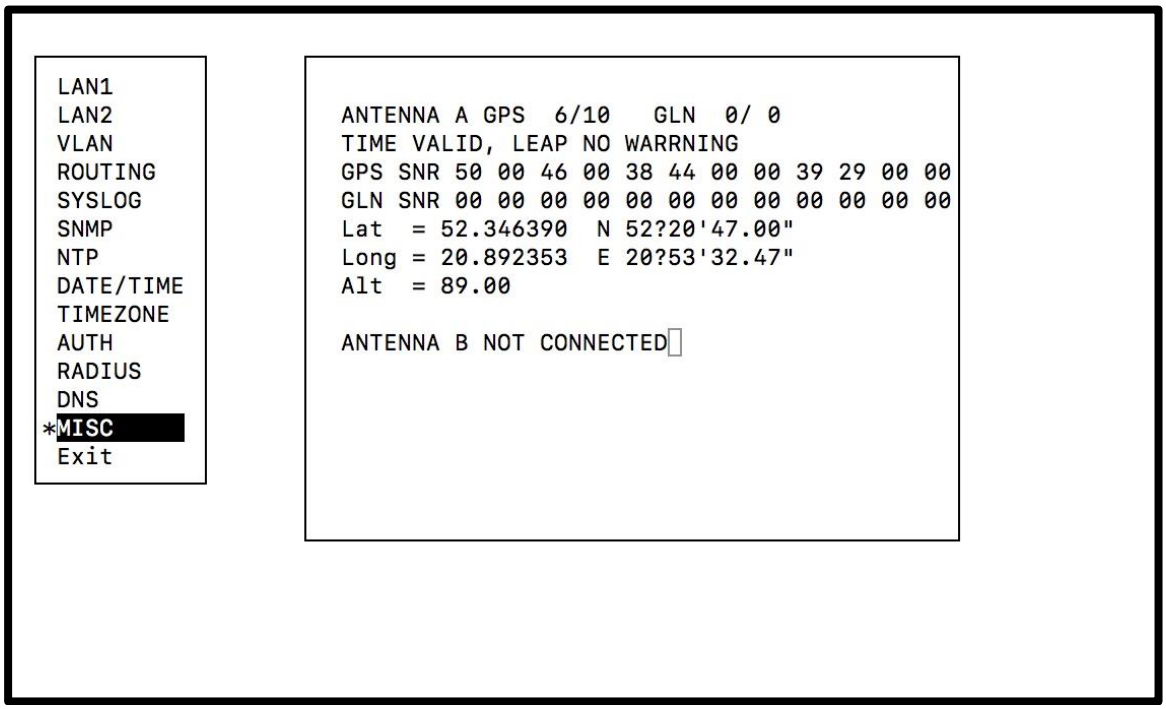
Problems with 2 antennas connected to server (very important)

If using 2x redundant antennas simultaneously, please set 1st to BIN mode (DIR-A sub-menu), and 2nd to NMEA text mode (DIR-B sub-menu). Otherwise both antennas can be marked 'x' (FALSETICKER).

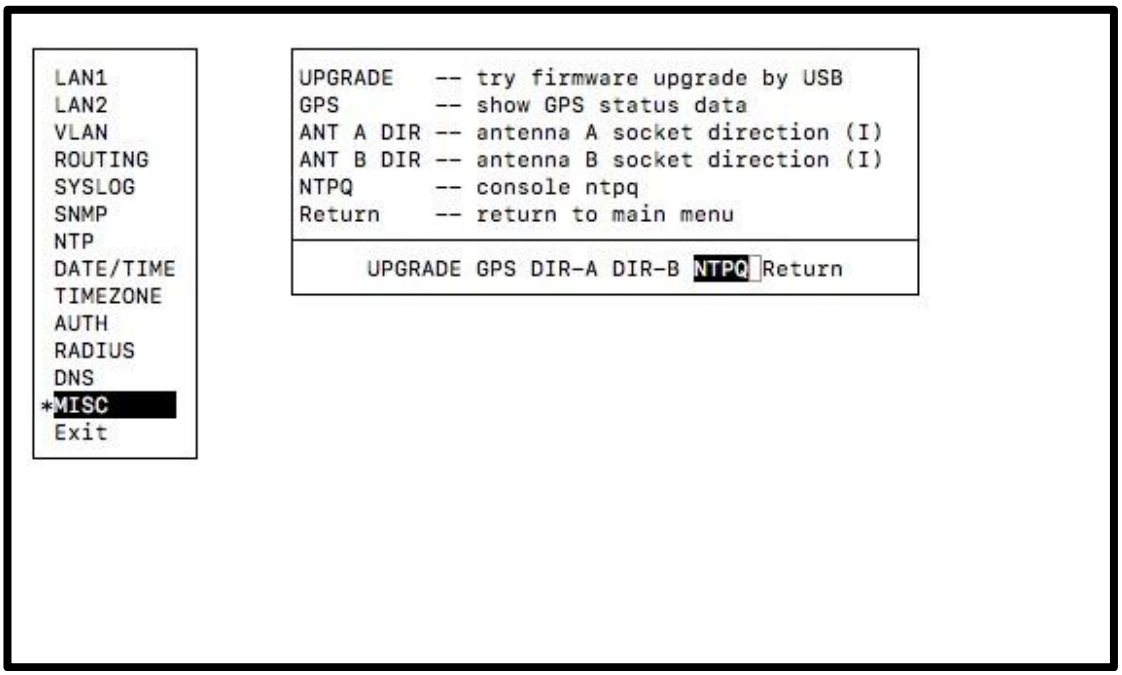
Tracing visibility of satellite signals

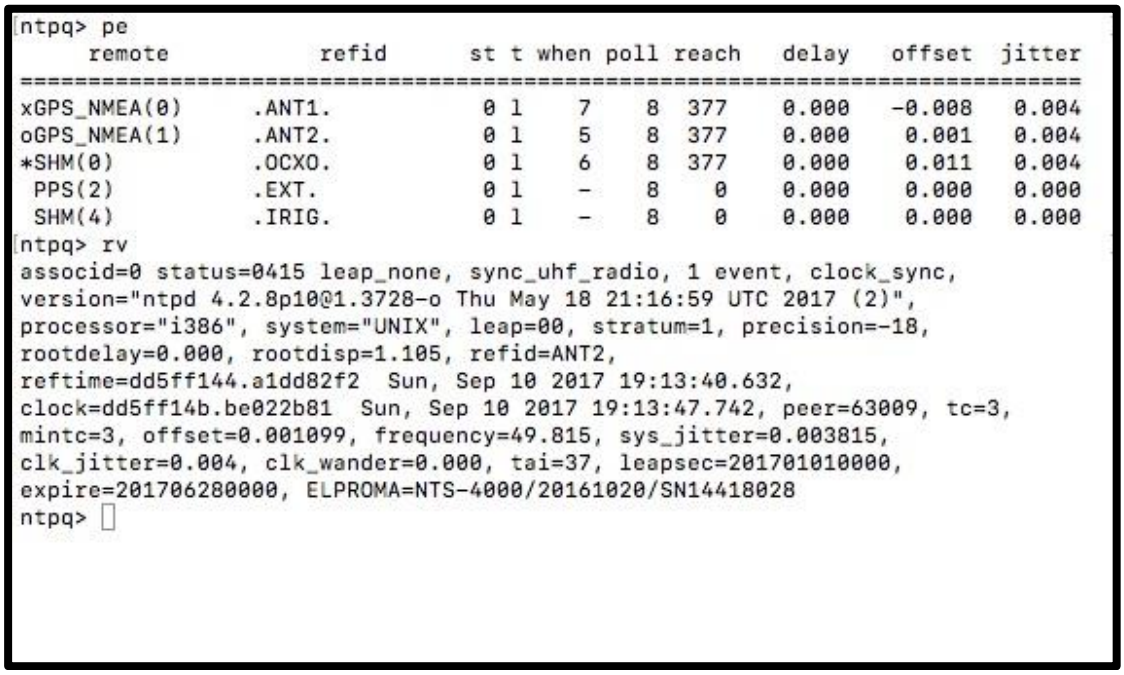
To trace satellites signals, please choose MISC and then GPS option. You should be able to observe at least min. 5 satellites otherwise synchronization to GNSS is not pending and server is FREE-RUN.





If GNSS connection is OK, you should see the screen similar to above. If values of signal strength are zero (00) it means GNSS receiver is not receiving signals. In such case please recheck antenna installation and restart (power OFF-ON) server. Once the strength is no-zero value, it is good to select NTPQ menu and trace NTP internal synchronization. The description of using NTPQ is not a part of this manual and can be find at site *www.ntp.org*





Tracing time ref. resources inside NTS time server using built-in NTPq diagnostic

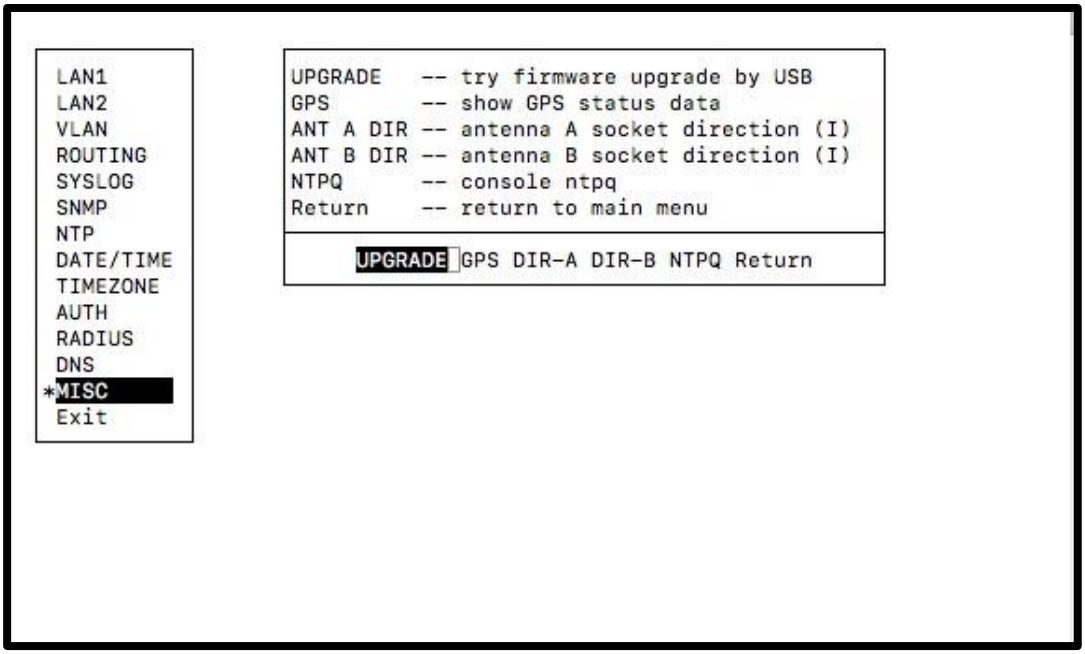
Normal operation of server (when antennas are installed correct, and the receiver is decoding satellite signals fine) the REACH column of NTPQ should not be zero (0). After several minutes of server being uptime this octal value should REACH number 377. This means GNSS data is correct and the server synchronization is pending to GNSS. The synchronization is confirmed by displaying displays '*' or 'o' located at the very first column of a table. Once it is done, server starts to synchronize locak oscillators. It will take another 10-20min to synchronize first OCXO (NTS-4000), and another 10-20 minutes to do PLL on RUBIDIUM (Rb) oscillator (NTS-5000 only). A HOLDOVER oscillator is ready and locked (PLL/FLL) to GNSS once NTPQ "pe" command displays '*', 'o', '+' or '-' character at the very first column of a table. This means oscillator belongs to group of NTP Truechimers (time ref. candidate).

11. QUICK INFO – Updating Firmware

NTS-x000 firmware update can arrive neither on USB memory, or it can be downloaded from cryptographically protected cloud. The updating is using secured protocol SSH. For security reasons firmware updates are not available public and via web service. Any update needs serial number verification. If you are registered customer will be informed about new firmware and software patches releases by e-mail. Please ref. to very first chapter “QUICK INFO - About” for details how to register your e-mail and NTS-x000 product.

Below steps informs how to provide firmware update step by step, and using SSH protocols:

1. Prepare USB flash drive with minimum 128Mb free space (FAT32 formatted)
2. Download ***nts345.v-yymmdd.img*** file from cloud and copy it to root folder of USB flash drive
3. Plug-in to NTS-x000 front panel USB connector (upper or lower)
4. Login to NTS-x000 using **LAN1** or **LAN2** and SSH protocol
5. Go to **MISC** menu, and select **UPGRADE** submenu using arrow-keys
6. Follow information on the screen (do not interrupt upgrading process)
7. Once firmware update is done, please **EXIT** and **LOGOUT**
8. **VERY IMPORTANT**! Clear your web browser history and delete all cookies. Restart web broser.
9. Restart your timeserver (power OFF-ON) or make hardware reset
10. The new firmware version should be displayed on LCD after restarting



Server SETUP via SSH (display view)

Firmware release	
NTS-5000	**24/06/2024**

Note!

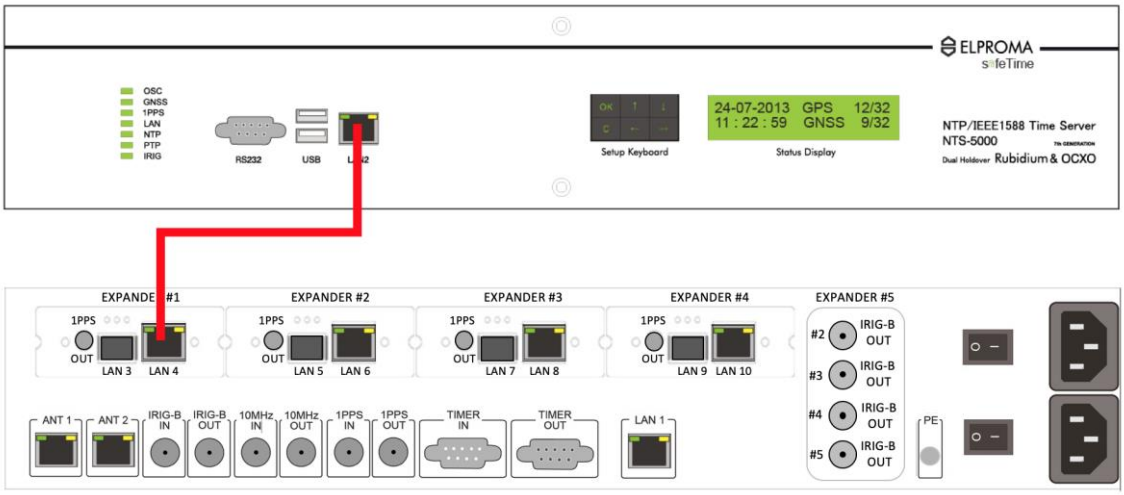
The firmware upgrades can be also provided via web browser GUI setup (www). For more details please ref. to SOFTWARE SETUP chapter.

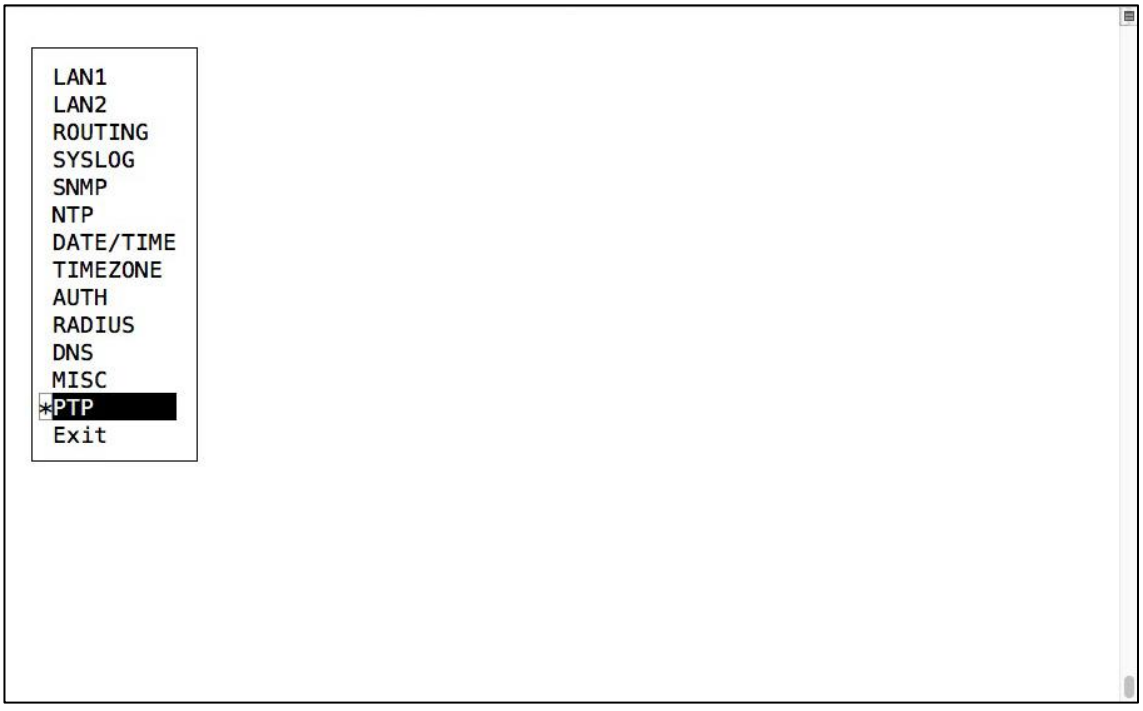
12. QUICK INFO – Updating Expanders 1-4

Disclaimer. This chapter is only for NTS-5000/NTS-5000LITE users who have purchased product equipped with special PTP EXPANDER 1-4 network cards. The strong cybersecurity nature of NTS-5000 forces all (max. 4) EXPANDER cards to be physically isolated (no TCP/IP communication) from each other and from main unit. Therefore, the site effect of isolation is fact that also PTP EXPANDER firmware updates need to be done on different and very special way, described below.

Before upgrading any Expander 1-4 card, please ensure your main unit has been successfully updated to latest firmware version.

IMPORTANT NOTE!
To update the firmware of Expander #1 network interface card you need to connect directly LAN2 of main server to LAN3 (SFP) or LAN4 (RJ45) first. Connection must be done directly. No intermedia Ethernet converters, switches, routers are allowed. For Expander #2 use connection LAN2->LAN6, Expander #3 LAN2->LAN8, Expander #4 LAN2->LAN10. Detected Expander 1-4 cards will appear in SSH setup:

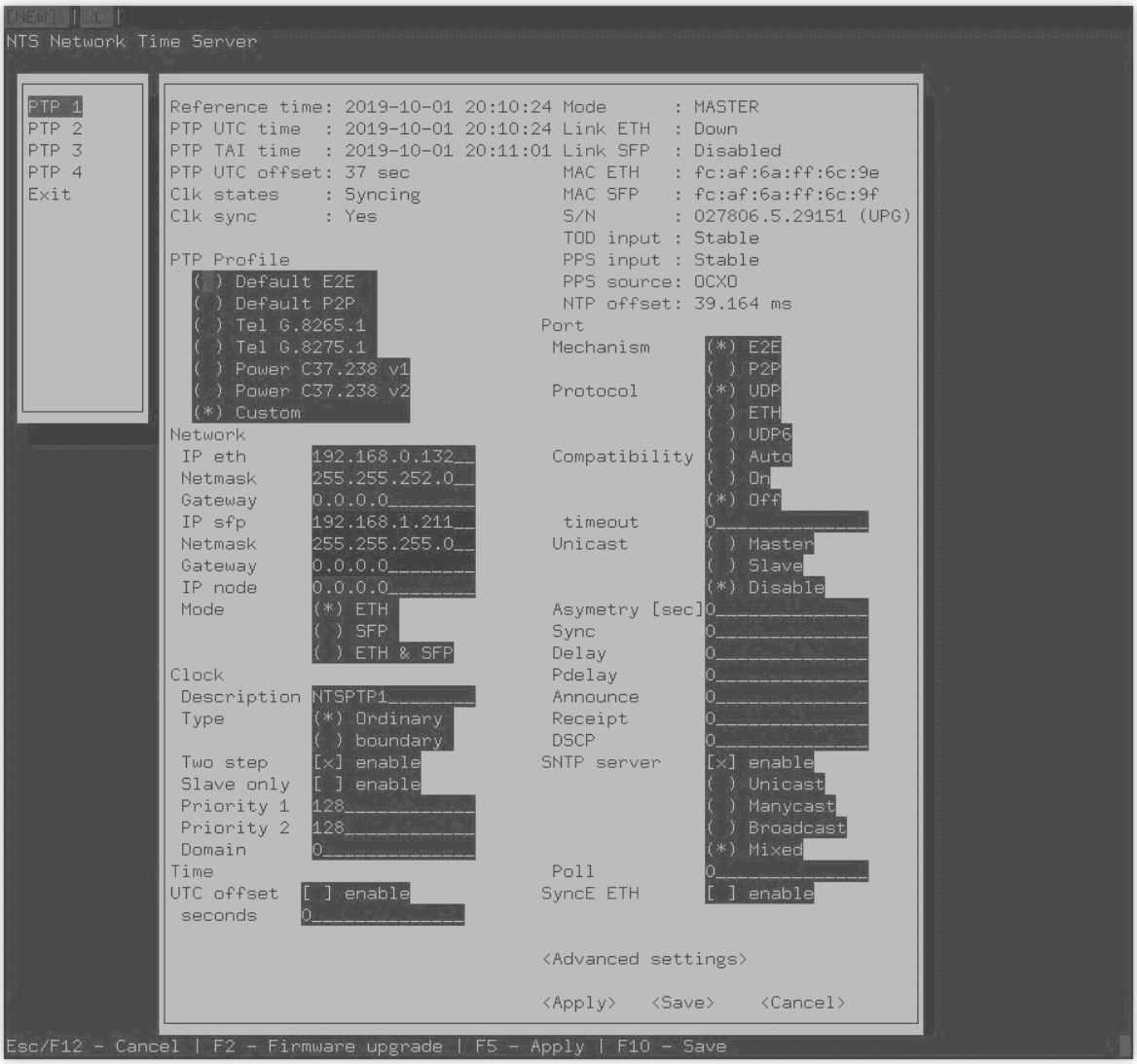


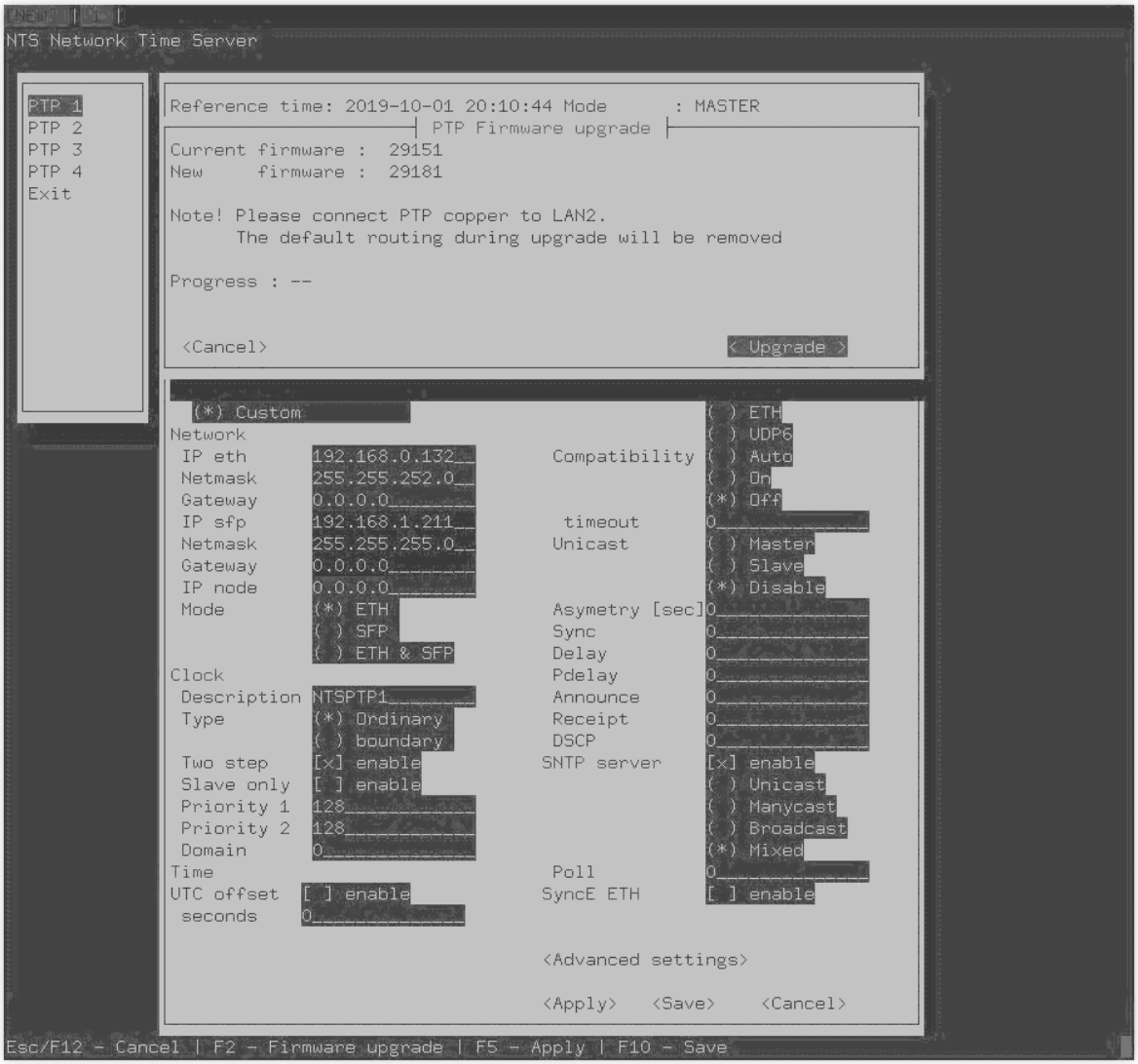


Please check S/N field first.

S/N: 027806.5.29151 - no firmware update available
S/N: 027806.5.29151 (UPG) - firmware update is available

If there is “(UPG)” flag just after the serial number. This indicates fact that your last NTS5000 main firmware update has included also extra sub0firmware update to be load to Expander #1. Please press F2 to start firmware upload.





How to read EXPANDER firmware rev. number.

There are 3 segments separated by colon e.g. S/N: 027806.5.29151 (UPG), so the constructor of firmware is **X.Y. Z** where:

X – is physical S/M of Expander module (027806)
Y- FPGA hardware type (4-M64, 5-M68, 6-M88)
Z – current rev. number of expander software firmware (29151)

Please repeat above steps for each Expander #card separately. Always use LAN2 of main unit to distribute firmware to specific expander.

13. QUICK INFO – Restoring Factory Defaults

Front panel keyboard view

Restoring Factory Defaults

Press & hold (at the same time) "OK" and "C" buttons, until following below message will be displayed on LCD.
Press "OK" one more time to RESET product and RESTORE factory defaults, or press "C" to abort the operation.
Following below message will be displaced on LCD and needs to be confirmed [OK] "Yes"

```
Are you sure?
[OK]-Yes [Cancel]-No
```

You need to confirm before restoring to factory defaults

Standard LAN1-LAN2 defaults:

LAN1: 10.0.0.210	MASK: 255.255.0.0	GATEWAY: 10.0.0.1
LAN2: 192.168.0.210	MASK: 255.255.255.0	GATEWAY: 192.168.0.1

Optional LAN3-LAN10 (NTS-5000 only) component settings:

LAN3:	192.168.3.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN4:	192.168.4.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN5:	192.168.5.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN6:	192.168.6.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN7:	192.168.7.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN8:	192.168.8.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN9:	192.168.9.210	MASK: 255.255.255.0	GATEWAY: <no value>
LAN10:	192.168.10.210	MASK: 255.255.255.0	GATEWAY: <no value>

Factory default user and password:

Username: **admin**
Password: **12345**

Software SETUP services defaults:

HTTP	ON
HTTPS	ON
SSH	ON
TELNET	OFF

Std. ref. time: **GNSS** (GPS/GLONASS only)

Interfaces:	Defaults	Available	NTS-x000 modes	rs485
Ant1 (Antenna "A")	INPUT	INPUT	(all)	RJ45
		OUTPUT	(NTS-4000 & NTS-5000 only)	RJ45
		DISABLE	(NTS-4000 & NTS-5000 only)	
Ant2 (Antenna "B")	INPUT	INPUT	(all)	RJ45
		OUTPUT	(NTS-4000 & NTS-5000 only)	RJ45
		DISABLE	(NTS-4000 & NTS-5000 only)	

Note! After restoring to factory defaults, please clear your web browser history and delete cookies.

User Manual

14. Hardware of NTS

IMORTANT NOTE!
Before reading this part of manual please read Quick Manual "Configure in 5 minutes" first. Some fundamental basics of setup operations are described earlier and not repeated here.

NTS - SERIES description:

NTS - M P LL . U

M – Model
P – Platform
LL – Number of LAN ports
U – Rack unit size

Model	Description
3	Server **without additional oscillators for HoldOver**, two GNSS receiver ports.
4	Server with **OCXO** oscillator for HoldOver, two GNSS receiver ports
5	Server with **OCXO and Rubidium** oscillator for HoldOver, two GNSS receiver ports.

Platform	Description
0	MainBoard with 500MHz CPU, standard 2x100Mbps RJ45 ports (additional 2x1 Gbps SFP for PTP HW timestamping expanders).
1	Reserved.
2	MainBoard with 1.5GHz CPU, standard 1x 100Mbps RJ45, and 2x1Gbps SFP ports (optional 2xadditional 1Gbps SFP ports).
3	Reserved.

LL	Lan ports counter
3	3 x LAN ports
4	4 x LAN ports
5	5 x LAN ports
	etc

U	Rack unit size
1U	Rack 19 1U
2U	Rack 19 2U

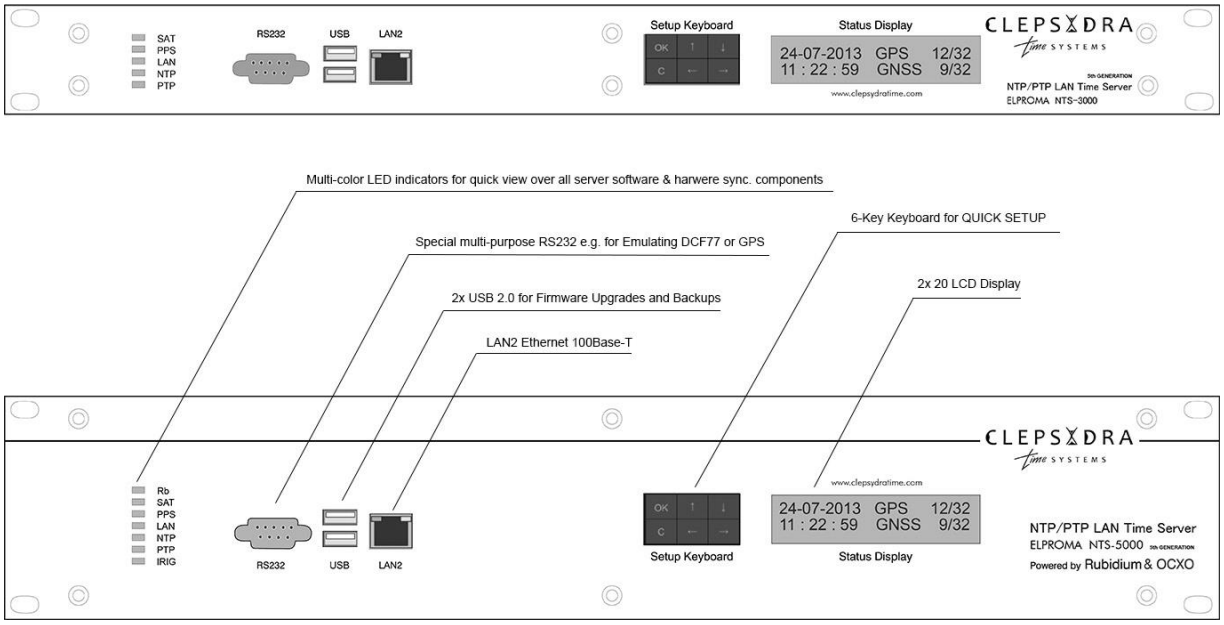
For example, Series NTS-5xxx Model NTS-5203.2U – two ports GNSS, OCXO & Rubidium, mainboard with 2xCPU, 1xRJ45 100Mbps, 2xSFP 1Gbps, Rack 19 2U size.

The NTS time servers has all very similar front panel view. All products are available under ELPROMA or branded to CLEPSYDRA brand. Below picture present all family of NTS time servers.

ELPROMA NTS family of time servers (from top: NTS-3000, NTS-4000, NTS-5000LITE and NTS-5000 Rubidium)

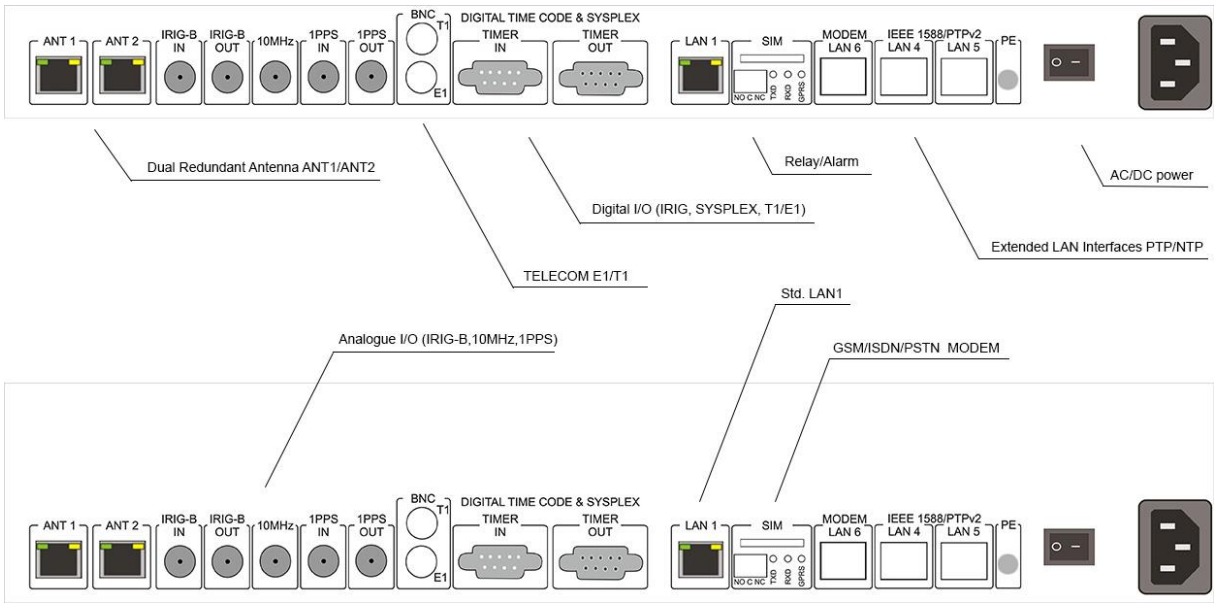
There is 2x20 characters LCD *Status Display* (green colour), 6-key mechanical keyboard for quick setup, RS232 (DSUB-9 mail) connector for direct SETUP, 2xUSB2.0 interface for firmware upgrade etc. There is LAN2 connector located on the front panel too. It contains 2x LEDs: green - indicates cable connection, yellow - flashes while data is being transmitted.

The front panel view of NTS time server is:



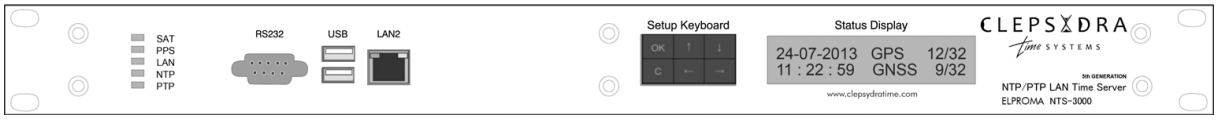
Standard Front Panel – CLEPSYDRA branded

The back panel of NTS is organized on way there are several I/O referential time sections:

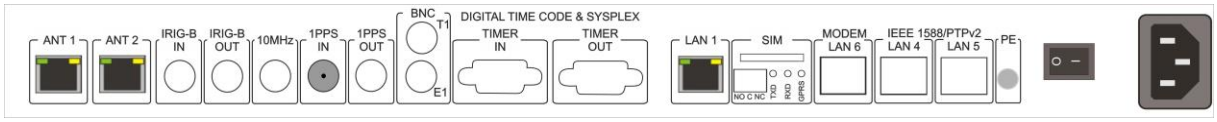


Standard Back Panel

15. Hardware of NTS-3000
(Standard Version)



NTS-3000 (standard) Front Panel



NTS-3000 (standard) Back Panel

Available only based on Platform 0

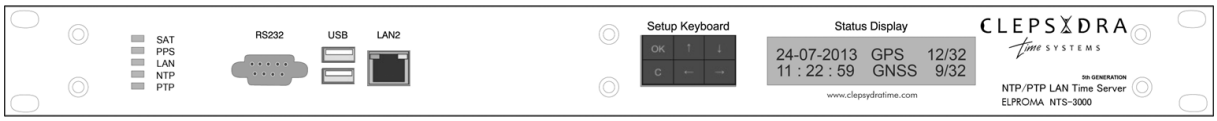
Table describe connectors it's availability and related into it functions:

Name	Connector	Standard	Purpose	Availability
Antenna (A)	RJ-45	RS-485	Antenna connector (main antenna)	+
Antenna (B)	RJ-45	RS-485	Antenna connector (backup antenna)	+
IRIG-B IN*	BNC	IRIG-B	IRIG-B source signal	-
IRIG-OUT*	BNC	IRIG-B	IRIG-B output signal	-
10 MHz	BNC	10MHz	10 MHz output reference signal	-
1 PPS IN	BNC	1pps	1 PPS (pulse per second) source signal	+
1 PPS OUT	BNC	1pps	1 PPS (pulse per second) output signal	-
TIMER IN	DSUB9	RS-232	2xPPS (pulse per second) input signal	-
TIMER OUT	DSUB9	Various	ToD, 1PPS, other TC std. optionally	-
LAN1	RJ-45	TCP/IP	Local Area Network (back panel)	+
LAN2	RJ-45	TCP/IP	Local Area Network (front panel)	+
RS-232	DSUB9	RS-232	For technical and service purpose	+
USB	KUSB	USB	For technical and service purpose	+

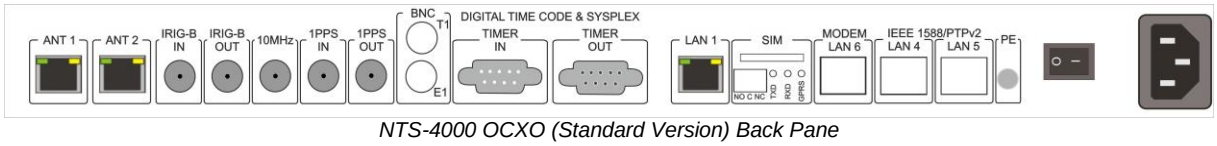
NTS-3000 (standard) Back Panel picture

NTS-3000 (standard) Front Panel picture

16. Hardware of NTS-4x00 OCXO
(Standard Version)



NTS-4000 OCXO (Standard Version) 1U rack'19 mount Front Panel



NTS-4000 OCXO (Standard Version) Back Pane

Available based on Platform 0 and 2

Table describe connectors it's availability and related into it functions:

Name	Connector	Standard	Purpose	Availability
Antenna (A)	RJ-45	RS-485	Antenna connector (main antenna)	+
Antenna (B)	RJ-45	RS-485	Antenna connector (backup antenna)	+
IRIG-B IN	BNC	IRIG-B	IRIG-B source signal	Optionally
IRIG-OUT	BNC	IRIG-B	IRIG-B output signal	Optionally
10 MHz	BNC	10MHz	10 MHz output reference signal	+
1 PPS IN	BNC	1pps	1 PPS (pulse per second) source signal	+
1 PPS OUT	BNC	1pps	1 PPS (pulse per second) output signal	+
TIMER IN	DSUB9	RS-232	2xPPS (pulse per second) input signal	+
TIMER OUT	DSUB9	Various	ToD, 1PPS, other TC std. optionally	+
LAN1	RJ-45	TCP/IP	Local Area Network – platform 0 & 2	+
LAN2	RJ-45	TCP/IP	Local Area Network – platform 0	+
LAN2-3	SFP	TCP/IP	Local Area Network – platform 2	+
RS-232	DSUB9	RS-232	For technical and service purpose	+
USB	KUSB	USB	For technical and service purpose	+

The NTS-4000 also comes in a 2U version, which replaces the NTS-5000LITE version

NTS-4000 OCXO (Standard Version) Back Panel picture

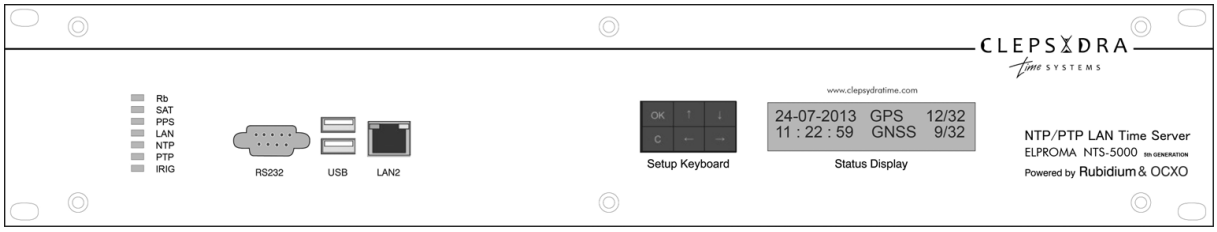
NTS-4000 (Standard Version) Front Panel picture

17. Hardware of NTS-5x00 Rubidium & OCXO

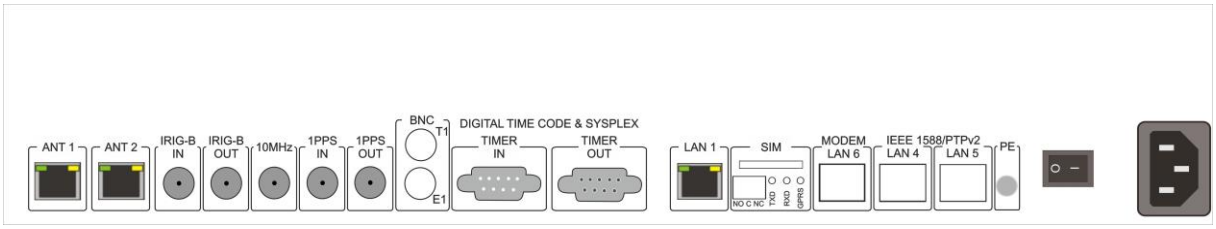
The NTS-5000 std. (standard) is equipped with dual Rubidium & OCXO holdover oscillator.
Available based on Platform 0 and 2

The NTS-5000 network appliance delivers UTC time directly to the Ethernet network (max. 10x LAN) using both: PTP (IEEE1588) and NTP protocols
Platform 0:
LAN1 and LAN2 are 10/100Mbps and have special features that are very helpful in maintaining and real-time monitoring of the NTS-5000 server.
Interfaces LAN3 to LAN10 are optional and support 1GbE Ethernet, acting as autonomous PTP/IEEE1588 GRANDMASTER or SUBMASTER with hardware timestamping (see “Extended version” on the next page).

Platform 2:
LAN1 is 10/100Mbps, while LAN2 and LAN3 (LAN4, LAN5 – optionally) are 1Gbps, replacing LAN3 – LAN6 from platform 0.



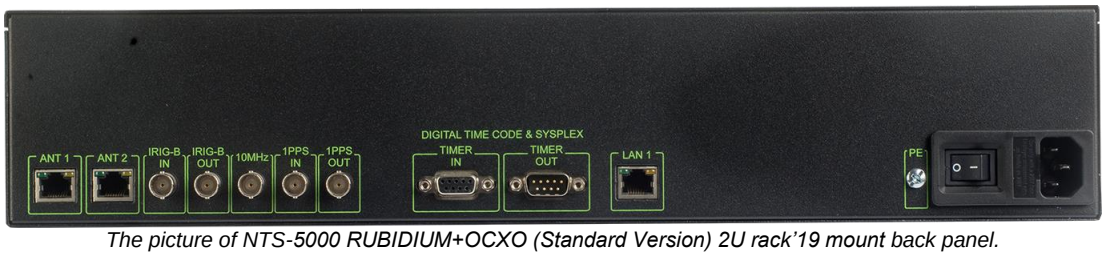
NTS-5000 RUBIDIUM+OCXO (Standard Version) 2U rack’19 mount Front Panel. The LAN2 is RJ45 100/10 Mbps Ethernet



NTS-5000 RUBIDIUM+OCXO (Standard Version) 2U rack’19 mount Back Panel. The LAN1 is RJ45 100/10 Mbps Ethernet

Below table describe connectors it’s availability, and related into it functions:

Name	Connector	Standard	Purpose	Availability
Antenna (A)	RJ-45	RS-485	Antenna connector (main antenna)	+
Antenna (B)	RJ-45	RS-485	Antenna connector (backup antenna)	+
IRIG-B IN	BNC	IRIG-B	IRIG-B source signal	Optionally
IRIG-OUT	BNC	IRIG-B	IRIG-B output signal	Optionally
10 MHz	BNC	10MHz	10 MHz output reference signal	+
1 PPS IN	BNC	1pps	1 PPS (pulse per second) source signal	+
1 PPS OUT	BNC	1pps	1 PPS (pulse per second) output signal	+
TIMER IN	DSUB9	RS-232	2xPPS (pulse per second) input signal	+
TIMER OUT	DSUB9	Various	ToD, 1PPS, other TC std. optionally	+
LAN1	RJ-45	TCP/IP	Local Area Network – platform 0 & 2	+
LAN2	RJ-45	TCP/IP	Local Area Network – platform 0	+
LAN2-3	SFP	TCP/IP	Local Area Network – platform 2	+
USB	KUSB	USB	Disabled (Covered) or firmware upgr.	+



The picture of NTS-5000 RUBIDIUM+OCXO (Standard Version) 2U rack'19 mount back panel.

NTS-5000 RUBIDIUM+OCXO (Standard Version) 2U rack'19 mount front panel.

18. Hardware of NTS-5x00 LITE (OCXO only)

Note! From 2024/Q3 NTS-5000LITE is replaced by NTS-4x00 2U version

Note! The NTS-5000LITE is low-cost version of NTS-5000 Rubidium. It is powered by OCXO oscillator only. The difference between NTS-5000 Rubidium and NTS-5000LITE is the RUBIDIUM quantum oscillator only. The Rubidium holdover ensures STRATUM-1 (ITU-I G.811) STRATUM-1 holdover operation with full accuracy for 72 hours. Please follow NTS-5000 to configure your NTS-5000LITE

19. Hardware of NTS-5000 NIC Expanders

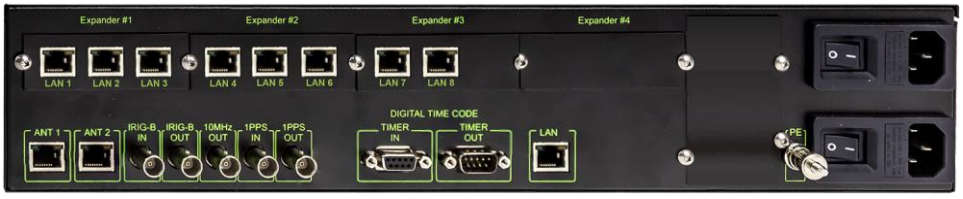
Note! Version available only for platform 0

NTS-5000 provides strong security as each of the LAN modules is 100% information isolated from another. It is so-called “galvanic” isolation. To improve security NTS-5000 also isolate each network interface LAN on a software level. Any security compromise on one LAN module will be fully software isolated from another LAN module. Multiple independent networks and devices requiring separation can be connected to the same NTS-5000 without worry that a security breach in one network will affect another network.

On top of NTS-5000, the GrandMaster server supports a special expansion 4 slots for additional network LAN interfaces. The available expansion modules are:

- 4x 2-port 1GbE Ethernet SFP/RJ45 or SFP/SFP (hardware high accuracy time-stamps)
- 1x 8-port 1GbE Ethernet 8x RJ45 + 1x SFP (software std. accuracy time-stamps)

4x 2-port 1GbE Ethernet SFP/RJ45 or SFP/SFP



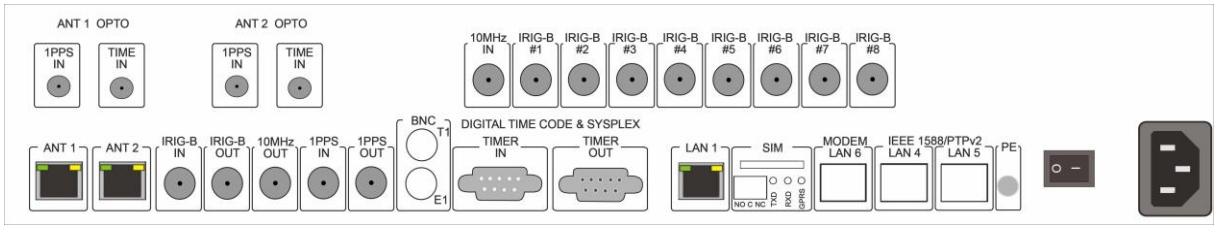
1x 8-port 1GbE Ethernet 8x RJ45 + extra 1x SFP

Ports LAN3-LAN10 are optional 1GbE Ethernet (both SFT and/or combined pare of SFP+RJ45 ended depending on the year of production). They are available via special Extender 1-4 cards.

20. Hardware of NTS-4/5x00 Custom

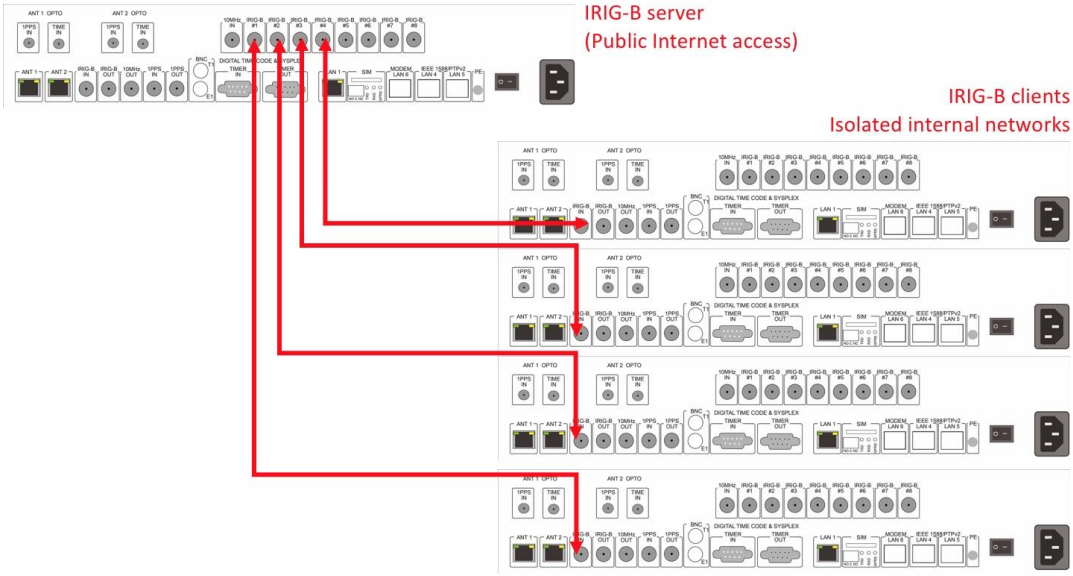
Note! Version available only for platform 0

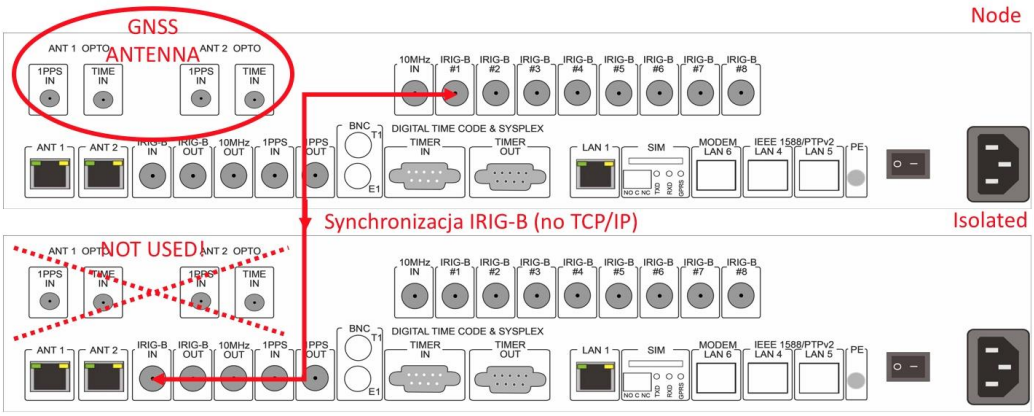
Elproma is able to customize existing NTS-5000 solutions. The server can be equipped with 1GbE, 10GbE. We are also able to design and manufacture a custom build version of time server that basis on NTS-5000 platform. Below there is example of NTS-5000 device manufactured since 2008 for Air Traffic Control application. Compering to standard product below NTS-5000 supports fibber-optic GNSS antenna and it includes 8x IRIG-B AM distribution channel.



NTS-5000Rb+OCXO w/ 8x IRIG-B distribution panel and 2x FIBER-OPTIC GNSS antenna (back panel)

One of advantages of using IRIG-B AM (analogue modulated) is fact there is no TCP/IP communication that hacker can break into the system. Therefore, frequently the NTS-5000 with 8x IRIRG-B is used to supply ref. time UTC over firewall to internal secured networks. Such connection is requiring 2nd level of NTS-5000 working IRIG-B clients. The connection scheme is shown below.

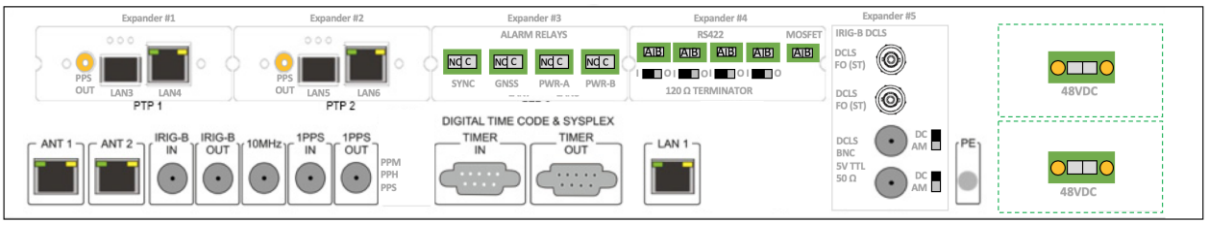




21. Hardware of NTS -5x00 IRIG-B DCLS

Special configuration of NTS-5000 is dedicated for modern smart-grid systems.
The typical unit configuration is:

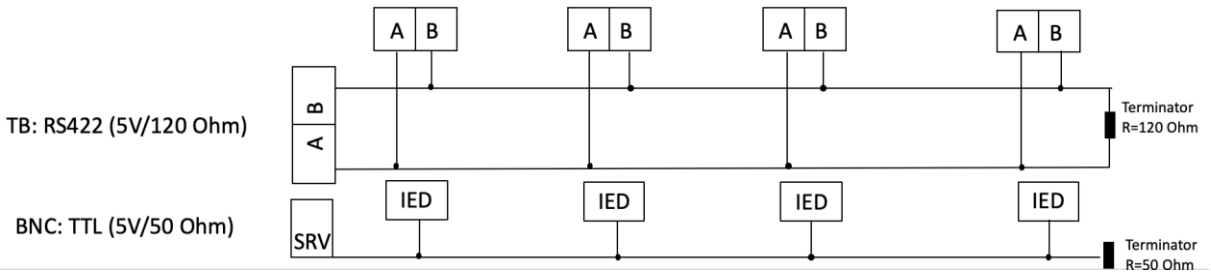
Expander #1: 2x PTP IEEE1588 Network Interface w/ hardware stamping
Supporting: IEEE C37.238 (incl. IEEE 61850-9-3 via C37.238) – only for Platform 0
Expander #2: 2x PTP IEEE1588 Network Interface w/ hardware stamping
Supporting: IEEE C37.238 (incl. IEEE 61850-9-3 via C37.238) – only for Platform 0
Expander #3: 4x ALARM RELAYS
Supporting alarms: SYNC, GNSS, PWR-A, PWR-B
Expander #4: 4x IRIG-B rs422 DCLS (w/ slide switch 120Ohm termination ON/OFF)
1x MOSFET PPS/PPM/PPH - support for Platform 0 and 2
Expander #5: 2x IRIG-B TTL level 5V (w/ slide switch for selecting AM or DCLS)
2x IRIG-B ST Fiber Optic IRIG-B DCLS - support for Platform 0 and 2



NTS-5000Rb+OCXO w/ 4x ALARM RELAY, 4x RS422 (IRIG-B DCLS), 2x Fiber Optic (IRIG-B DCLS), 2x TTL 5V (IRIG-B)

In above configuration, LAN1 & LAN2 are used for monitoring synchronization facility only. Server receives ref. time from GNSS (ANT-1 and/or ANT-2) and redistribute it via LAN3, LAN4, LAN5, LAN6 GE interfaces using hardware stamping of PTP IEEE1588. Simultaneously it generates all IRIG-B outputs in all available hardware standards too.

Typical IED connections scheme is:

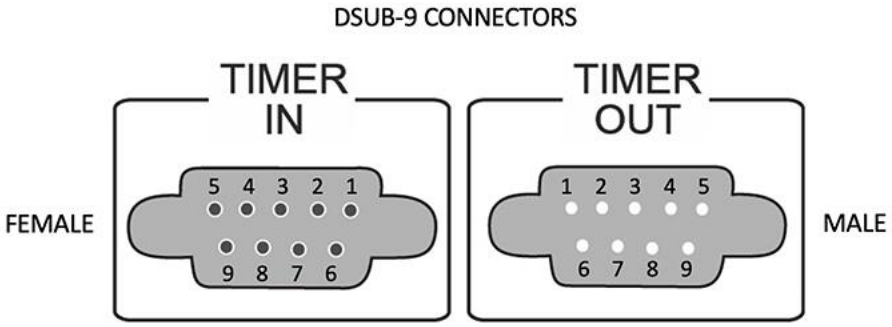


IED connection block scheme: (upper) RS422 w/ 120 termination, (lower) TTL 5V 50 Ohm

22. Hardware of NTS – The DSUB9 Interface

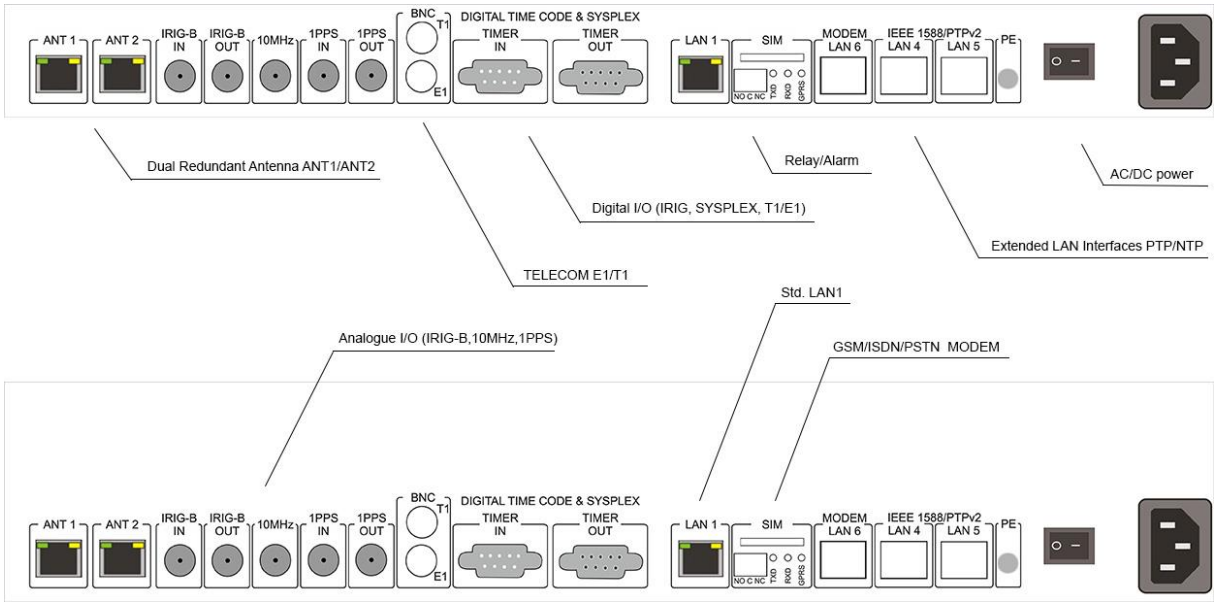
Server: NTS-3000, NTS-4000, NTS-5000, NTS-5000LITE, NTS-9000 are equipped with 9pin DSUB9 connectors providing various of hardware synchronization signals.

The pin-out is:



1 PIN - 1PPS IN (if BNC not used)	1 PIN - 1PPS OUT RS-232 standard
2 PIN - RxD RS232	2 PIN - RxD RS232
3 PIN - TxD RS232	3 PIN - TxD RS232
4 PIN - *(reserved)*	4 PIN - IRIG DCLS RS485+
5 PIN - GND	5 PIN - GND
6 PIN - PPS IN + RS485+	6 PIN - 1PPS OUT RS-485+
7 PIN - 1PPS IN RS-485-	7 PIN - 1PPS OUT RS-485-
8 PIN - *(reserved)*	8 PIN - IRIG DCLS RS485 -
9 PIN - *(reserved)*	9 PIN - IRIG DCLS TTL

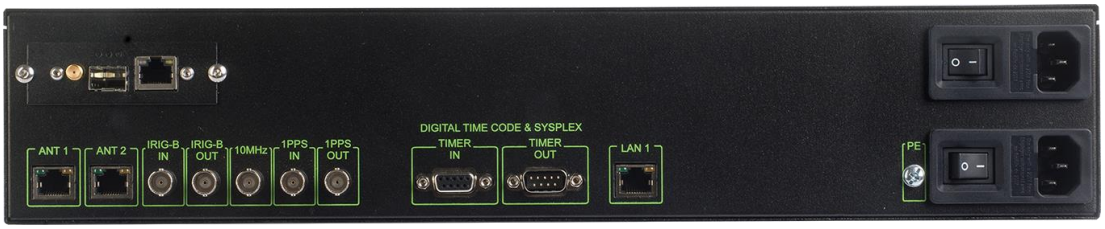
The back panel view with 2x DSUB9 connectors (DIGITAL TIME CODE)



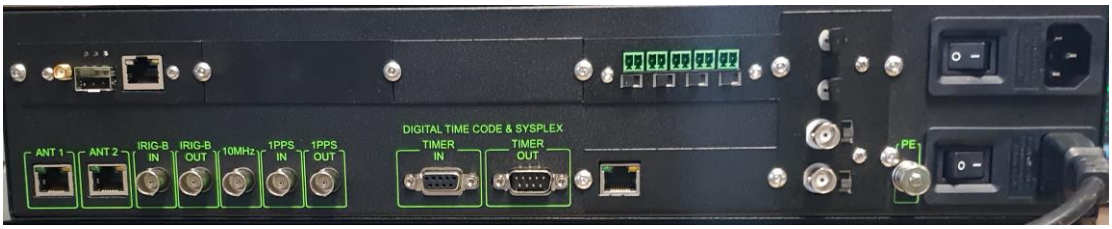
23. Hardware of NTS-TC (Time Converter)

Converting UTC/TAI time from IEEE1588 to IRIG-B

NTS-TC (time-converter PTP-2-IRIG) –front panel view



NTS-TC (time-converter PTP-2-IRIG) – back panel view (basic version w/ IRIG-B AM only)

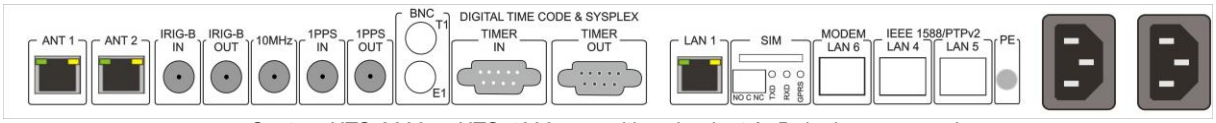


NTS-TC (time-converter PTP-2-IRIG) – back panel view (max. version w/ 4x RS422, 2x FO, 2x BNC TTL 5V AM/DCLS)

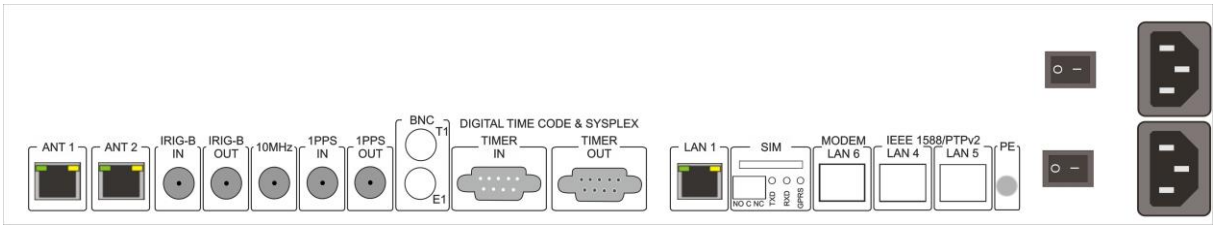
The **NTS-time-converter** basis on NTS-5000 hardware platform. It is dedicated for time-code conversions from PTP/IEEE1588 to IRIG and/or (back) from IRIG-B to PTP IEEE1588. Depends on director of signal conversion, the PTP/IEEE1588 operates in Master or Slave PTPv2 mode. Unit can be optionally equipped with Rubidium and OCXO holdover oscillator. In case of failing INPUT time-code, unit can product OUTPUT time base on GNSS or from local holdover oscillator OCXO*. In case of using GNSS, it is necessary to connect at least one NTS-antenna to NTS-TC. This product is 100% compatible (SETUP level) with NTS-5000 time server therefore, to configure NTS-TC please refer to NTS-5000/NTS-5000LITE.

24. Extra Hardware – Redundant PWR Supply

Standard NTS-3000 product is delivered with single power supply, The NTS-4000 and NTS-5000 are delivered with dual power supply. Device starts automatically after power OFF/ON or any double line redundant power failure.



Custom NTS-3000 or NTS-4000ocxo with redundant A+B dual power supply



Custom NTS-5000 Rb & OCXO or NTS-5000LITE with redundant A+B dual power supply

WARNING

Elproma time servers can be equipped with various types of AC, DC power supplies supporting different range of voltage. Before using Elproma product please check the type of power supply labelled on the back panel of time server.

Important note #1! Standard NTS is delivered by default with power supply 110-230VAC. This power supply also supports DC in range of 120-370VDC.

Following power supplies are available single or dual redundant mode:

20- 70 VDC (max 2A)
110-230 VAC (max 1A) /default std. /
120-370 VDC (max 1A)

Important note #2! The dual redundant power supply needs to be ordered together with a new NTS product. It is not possible to update NTS later on adding 2nd power supply.

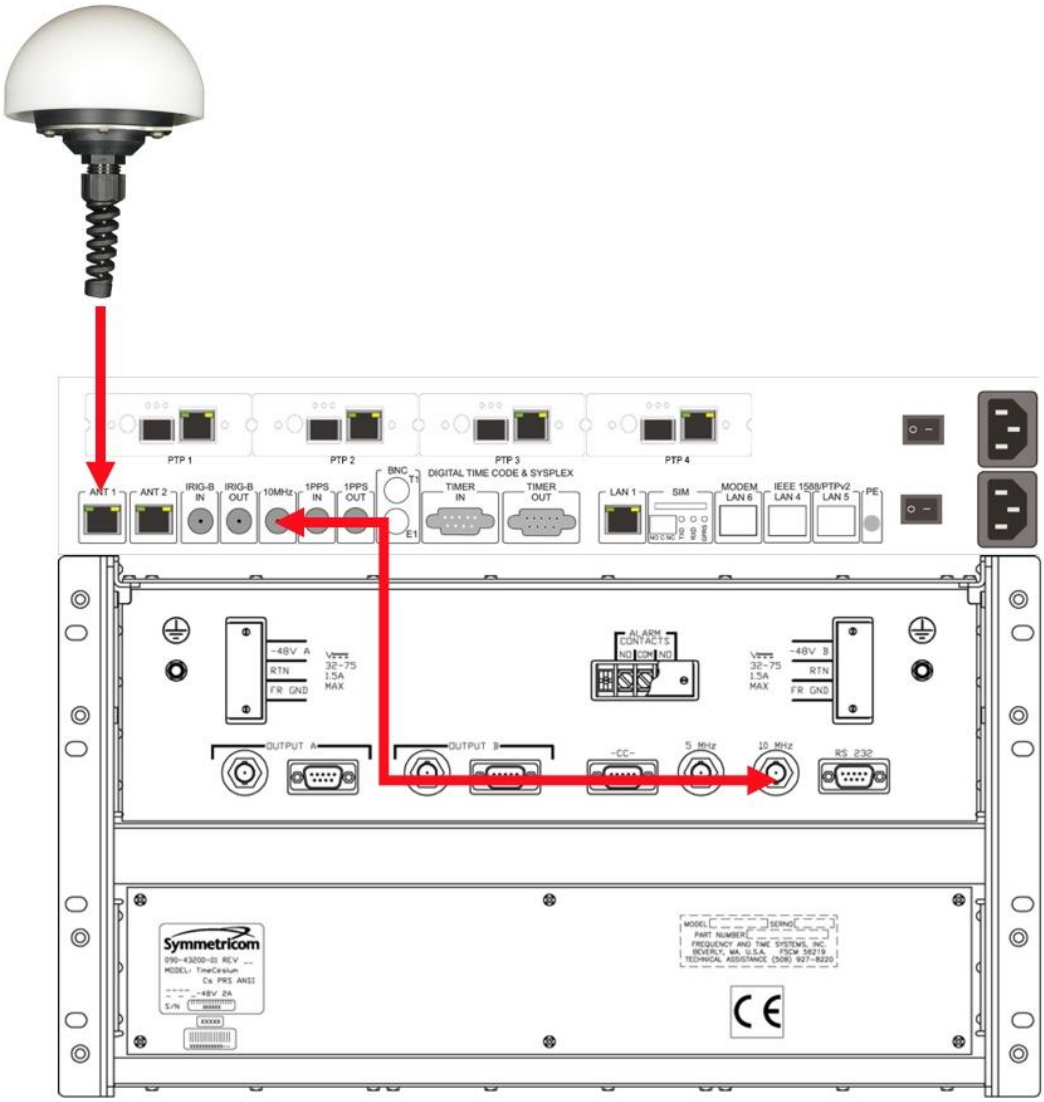
25. Extra Hardware – Connecting to Cesium

(Based on cesium Model 4400/4500 with 10Mhz connection)

Any NTS family time server can work with external Cesium primary reference of time or frequency. Using external atomic Cesium (Cs) clocks improves holdover operation ensuring server robust frequency stability and high accuracy of synchronization. Depends on type of available connectivity this can be limited to synchronization of frequency (PPS, 10MHz) only or both phase & frequency (ToD + PPS) Synchronizing UTC (TAI) phase and frequency requires special version of NTS product to support direct phase. This chapter describes a connectivity of NTS to frequency reference only – the one that is supported by standard product supporting PPS, or special customized one supporting 10MHz input.

Important note! *Using Cs frequency ref. is requiring at least one GNSS antenna (NTS-antenna) to be connected to NTS. This is important because a time server needs initial timestamp (ToD – a Time of a Day) information to operate UTC or TAI time scale. The UTC (TAI) can be also initialized from remote NTP server using Network Time Protocol.*

Connecting cesium clock using frequency ref. 10MHz
(standard product support PPS-input only)



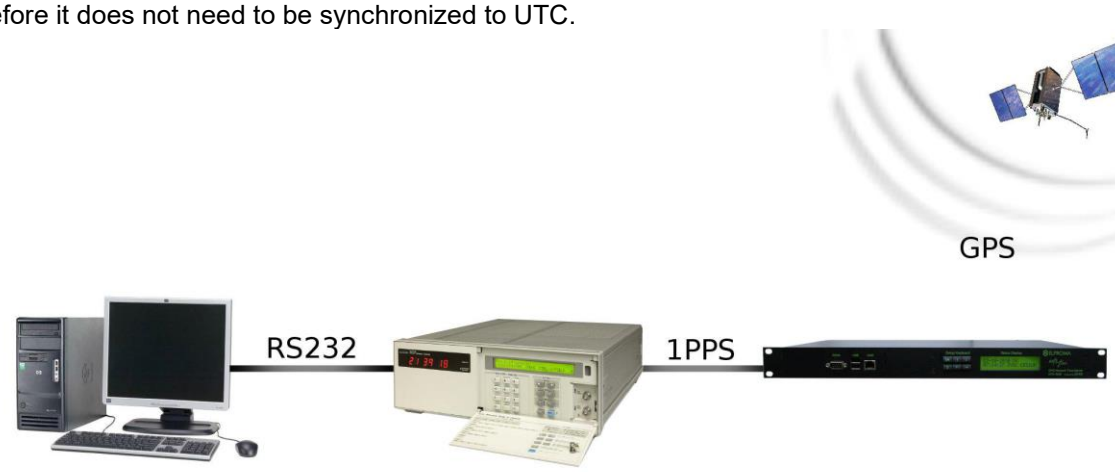
Connecting 10MHz cesium 4400/4500 frequency reference to NTS-5000 input. The same solution can base on 1PPS too.

26. Extra Hardware – Connecting To 5071A

(Based on cesium Model 5071 supporting PPS alone or PPS+ToD via rs232 connection)

The 5071A Cesium clock support is available at NTS series since year 2006. Early time this functionality was available for model NTS3000 only. Later it was included to NTS-4000 too. Since 2019, all Elproma NTS series (NTS-3000, NTS-4000, NTS-5000) can support 5071A Cesium atomic clocks. The 5071A connectivity can be set using 1 of following 2 schemes:

Scheme #1 (Frequency PPS from Cesium only)
NTS-3000, NTS-4000, NTS-5000 uses only frequency reference 1PPS (BNC) from 5071A. The initial ToD (date & time – the UTC phase) is provided from GPS. This solution is requiring NTS-antenna to be connected to NTS time server. The 5071 is used only as a frequency reference and therefore it does not need to be synchronized to UTC.



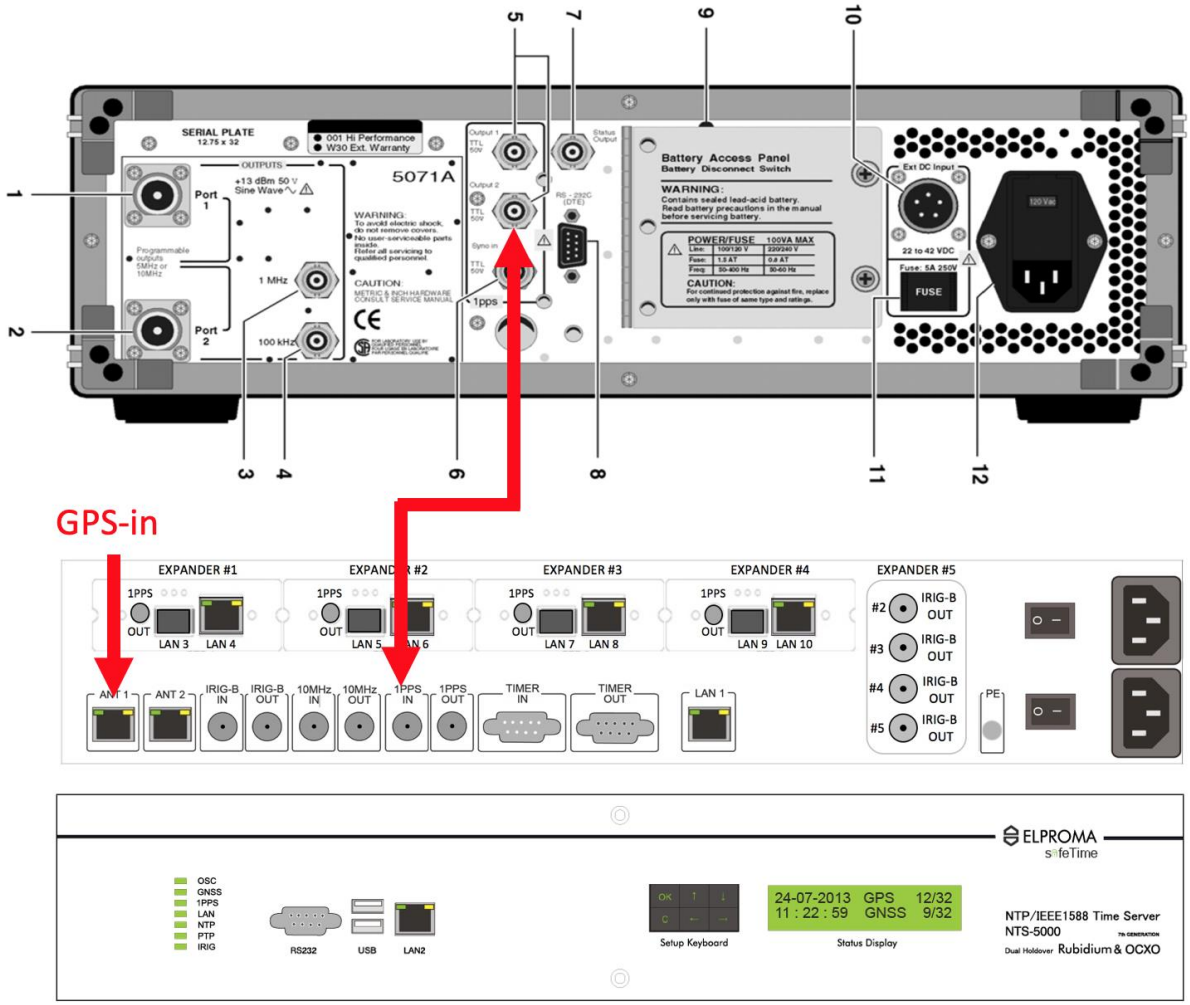
Scheme #2 (Time & Frequency from Cesium)
NTS-3000, NTS-4000, NTS-5000 are using both 1PPS (BNC) + ToD(rs232) from 5071A. In this connectivity 5071A needs to ensure both UTC time & frequency reference, therefore NTS does not need to be equipped with (GPS) NTS-antenna. You will need to purchase special software firmware licence that enables such connectivity. In case of time server NTS-5000 the product and a license are well known as one bundle product id. **NTS-9000**. In case of EU market this can include 5071 Cesium too.

NOTE! In Scheme #2 the NTS time server is 100% transparent for PC telemetry dataflow going from/to 5071A via rs232 interface. Typically, PC is used to run Cesium beam monitoring software.

Ad. Scheme #1 5071A connectivity (only frequency 1PPS from Cesium)

The 1PPS alone connection is requiring at least one GNSS antenna (NTS-antenna) or another remote NTP server to provide initial ToD timestamp necessary to support full UTC time scale (date & time).

Please connect 5071A PPS-output using quality RG58 cable. Use GPS antenna to provide initial ToD information (date & time).

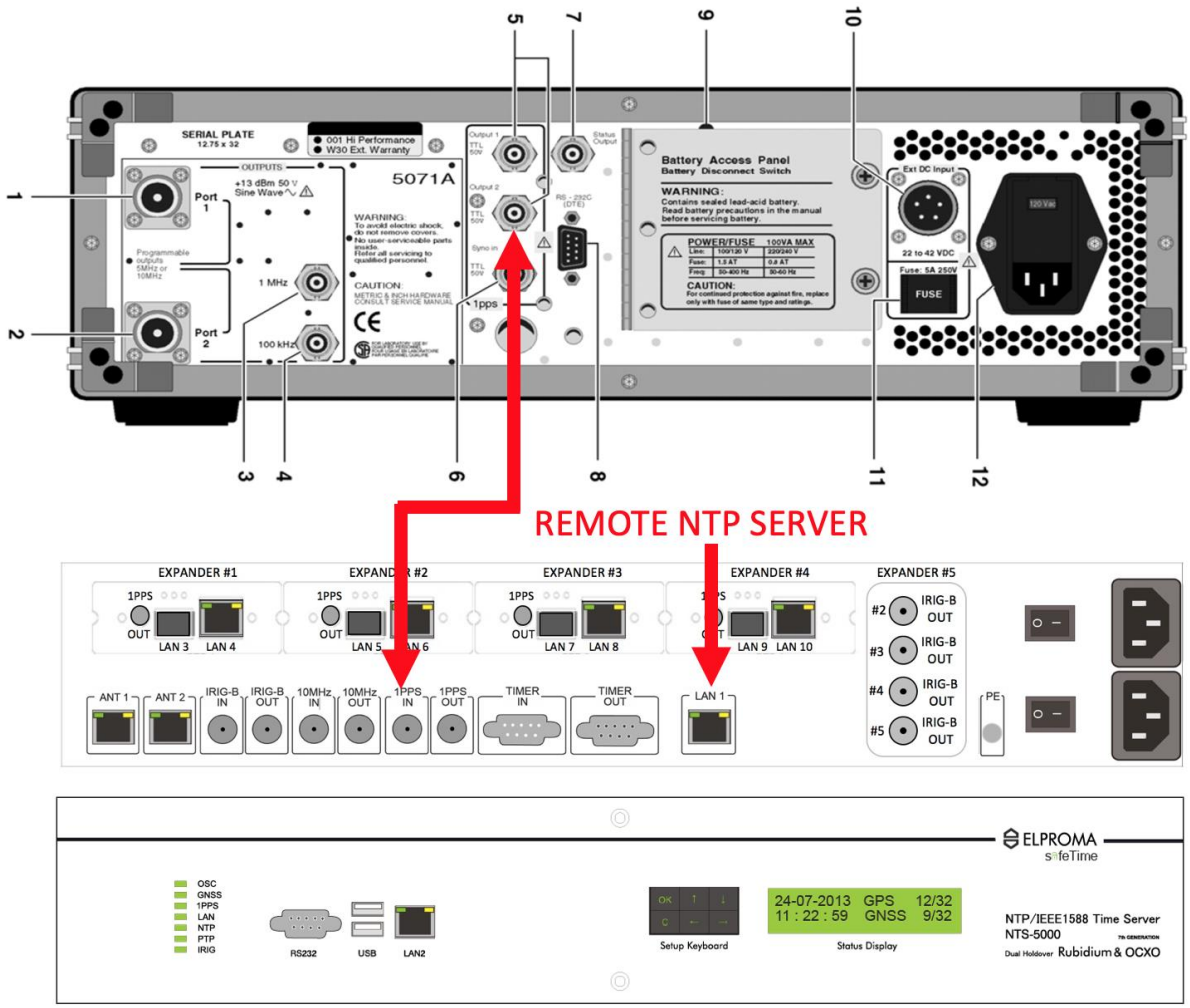


PPS reference is provided directly from 5071A. The initial ToD information is supported from GNSS.

In above connection scheme, the initial ToD (Time of a Day) is taken from GPS receiver connected to ANT1 (or ANT2). It can take several minutes (depends on quality of received GPS signals) before NTS server gets ready to synchronize to 5071A PPS. Once the NTS server is lock to GPS, it will start to synchronize to 5071A using PPS frequency reference, and it does not need GPS reference anymore.

Alternatively, the initial ToD information can be taken from another (remote) NTP server using network interface LA N1 (or LAN2). In this case your server will temporary reduce STRATUM to N-1 (where N means a STRATA of remote NTP server providing initial ToD information to your server). Once the ToD

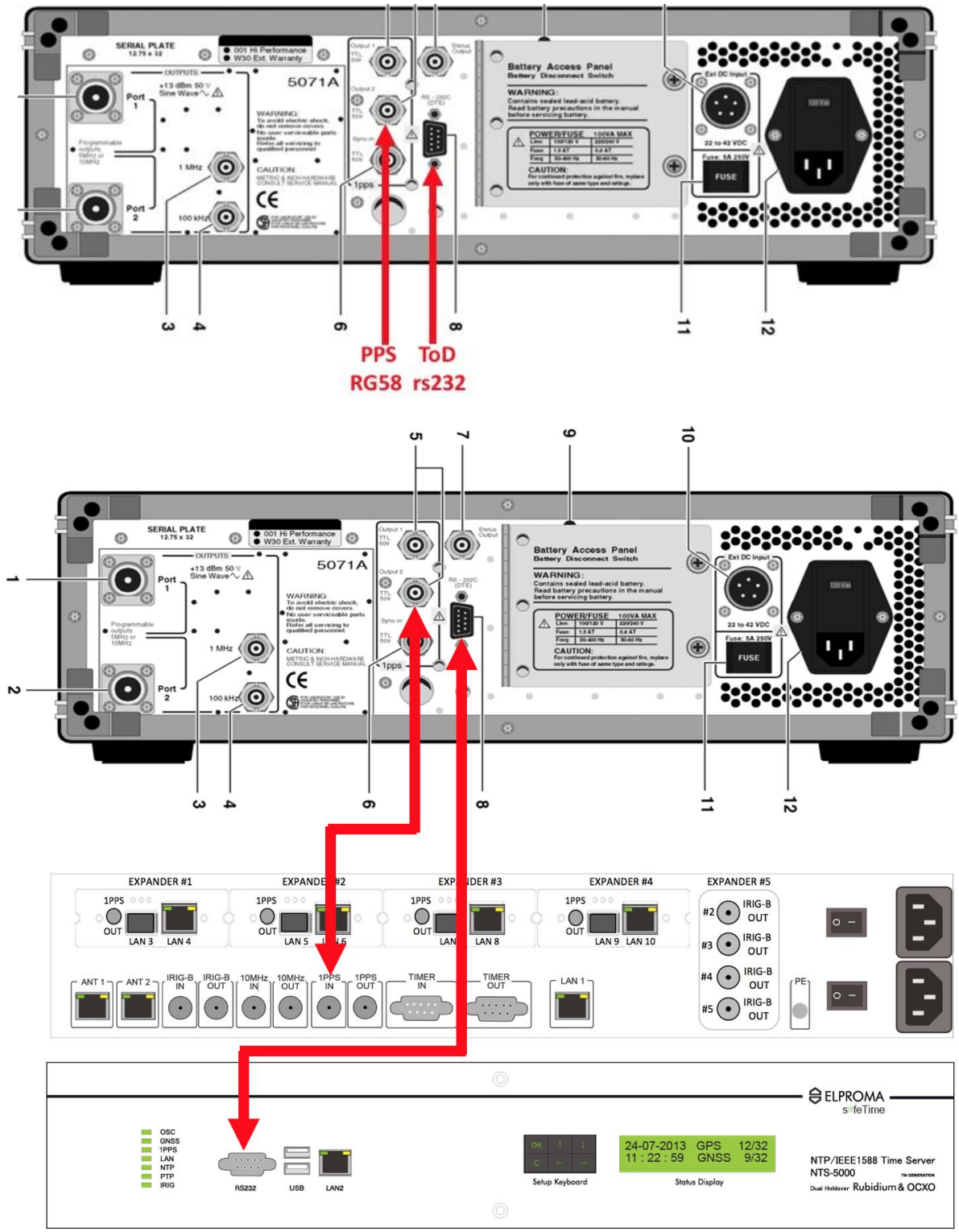
initialization (NTP) is done, your server will switch to PPS. Reference from 5071A increasing STRATA to STRATUM 1 operation. Once this information is done, you will not need remote NTP server anymore.



Singe frequency reference 1PPS synchronization of NTS. The initial ToD is taken from another (remote) NTP time server

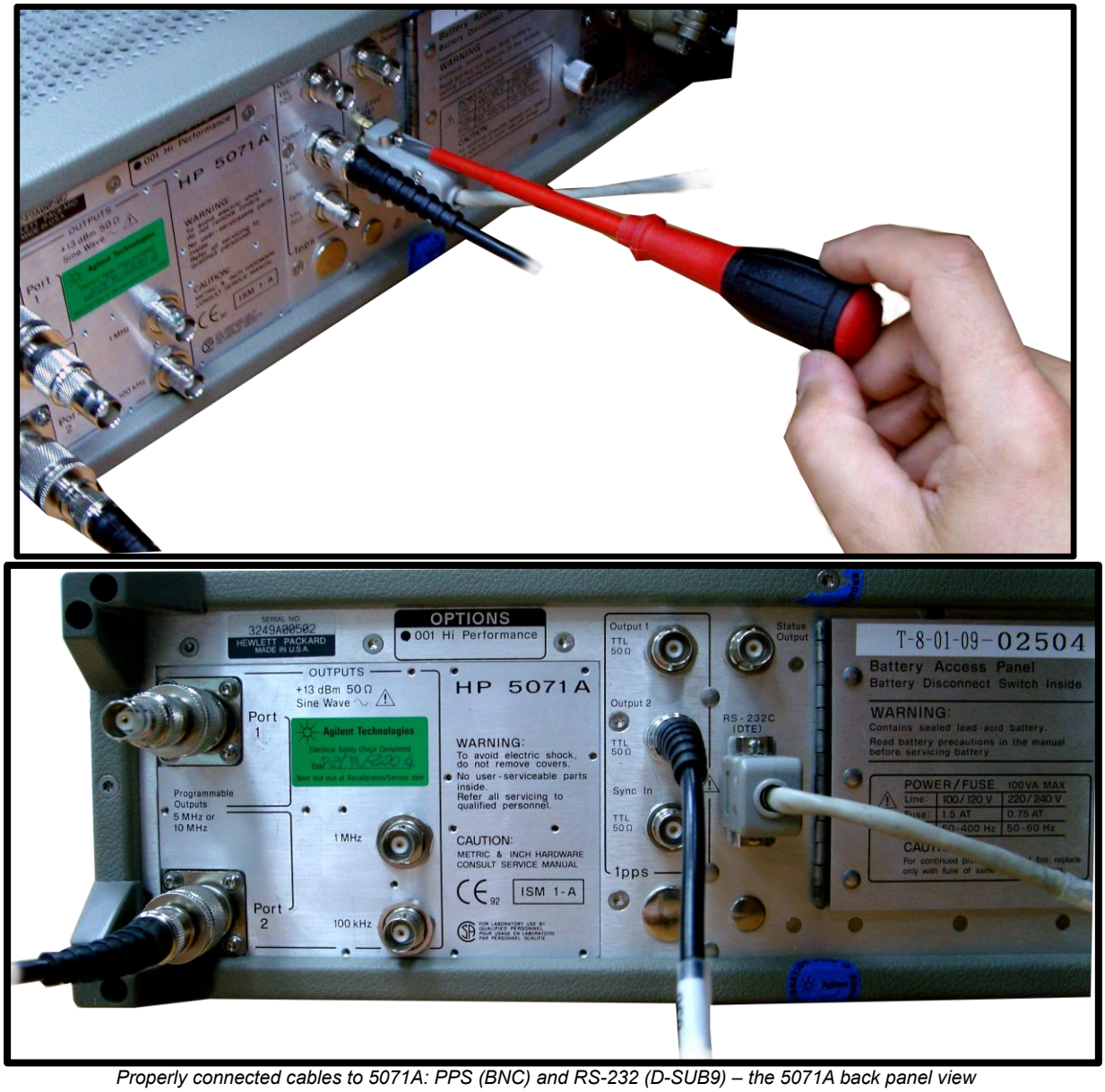
Scheme #2 - Installing special version of NTS with Cesium 5071A using both: PPS + ToD

Elproma has developed solution that supports simultaneously 5071A using both: ToD timestamps and PPS frequency reference. Such dual PPS + ToD synchronization to 5071A does not need any GPS receiver nor remoted NTP server. Furthermore, you will not lose cesium telemetry facility due to fact NTS-x000 behaves 100% transparent for all Cesium data and PC requests.



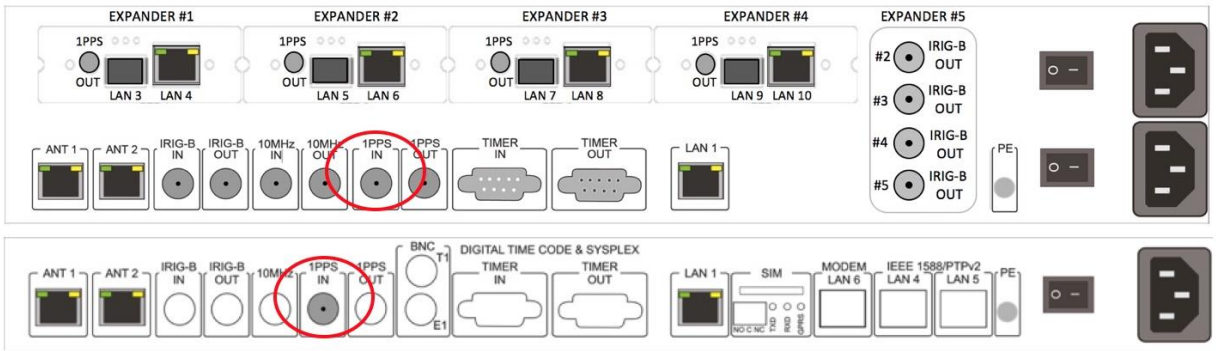
Connecting NTS-x000 to 5071A using PPS + ToD. Please use RG58 (PPS) and serial RS232 cable (D-SUB9 ended) cables.

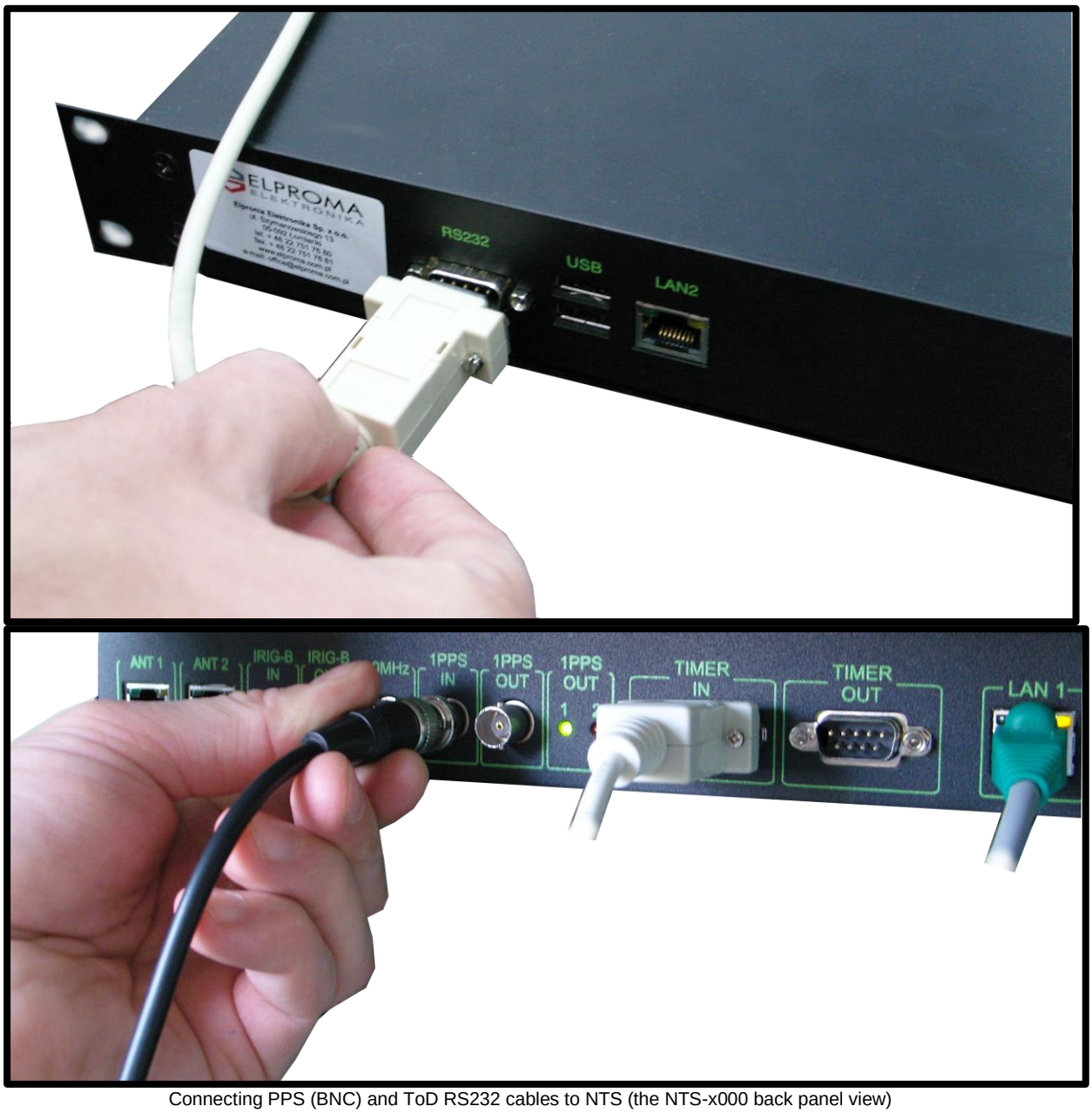
Preparing 5071A. Find 1PPS-out and RS-232 (D-SUB) interface on the back panel of 5071A. Please connect BNC RG58 cable to PPS-out of 5071A. Then please install RS-232 cable.



Properly connected cables to 5071A: PPS (BNC) and RS-232 (D-SUB9) – the 5071A back panel view

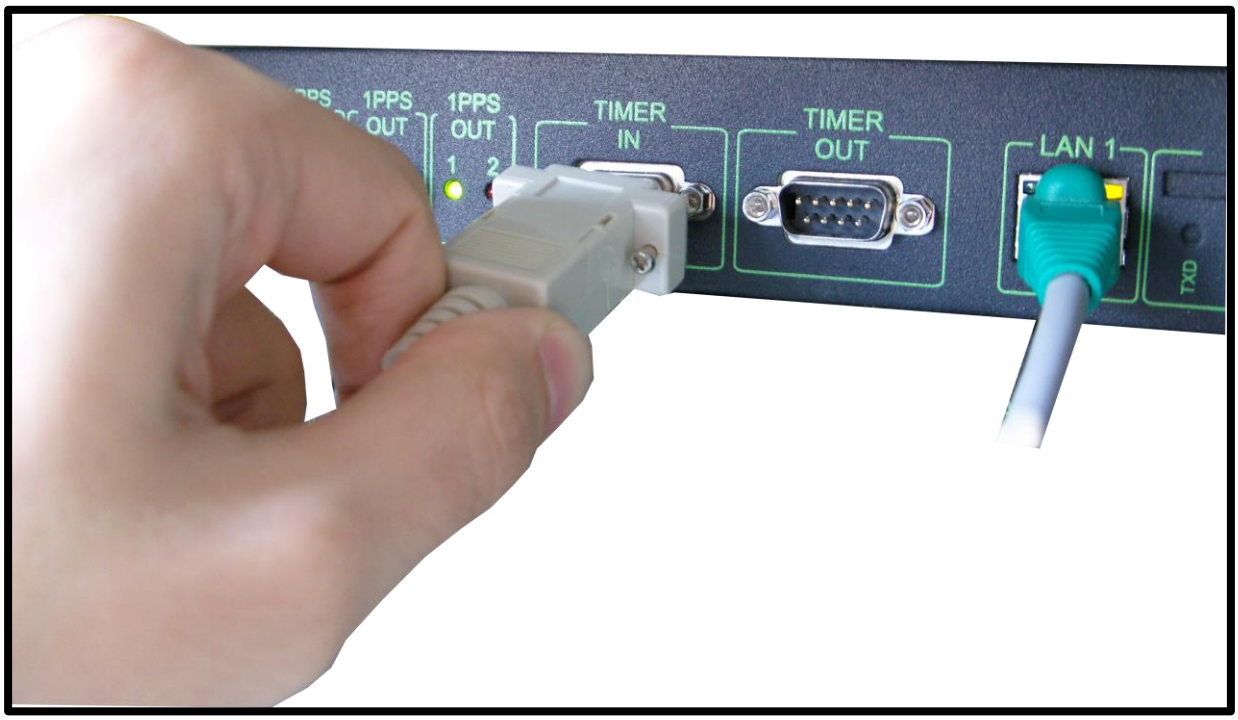
Connecting 5071A and NTS-x000. Please connect RG-58 (PPS) cable to back panel BNC of NTSx000 labeled PPS-in, and connect RS232 cable to **<u>NTS-x000 front panel D-SUB9</u>** connector as presented.





Connecting PPS (BNC) and ToD RS232 cables to NTS (the NTS-x000 back panel view)

Connecting PC to NTS-x000. Please connect RS232 cable to back panel TIMER-IN of your NTS-x000.



Connecting PC to NTS-x000 using rs232 interface

HIGHLIGHTS:

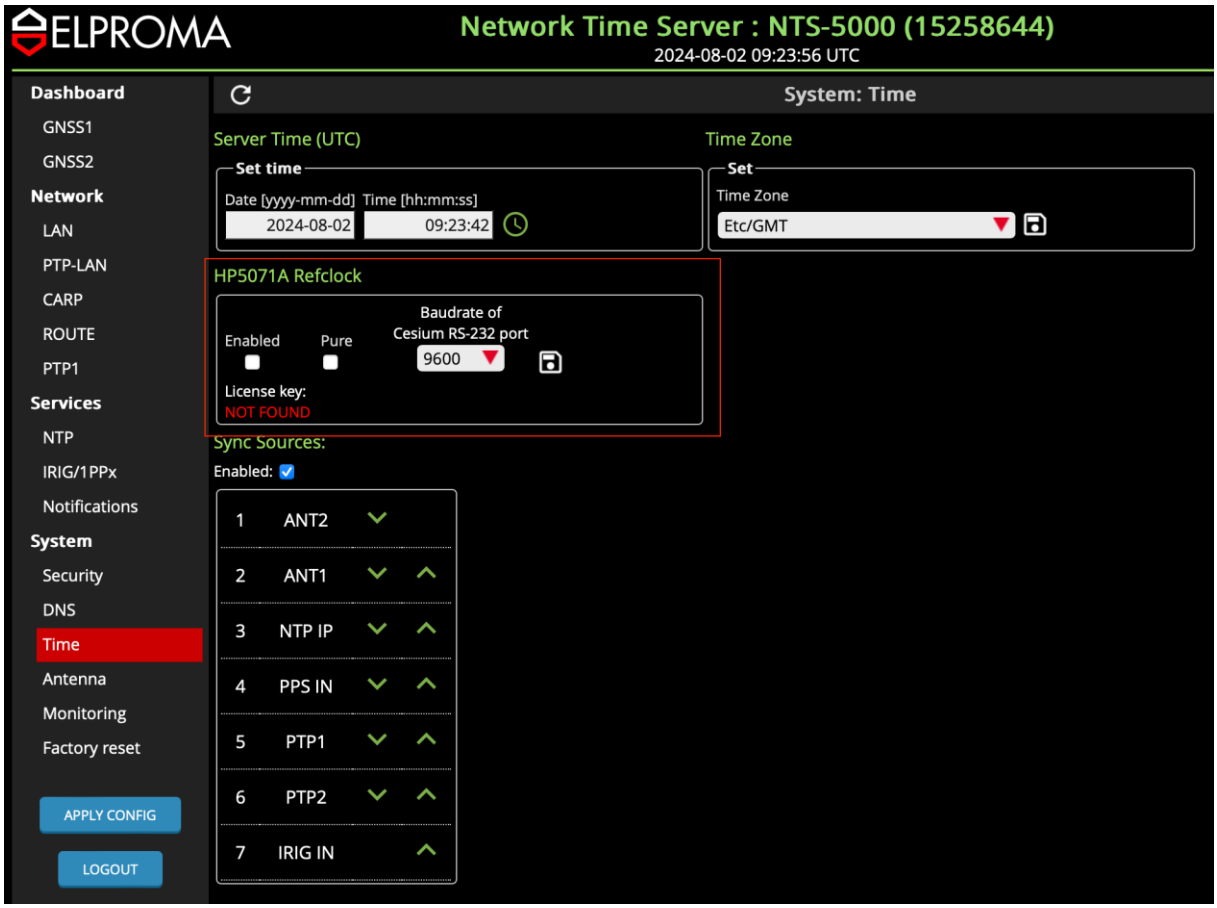
The PC is connected to **back panel** D-SUB9 connector of NTS-x000.
The 5071A is connected to **front panel D-SUB9** connector of NTS-x000.

Your NTS-x000 behaves 100% transparent for all Cesium data and PC telemetry requests.
You will be able to trace Cesium telemetry data on your PC automatically.

Software SETUP.

You are now ready to make one step software setup configuration.
Please execute your favorite web browser to access NTS-x000 software setup using HTTPS

Select “System” from main MENU, then please choose a last row labeled ***“HP5071A Ref clock”***.



The after 2019 setup view

Please select “HP5071A Ref clock” checkbox labeled “ENABLE” to be ON.
This will let NTS-x000 time server begin to receive timing-data from 5071A via rs232 interface.

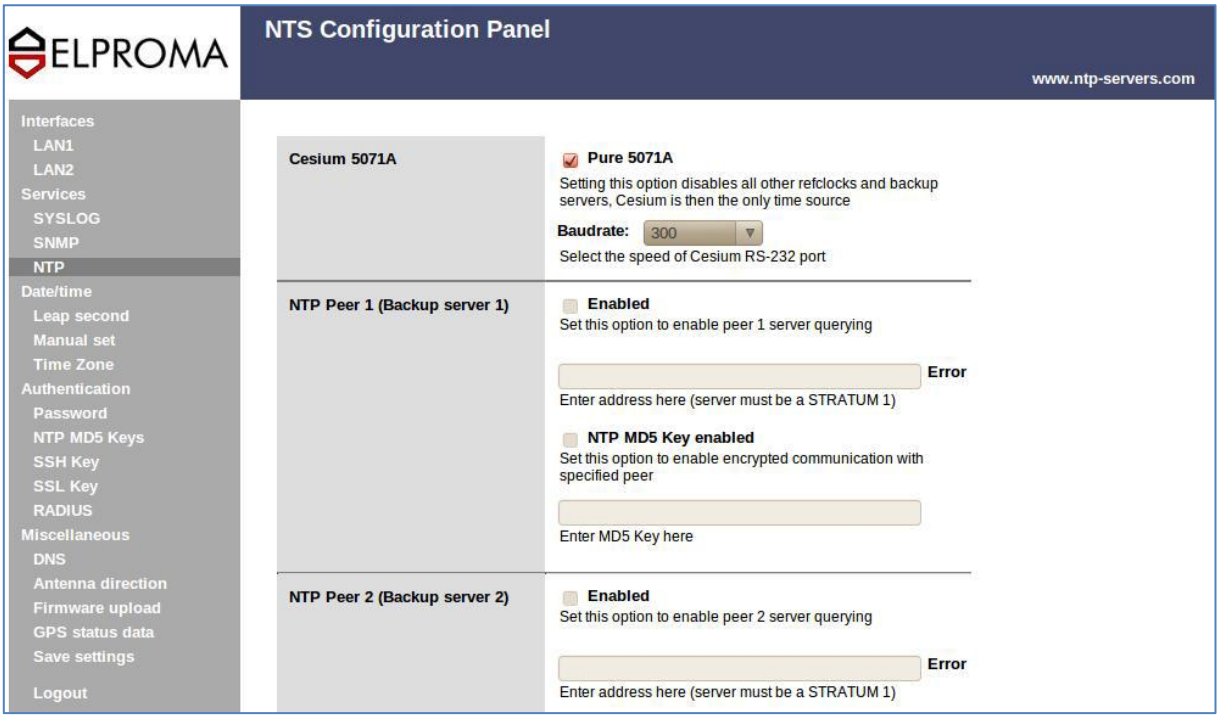
By clicking ON checkbox labeled “PURE”, you will ensure there is no other ref. source of UTC time to be considered by your NTS-x000. This means only 5071A will be your reference of time and frequency. Saying in other words, by selecting PURE=ON, you ensure exclusive use 5071A cesium clock input.

Set correct baudrate (the default baudrate is 300).
Please save setting and restart NTS-x000 server.

You are now ready to use NTS-x000 with 5071A Cesium Clock.
To continue your configuration please refer to software SETUP.

Older software SETUP version (models 2004-2018).
.
Select “Services” from menu - then please choose “NTP”.

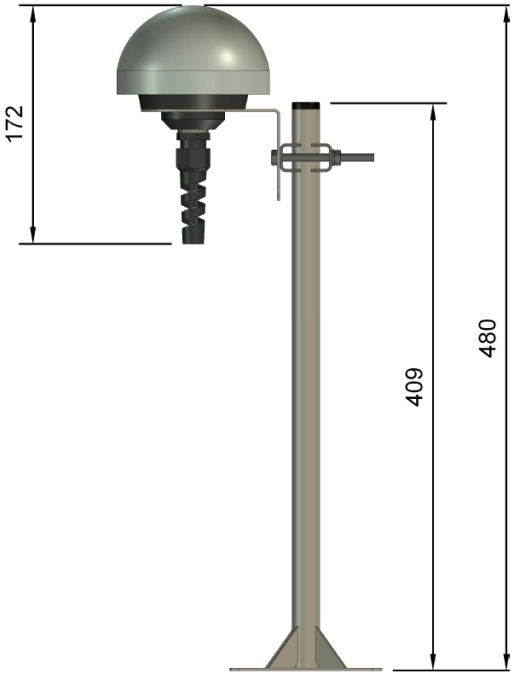
Select checkbox PURE to ensure the 5071A is the only ref. source of time for NTS-x000.
Set correct baudrate (the default baudrate is 300).
Save setting and restart NTS-x000 server

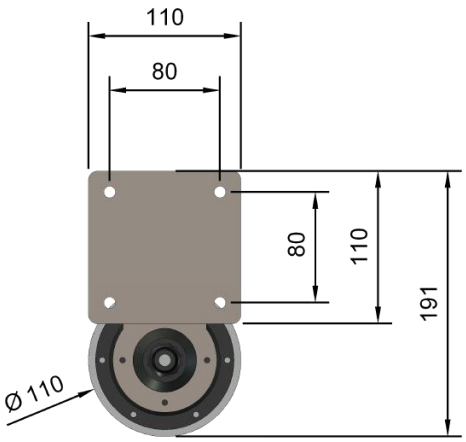


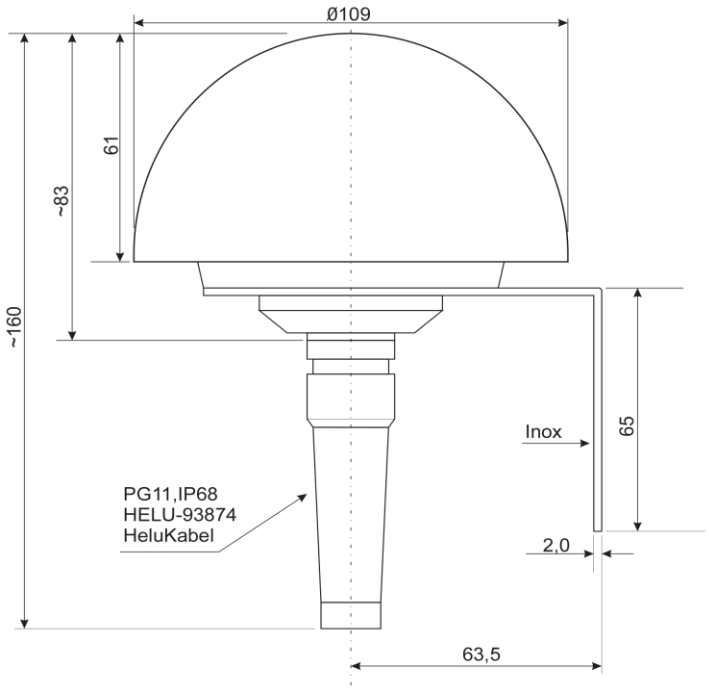
Old 2004-2019 setup view

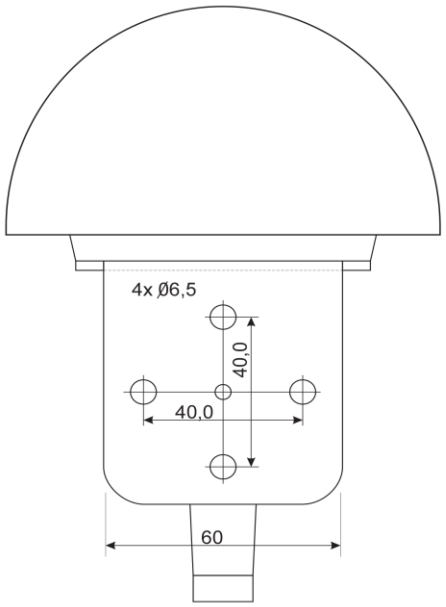
27. Extra Hardware – GNSS NTS-antenna

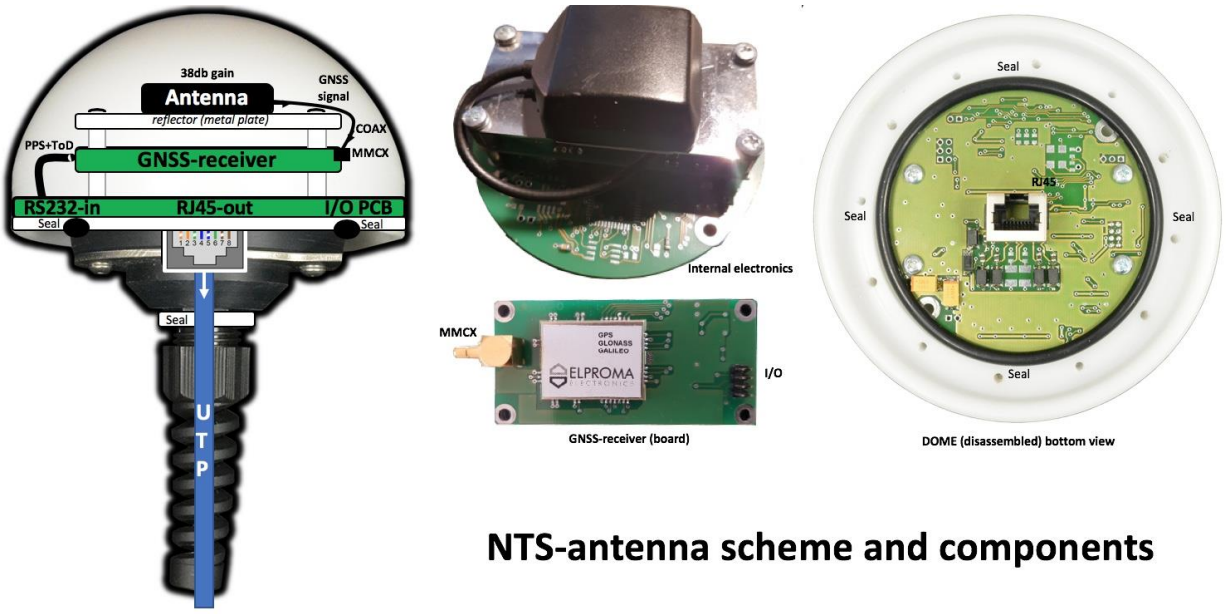
Time server is equipped with 1pcs. of **NTS-antenna,** however it can support max. 2pcs. Antenna is delivered with complete mounting set including *mast, mounting grip, screws.* The receiver will sync automatically with the satellites available after activation without the intervention of the user.



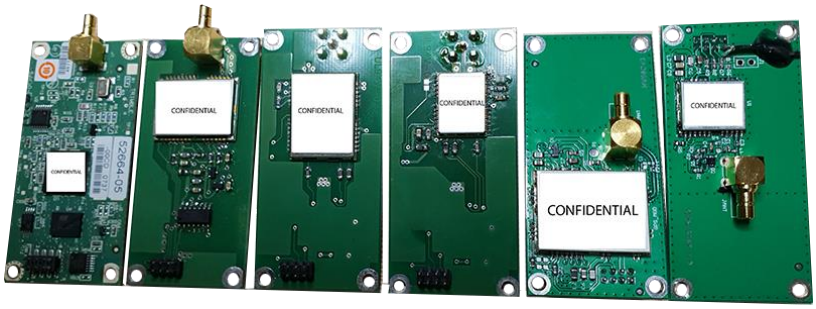








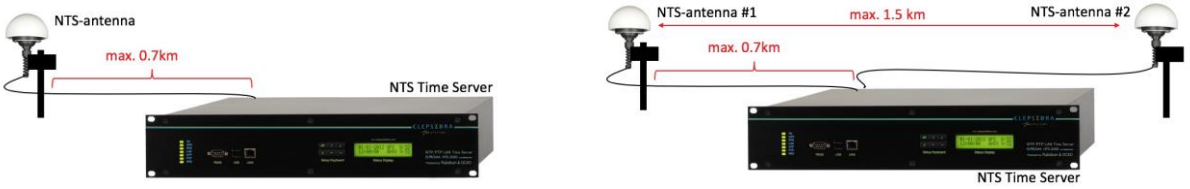
NTS-antenna scheme and components



Standard NTS-antenna is made by vandal resistant DOME housing. Inside there are:

- ***GNSS coil antenna*** *w/ 38dB signal gain (located on special RF reflector plane),*
- *Replaceable* ***GNSS receiver*** *board supporting GPS, GLONASS, BEIDOU,GALILEO,* (selectable ON/OFF to operate exclusively mode GPS-only, GALILEO-only, GPS+GALILEO, GLONASS-only, BEIDOU-only, GLONASS+BEIDoU+GPS)
- *Round* ***I/O*** *frequency converter to electric signal rs485 w/ 1PPS support (RJ45 ended)*

Elproma offers various of exchangeable GNSS-receiver boards each powered by different GNSS receivers. The NTS-antenna is connected to NTS using UTP (unshielded) or STP (shielded) cat.5 cable. The UTP/STP cable is not included and needs to be purchased separately. Elproma always recommend to use external environment version of cable. The maximum distance for single antenna is 0.7km from NTS time server. Using 2pcs. independent NTS-antennas ensure GNSS hardware redundancy, but also it is improving cyber security of solution. Using 2pcs. of antenna enables “geographical” diversification of shortrange jamming/spoofing risk of attack. Antennas can be configured on way will automatically recognise GNSS jamming/spoofing. It will then send the alarm down to server and antenna will switch OFF. Server will continue then in oscillator holdover mode and antenna stays waiting until end of jamming/spoofing. Special algorithm is sensing quality of 1PPS signal selecting correct time reference.

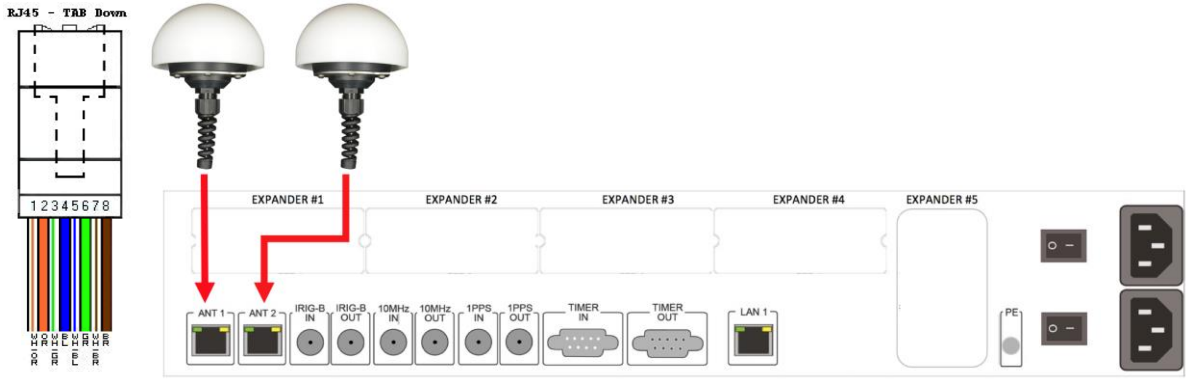


Single NTS-antenna distance is limited to 0.7km. Two antennas reduces risk of jamming/spoofing (“geographical” protection)

Antenna is also prepared to protect anti-jamming/spoofing on another way. The antenna system is built according to the principle that if the system has no reception of external time signals, the risk of external interference is non-existent. Therefore, the antenna (includes receiver) is switched on only for very short

periods and in between an ultra-stable oscillator is used as the time base. The GNSS receiver is switched on for one or two short intervals per day. The specific security policy needs to be discussed with local security authorities. When, the receiver is connected, the received time is checked from several aspects such as time deviation, short and long-term drift, and precision. If all criteria are met, the time is accepted and used for correction of the oscillator and for distribution. If the time for any reason does not meet the requirements, the receiver is disconnected, and an alarm is created.

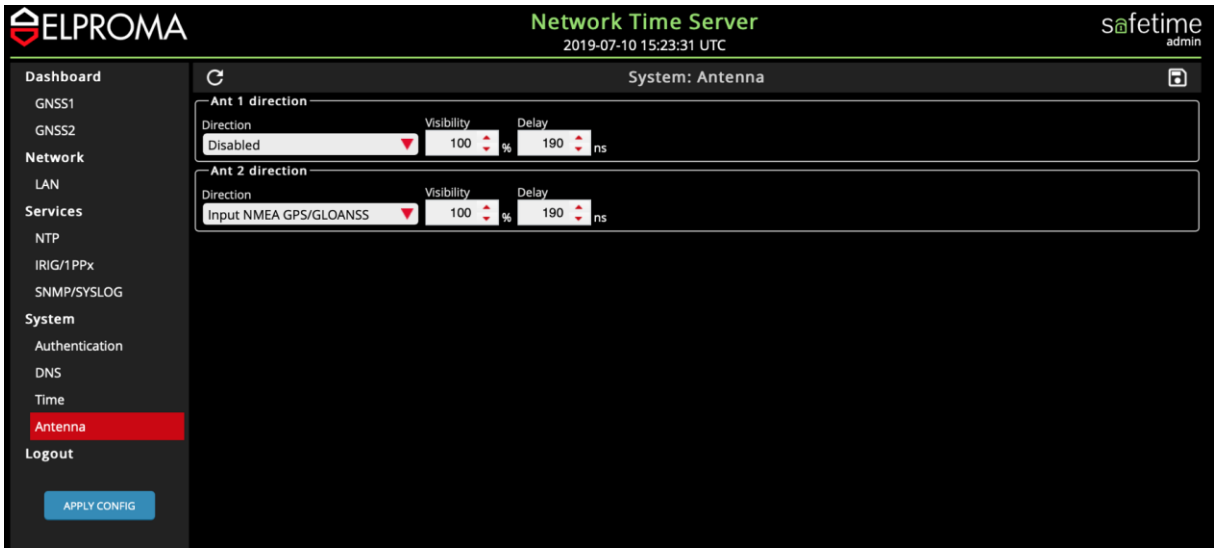
The 2x antennas can be connected on max. distance of 1.5km from each other, enabling “geographical” risk diversification of using portable shortrange jamming/spoofing devices when distance is min. 50m.



ANT-1/ANT-2 RJ45 (pin)	Signals	Std. UTP cable color
1	PPS+	White/Orange
2	PPS-	Orange
3	ToD+ (TR+)	White/Green
4	JAM/SPF- (or DCF-)	Blue
5	JAM/SPF+ (or DCF+)	White/Blue
6	ToD- (TR-)	Green
7	+VCC (+24VDC)	White/Brown
8	0V	Brown
GND	GND	Not used

ANT-1/ANT-2 interfaces can be configured individually from setup level

- **INPUT** supplying ref. time to NTS-antenna in one of modes:
  - **BIN**ARY mode **(default)**, supporting leap second (secured mode)
  - **NMEA**183 text mode, not supporting leap second (unsecured)
- **OUTPUT** emulating NMEA183 to another server
- **OFF** - port is disabled (the antenna power is OFF)



LED indicators

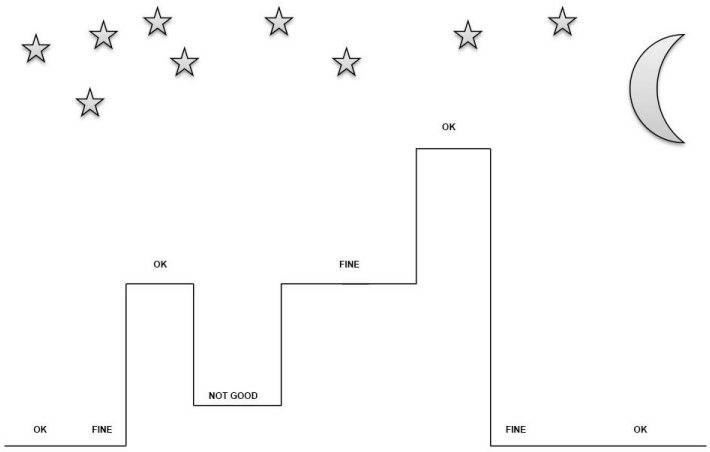
There are 2x LED (red & green) on the back panel of NTS time server (ANT1, ANT2) RJ45 interfaces:

GREEN LED	STATUS
OFF	NTP daemon not started
ON	NTP daemon started
BLINKS (NTS-3000 and -4000)	Synchronized to OCXO *(if option applicable)*
BLINKS (NTS-5000)	Synchronized to 1PPS from external BNC connector, Rubidium or OCXO *(if option applicable)*

RED LED	STATUS
OFF	No GNSS signal
ON	Synchronized to GPS (NMEA)
BLINKS	Synchronized to GPS (1PPS)

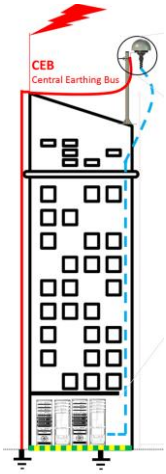
Mounting NTS-antenna

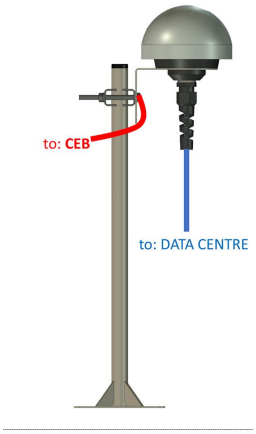
When mounting the antenna, ensure the antenna has a clear view of the full horizon and is at least 2 meters away from telecom, energy transmission sources which may interfere with reception. Avoid the direct path of any microwave links.



"OK" – recommended places, "FINE" – acceptable for multipath-mitigation version, "NOT GOOD" – do not install there

.





When mounting NTS-antenna, please ensure all the mast and bracket are properly grounded to **ECB – The Grounded Central Earthing Bus**. This must be achieved by employing a certified, low impedance connection (a broad, flat lightning conductor strap of sufficient thickness to provide adequate mechanical durability) able to carry the thousands of amperes which may flow. Attaching the antenna mast and mounting clamp onto a pole which is correctly grounded is the recommended method. Optionally another 2nd lightning arrester, a of NTS-protect-2 system should be mounted where the antenna cable enters the building and properly grounded to earth termination.

28. Extra Hardware – Lighting NTS-protect

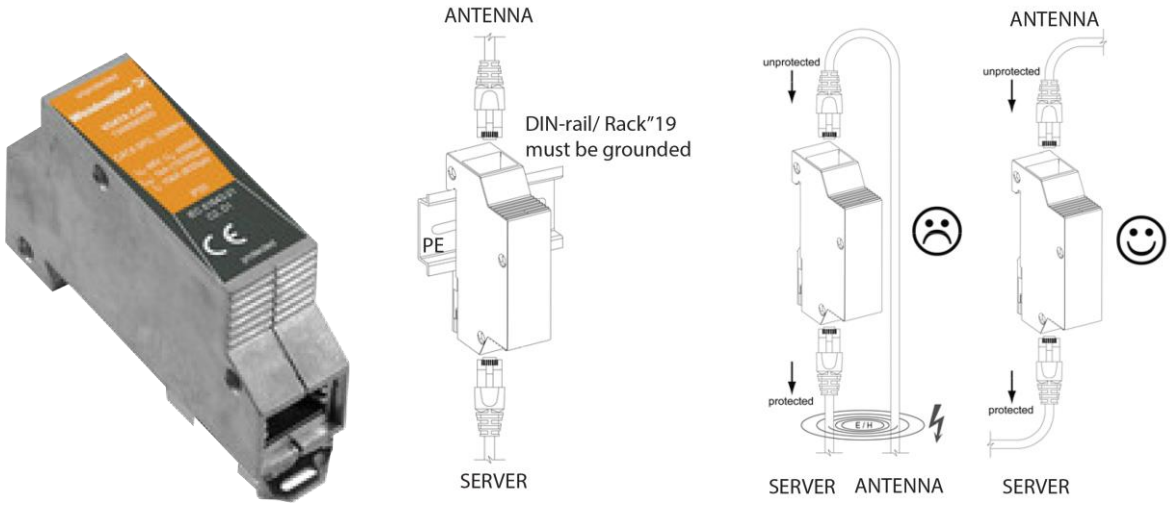
Introduction

As the NTS-antenna is a roof mounted device to ensure clear view of the sky. The cable is UTP Cat5+ offering max. 700m connectivity without signal amplifier. With shielding STP Cat 5+ cable version the distance is up to 1.4km. Therefore, it is likely to be exposed to lightning strikes. The protection against this is afforded by ensuring adequate grounding of all mountings as described below. The NTS-protect basis upon the rule of voltage compensation in accordance with IEC 61024-1 standard. It stipulates upholding safe levels of overvoltage that will not damage the insulation in all protected electrical I/O circuits of the NTS-x000 servers.

The NTS-protect system has been designed so to be in compliance with the regulation *Journal of Laws, No. 75 of June 15, 2002 items 180 and 183* providing that wiring systems should secure against switching overvoltage and lightning surge, and that voltage limiters shall apply thereto.

The Lighting Arrester

Elproma uses Weidmuller lighting arrester type 1348590000 as a basic component of NTS-protect. This product has been well laboratory tested and it is approved for using with all NTS Time Servers. It is ultrafast (1ns switching time), low latency (630 picosecond delay) surge and overvoltage breaker. It is metal housing and therefore, a vandal resistant too. Device is IP20 and can operate -50C to +85C.



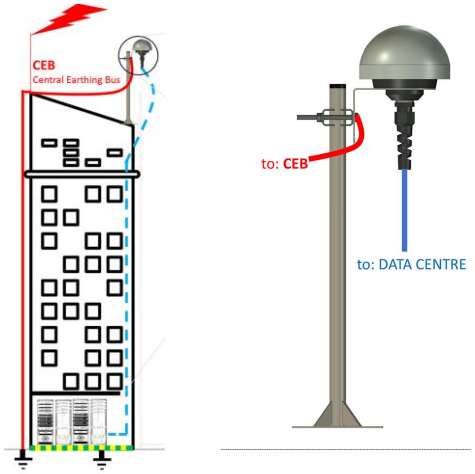
The view of lighting arrester from Weidmuller, *it is very important to ground (PE) arrestor and plane a way of antenna cabling.*

IMPORTANT NOTE! The lightning arresters are never 100% efficient, a residual attenuated electrical pulse being transmitted down the antenna cable, may still contain sufficient energy to damage equipment within the building. Therefore, it is very important to PE ground it and plane a way of cabling.

For above reasons, the 2nd (NTS-protect-2 configuration) or even the 3rd (NTS-protect-3 configuration) lightning arresters might be considered at the begin and at the end of the antenna cable. There are 3 versions of NTS-protect system:

1) **NTS-protect-1** *(std) called* NTS-protect , *a* single arrester system mounted at rack"19 cabinet
2) **NTS-protect-2** *(extended)* NTS-protect-1, plus extra arrester at the entrance of a building
3) **NTS-protect-3** *(max)* NTS-protect-2, plus extra 3rd arrester mounted to antenna mast

.

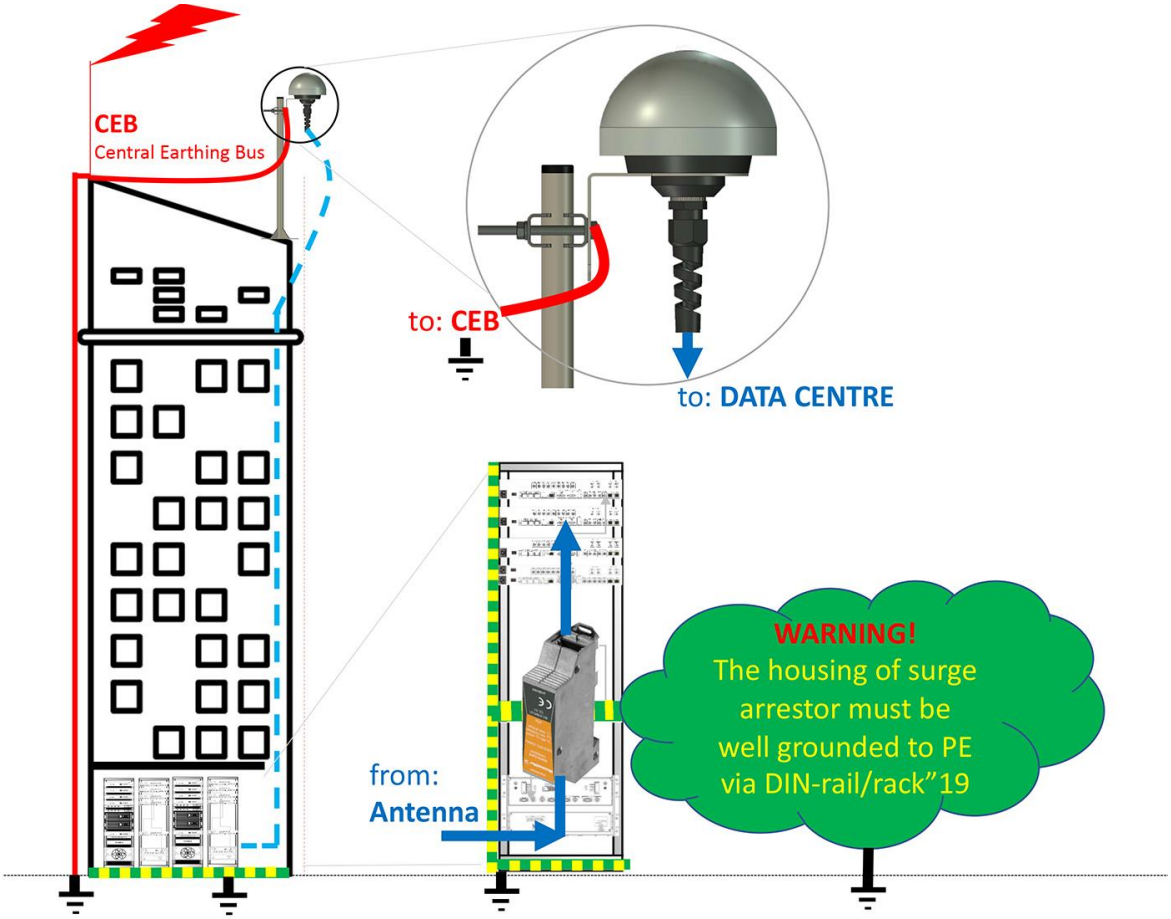


When mounting NTS-antenna, please ensure all the mast and bracket are properly grounded to ECB - Grounded Central Earthing Bus. This must be achieved by employing a certified, low impedance connection (a broad, flat lightning conductor strap of sufficient thickness to provide adequate mechanical durability) able to carry the thousands of amperes which may flow. Attaching the antenna mast and mounting clamp onto a pole which is correctly grounded is the recommended method. Optionally another 2nd lightning arrester, a of NTS-protect-2 system should be mounted where the antenna cable enters the building and properly grounded to earth termination.

The NTS time-server communicates with the GNSS NTS-antenna module via low-signal circuits of the voltage levels not exceeding up 24VDC. The transmission is carried out through std. UTP or STP cat5+ cable of a core diameter equaling 0,5 mm.

Mounting NTS-protect-1

This is default std. single arrester protecting system. The installation is shown on below picture.



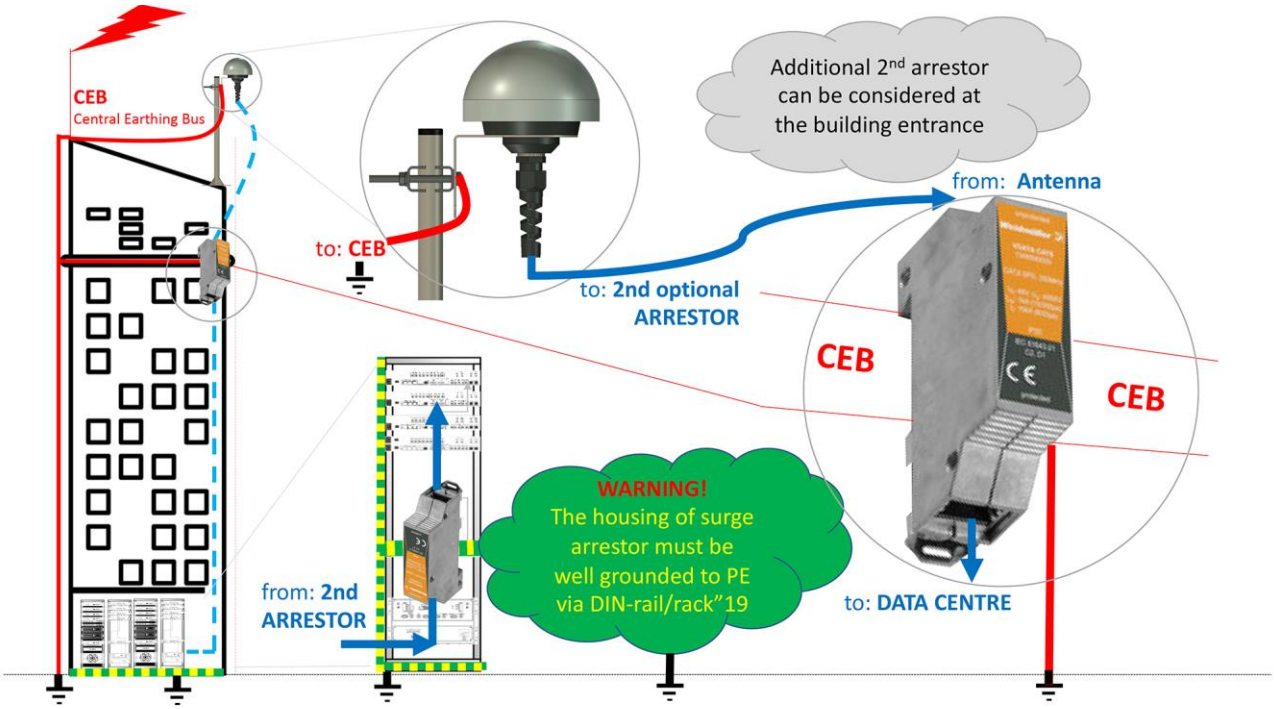
Installation:

1. Ensure the NTS-server is power-OFF.
2. Ensure disconnecting antenna cable from ANT1 (or ANT2) RJ45 interface of NTS
3. Mount DIN-rail on the bottom back part of rack”19 cabinet. Ground it PE to rack”19 cabinet
4. Connect NTS-antenna RJ45 to unprotected (top) signed RJ45, and NTS-x000 to protected RJ45 (bottom) connector of the surge arrester. Use std. RJ45 configuration as described in antenna installation chapter. All arrestor connections a both side pin-2-pin (1-1 etc.).

DIN-rail mounted on the backside of rack”19 cabinet must be grounded (PE)

Mounting NTS-protect-2

This is additional 2nd arrester mounted on the antenna cable at the enter to the building. The NTS-protec-2 includes NTS-protect-1 therefore please refer to previous chapter for instllation instructions. The 2nd arrester should be mounted as near as possible to enter to the building and must be grounded to PE or to external CENTRAL EARTHING BUS.



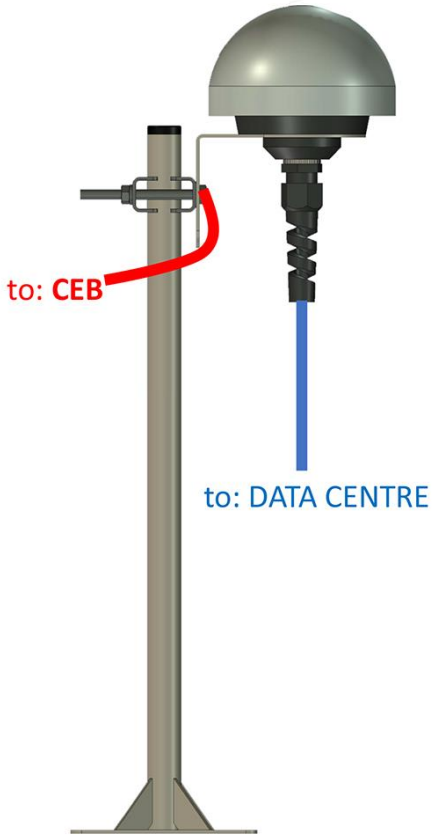
Installation:

1. Ensure the NTS-server is power-OFF.

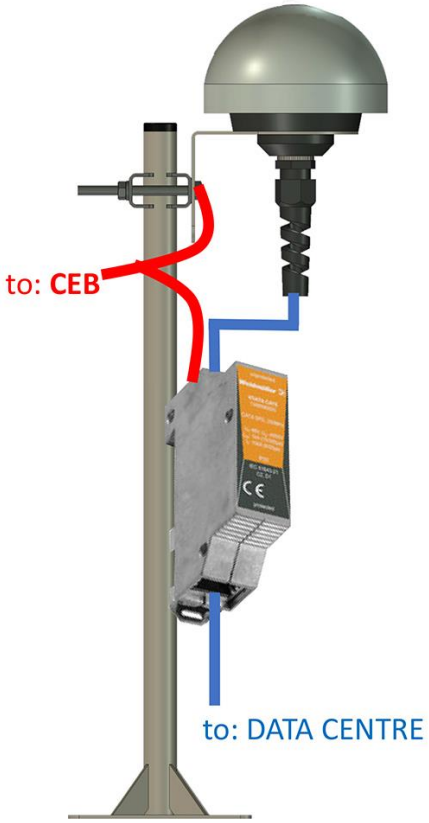
2. Ensure disconnecting antenna cable from NTS-antenna and from ANT1 (ANT2) RJ45
3. Mount 2nd arrester near place antenna cable goes into the building and ground it.
4. Ensure grounding (min. PE) of surge arrester. Best if grounded to CEB.
5. Connect NTS-antenna RJ45 and plug antenna into ANT1/ANT2 of NTS time server

Mounting NTS-protect-3

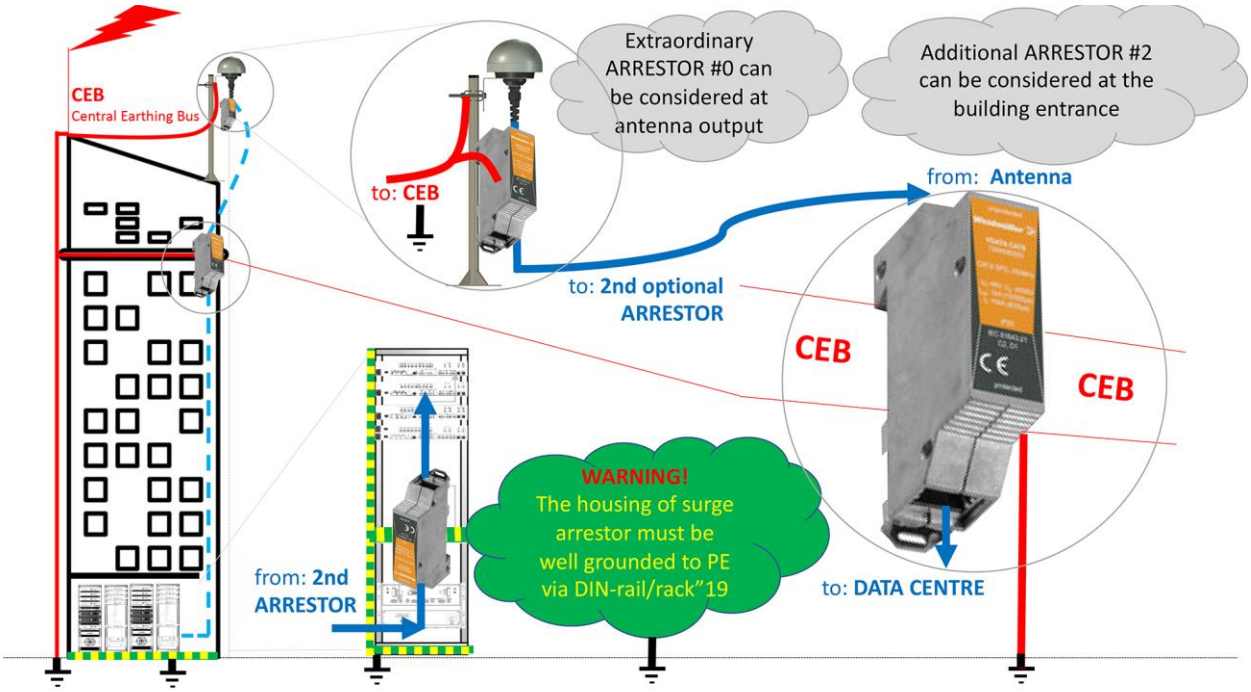
This is the 3rd extraordinary arrester mounted to the mast of NTS-antenna. This option includes NTS-antenna2. (and intermediate automatically it includes NTS-antenna-1 too) so please ref. to previous pages of installation guide first. Actually, the NTS-protect-3 change from std. NTS-antenna to one with extra 3rd arrester mounted on the mast (see below). Currently Elproma does not support waterproof (IP-65/IP-68) housing for 3rd arrester (IP-20). Please purchase housing locally.



NTS-antenna (NTS-protect 1 & 2)



NTS-antenna at NTS-protect-3



NTS-protect-3 installation diagram. The NTS-protect-2 (NTS-protect-1) should be installed first.

29. Extra Hardware – Fiber Optic Converter

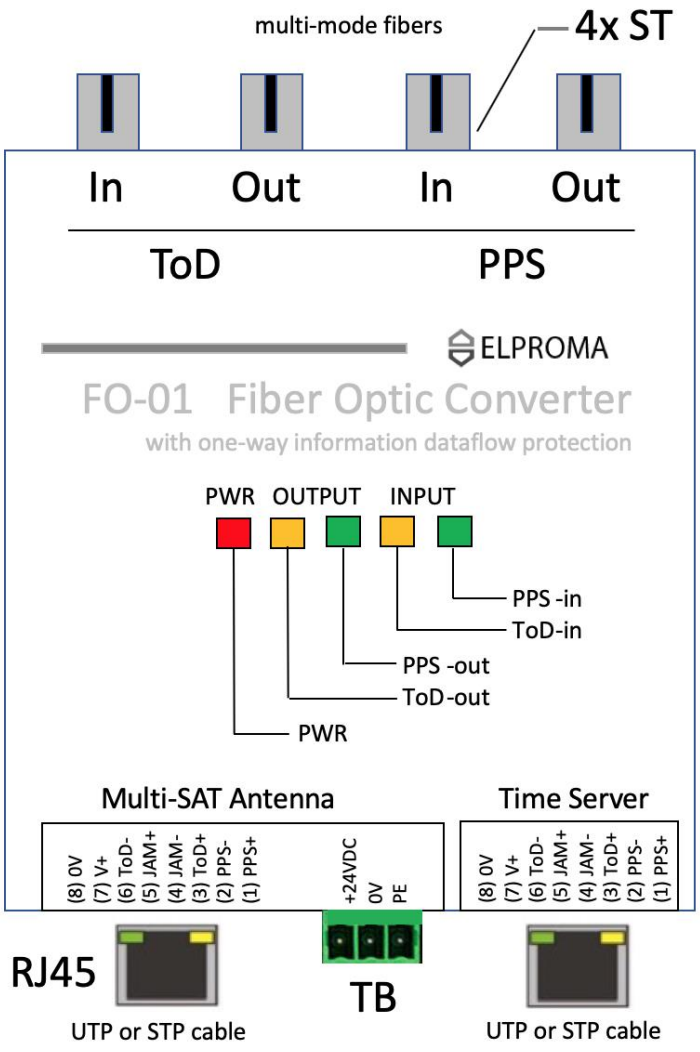
. Introduction

The FO-01 enable fiber optic NTS-antenna connectivity to NTS-x000 (any server model). It is requiring 4pcs. of **multi-mode fibers** to supporting: ToD-in, PPS-in, ToD-out, PPS-out. Minimum configuration is requiring pair of FO-01 device: one for Master (sender) to support NTS-antenna, 2nd Slave (receiver) to support NTS-x000 server. More advanced configurations enable functionality of sharing single NTS-antenna between multiple NTS-x000 time servers.

The max. fiber connection distance is 1.5km (1 mile) end-to-end device. No intermediate devices such as: switches, routers, splitters, amplifiers are allowed between FO-01 devices. To ensure NATO standards of cyber-security the FO-01 scheme and BOM is available on request for security auditors.

The FO-01 device is symmetric, and it does not meter if it will support antenna or server. However, in case of NTS-antenna side FO-01 converter requires extra external power supply 24VDC. The FO-01 time server side is powered directly from NTS-x000 via RJ45 electric interface.

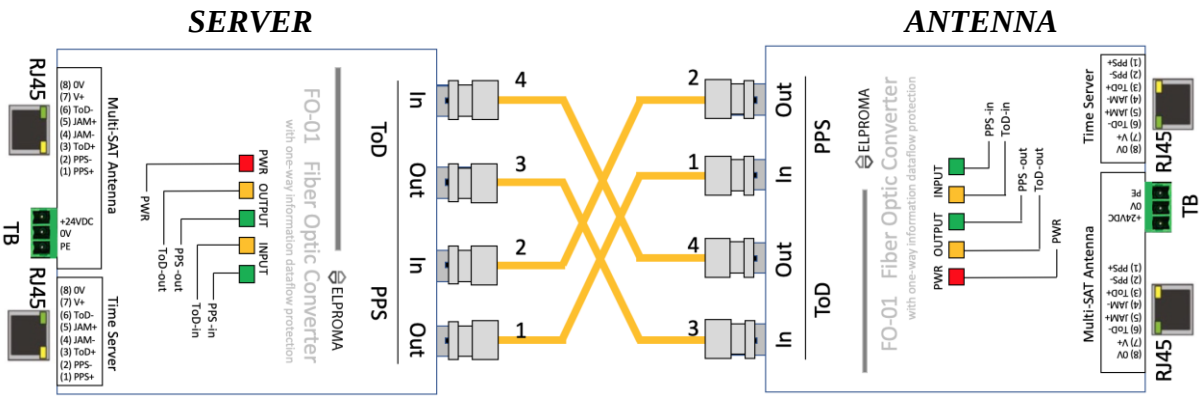
The FO-01 is ready to use device, fully automatic unit with auto configuration.



FO-01 Electric-2-Fiber Connector. Antenna side requires external power supply +24VDC connected via terminal block (TB)

. Intercom multi-mode fiber connection

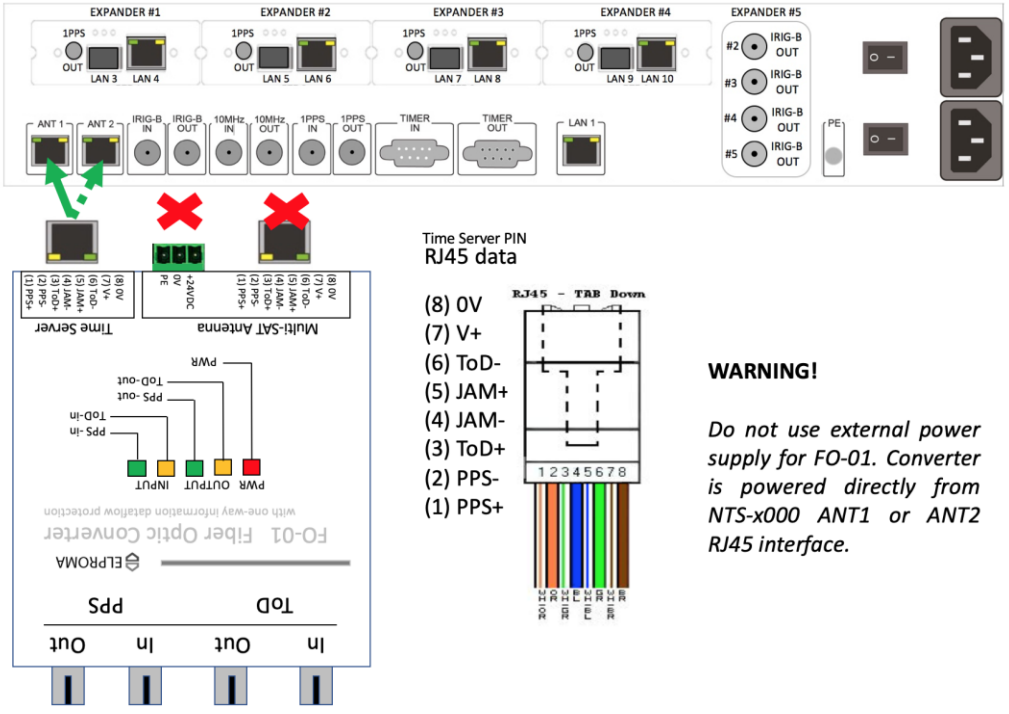
To connect pare of FO-01 devices please use 4pcs. of multi-mode fibers max. 1.5km and connect them using crossed configuration as presented below:



Intercom fiber connection of single pair of FO-01

. Connection Converter To Server

You can use both ANT1 and/or ANT2 server interface RJ45 for connecting FO-01 to NTS-x000 time server. In this configuration FO-01 is powered directly from NTS-x000 time server interface. The max. UTP/STP cable connection between FO-01 and NTS-x000 is limited to 0.7 km.

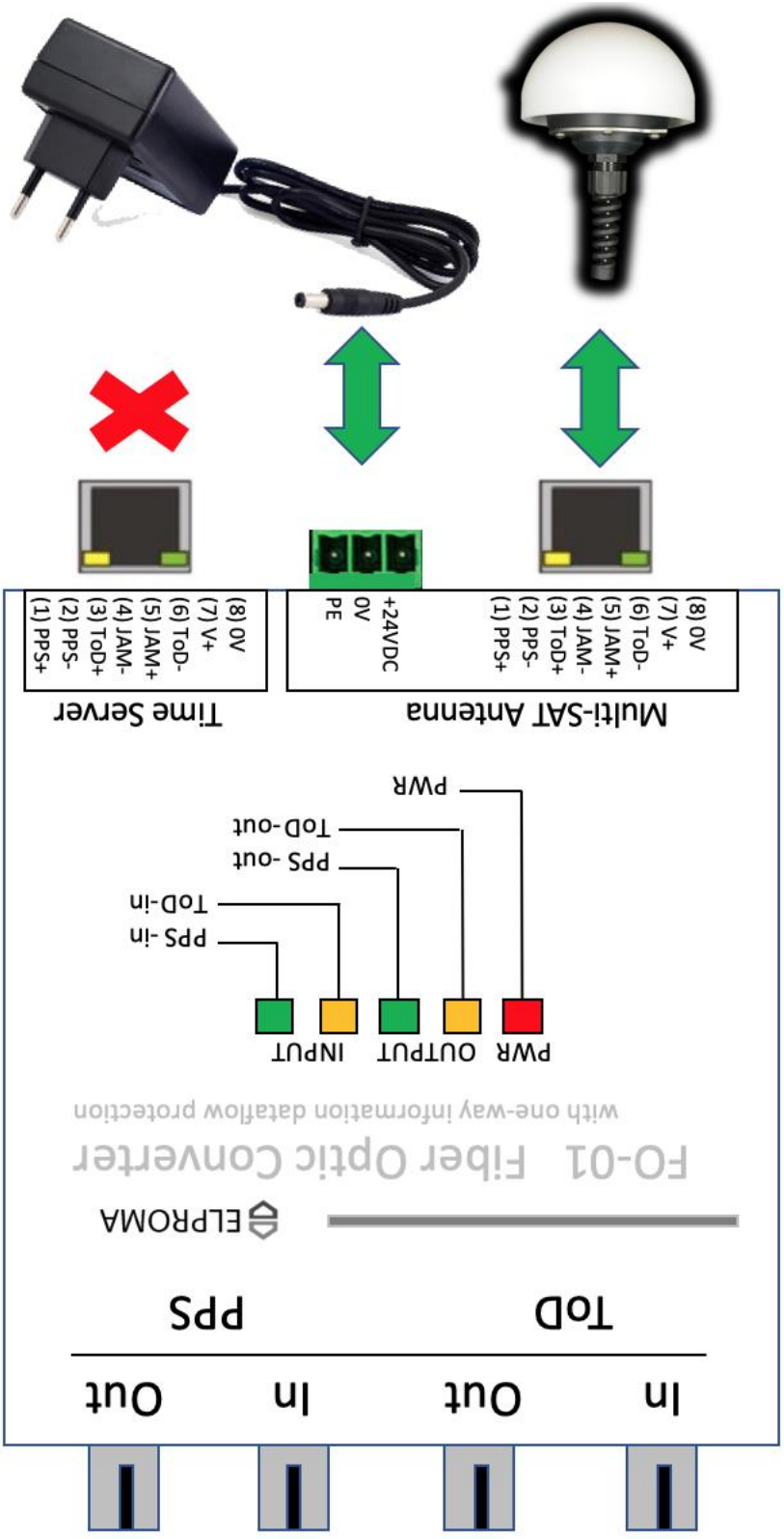


WARNING!

Do not use external power supply for FO-01. Converter is powered directly from NTS-x000 ANT1 or ANT2 RJ45 interface.

. Connection Converter To Antenna

When connecting NTS-antenna and FO-01 there is necessary to use external AC/DC power supply. The max. UTP/STP cable connection between FO-01 and NTS-antenna is limited to 0.7 km.



You can use UTP cat 5. On max. distance of 0.7km from FO-01 supplying NTS-antenna. This side requires external power supply 24VDC

Setup WWW

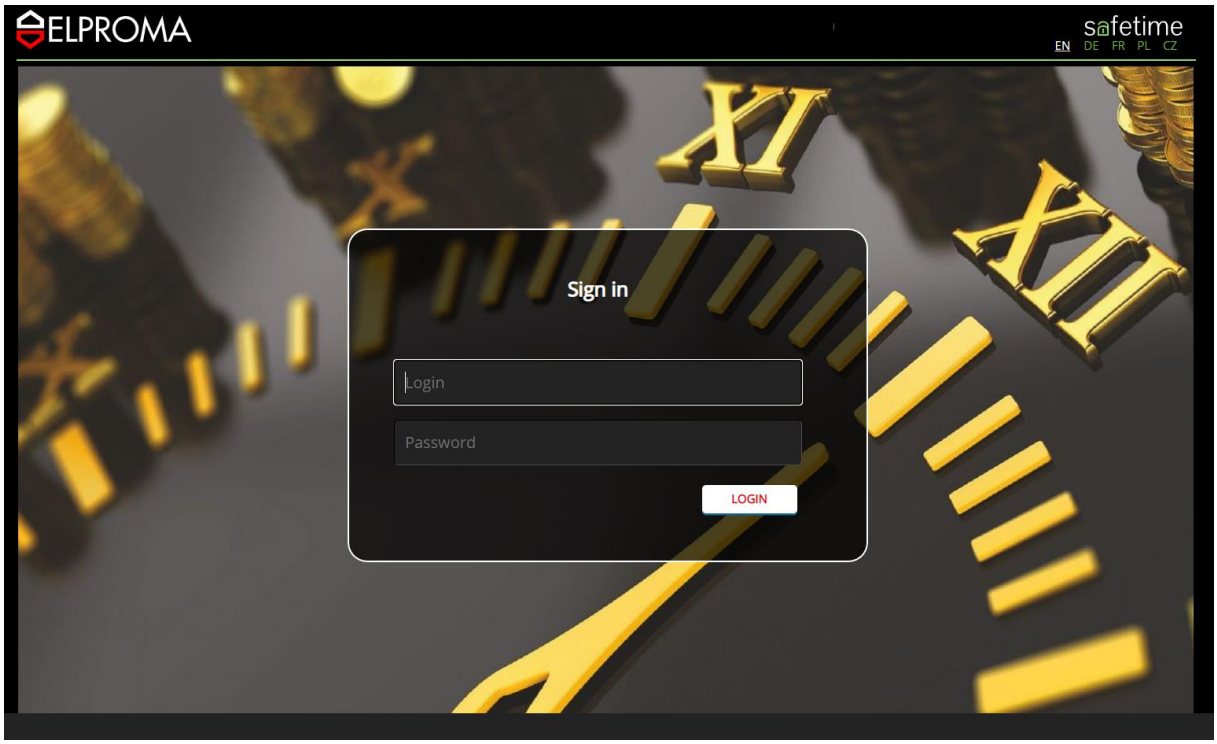
30. Software WWW – Login

IMPORTANT NOTE! New web setup is not compatible with Internet Explorer (IE) browser. All other browsers are supported. Elproma recommends **Chrome** and **Firefox** web browsers.

New web SETUP is available via LAN1 or LAN2 interface only. Other interfaces as LAN3-LAN10* does not support software SETUP directly, and they can be configured via LAN1-LAN2 only. Please connect your PC to LAN first, and ensure it operates in same IPv4 subnet. The factory defaults are specified earlier in chapter “QUICK INFO – Restoring Factory Defaults”. Only single exclusive access is available per single server. If you access it via LAN1 the setup will not be available via LAN2 or RS232 etc. Please type LAN1 (LAN2) IPv4 address in your favourite web browser. Press the lock icon located in right upper corner of screen to activate LOGIN screen. The user default login and password are:

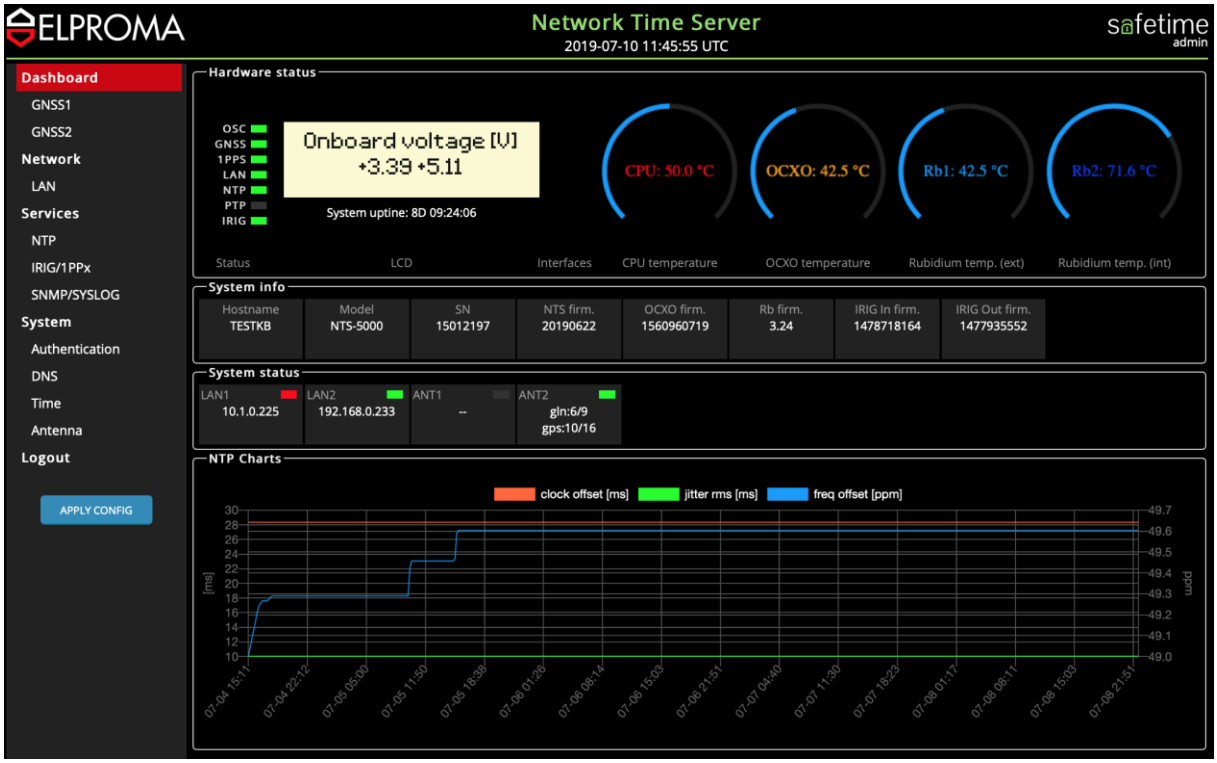
Username: **admin**
Password: **12345**

and click LOGIN button located below.

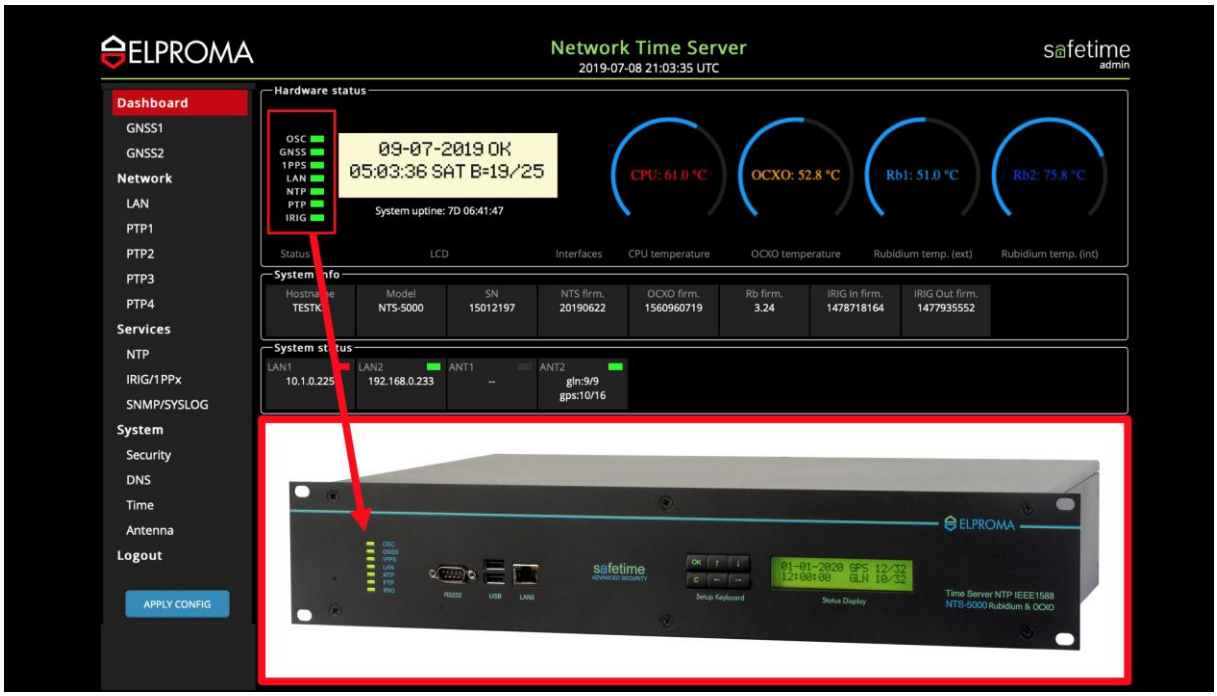


31. Software WWW – Main Screen (SCADA)

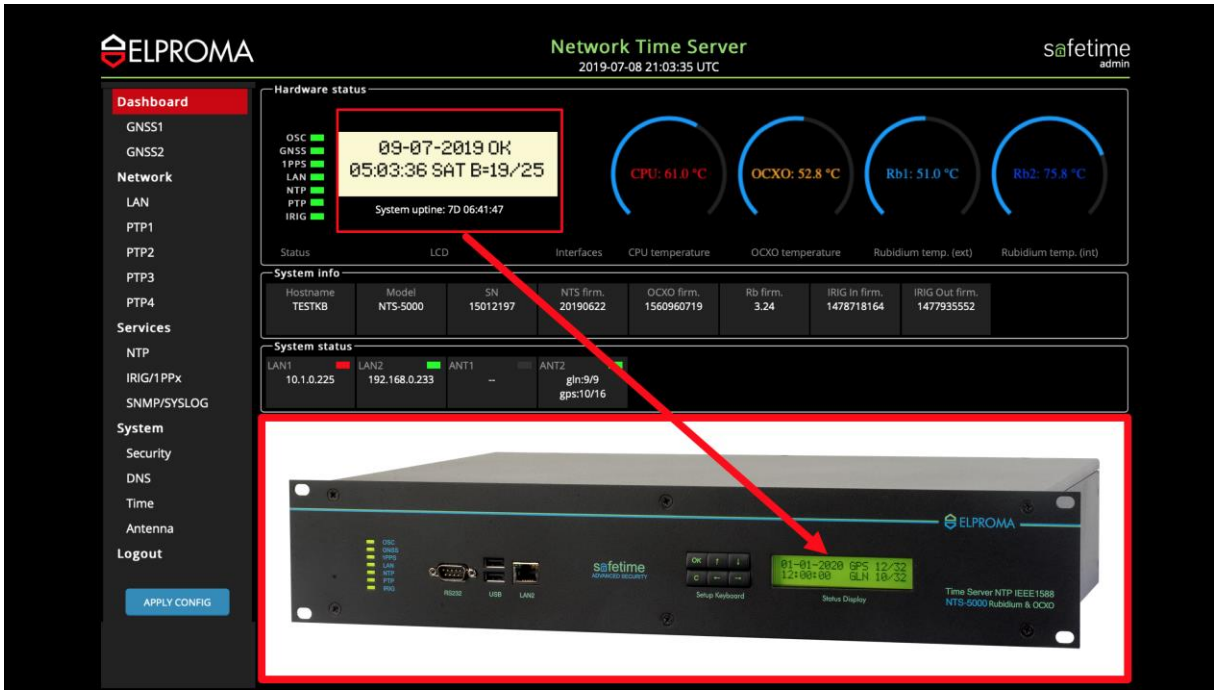
Directly, after successful LOGIN the main DASHBOARD screen appears.



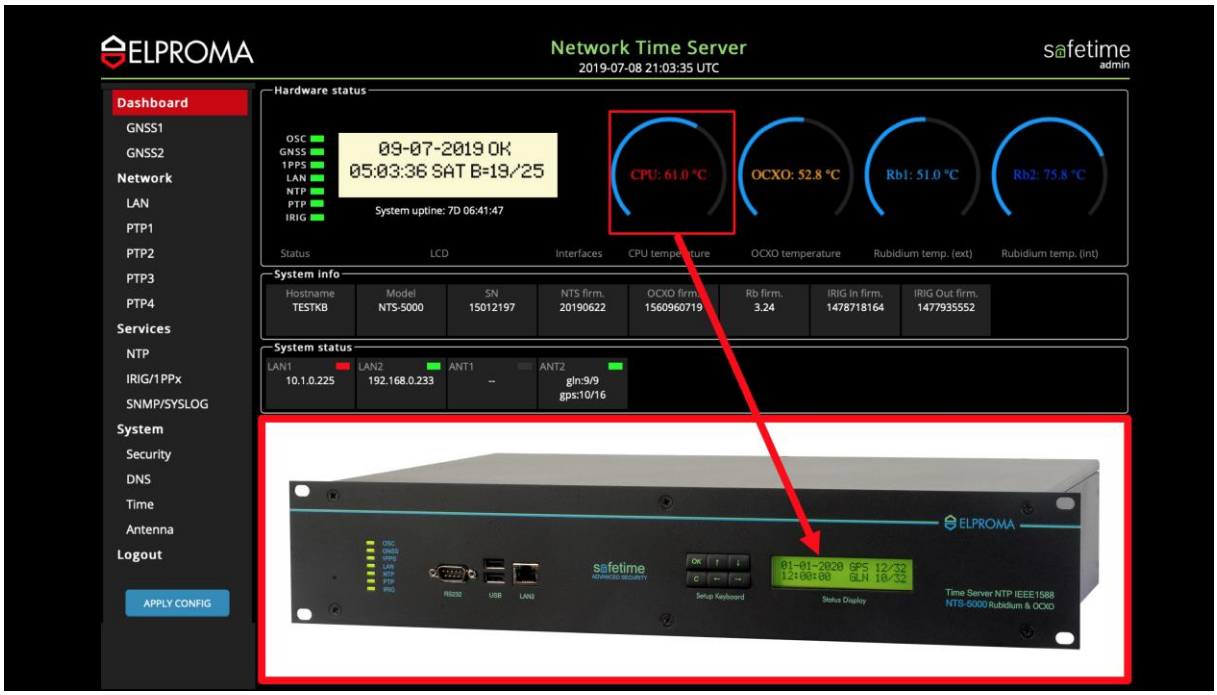
The DASHBOARD of a new SOFTWARE WWW setup keeps basic SCADA monitoring functionalities. The following parameters corresponds real-time to data available on physical front panel of NTS-x000.



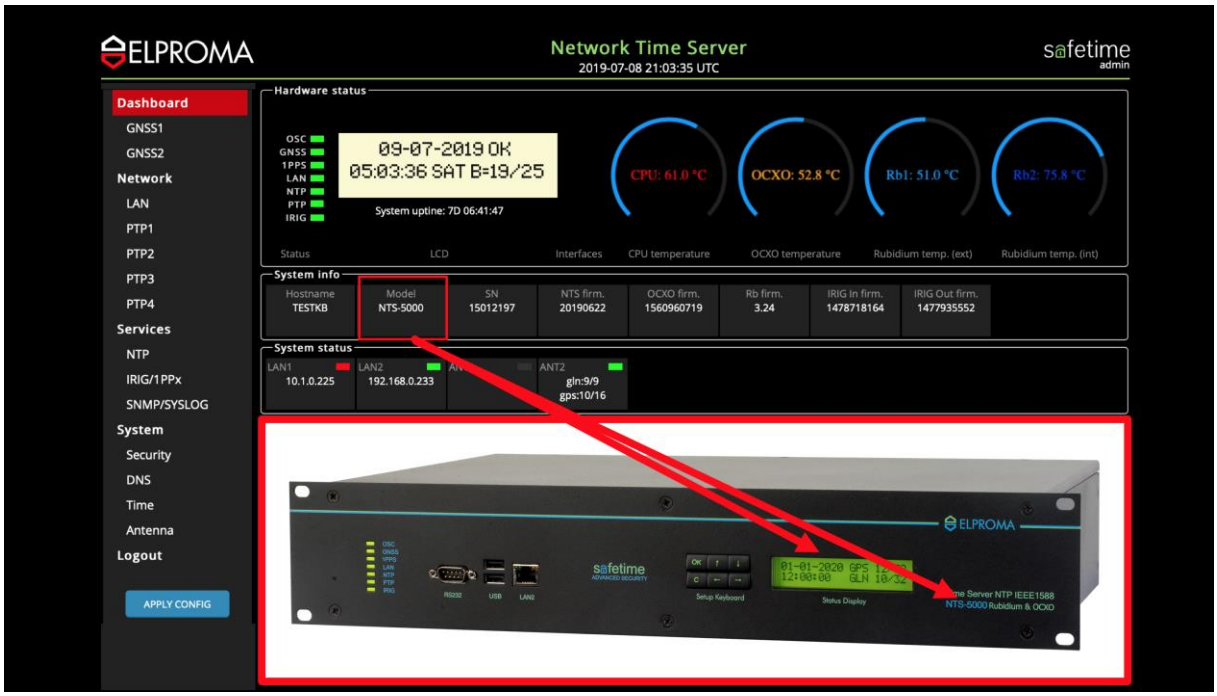
6x LED indicators (from left: OSC, GNSS, PPS, LAN, NTP, PTP, IRIG)



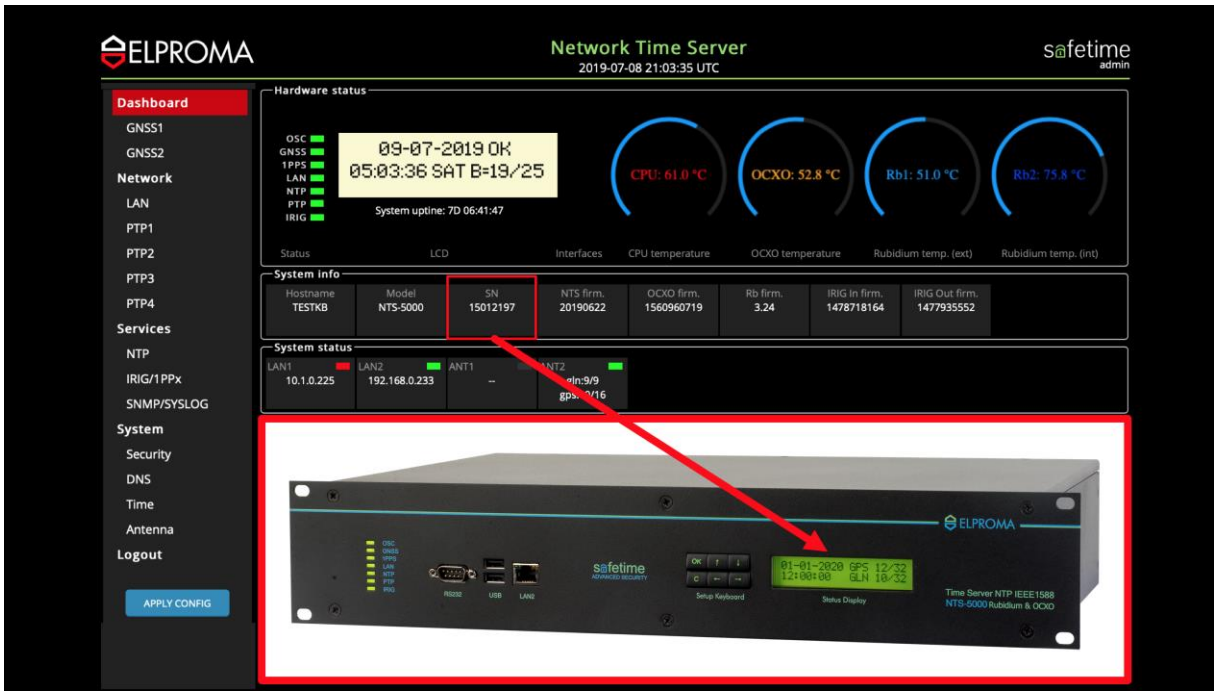
2x 20-character green colour LCD display with date & time, and GNSS satellite basic status



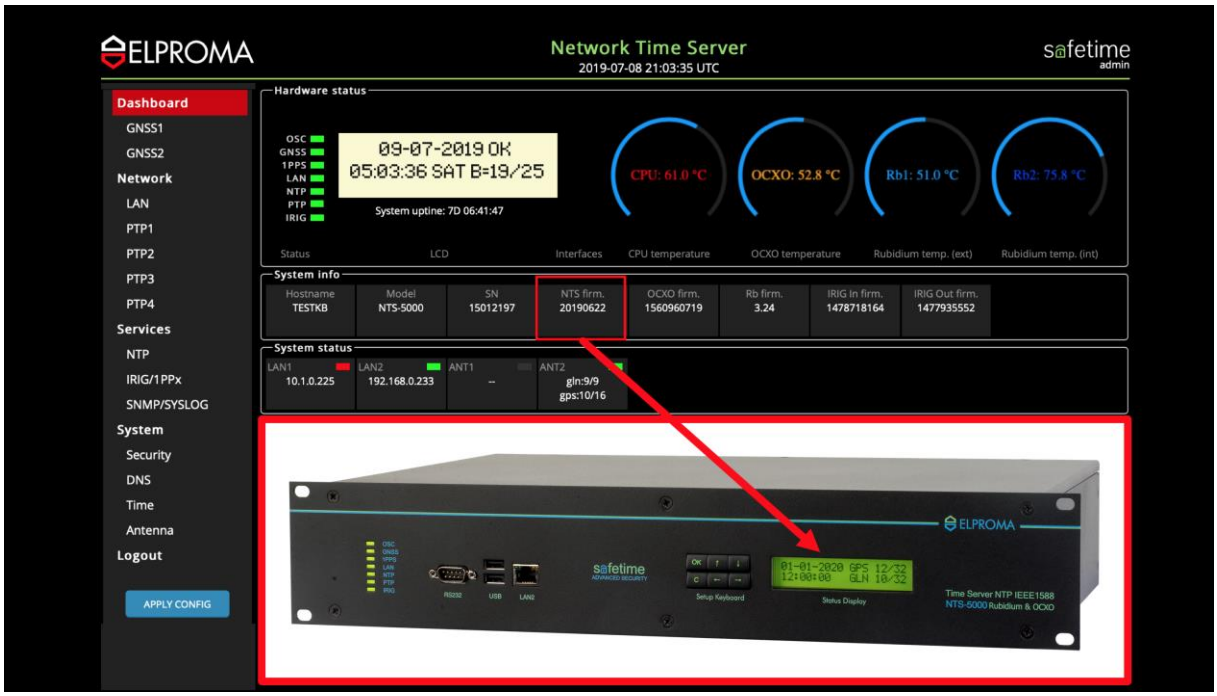
Temperature information (every 5 min. visible on LCD)



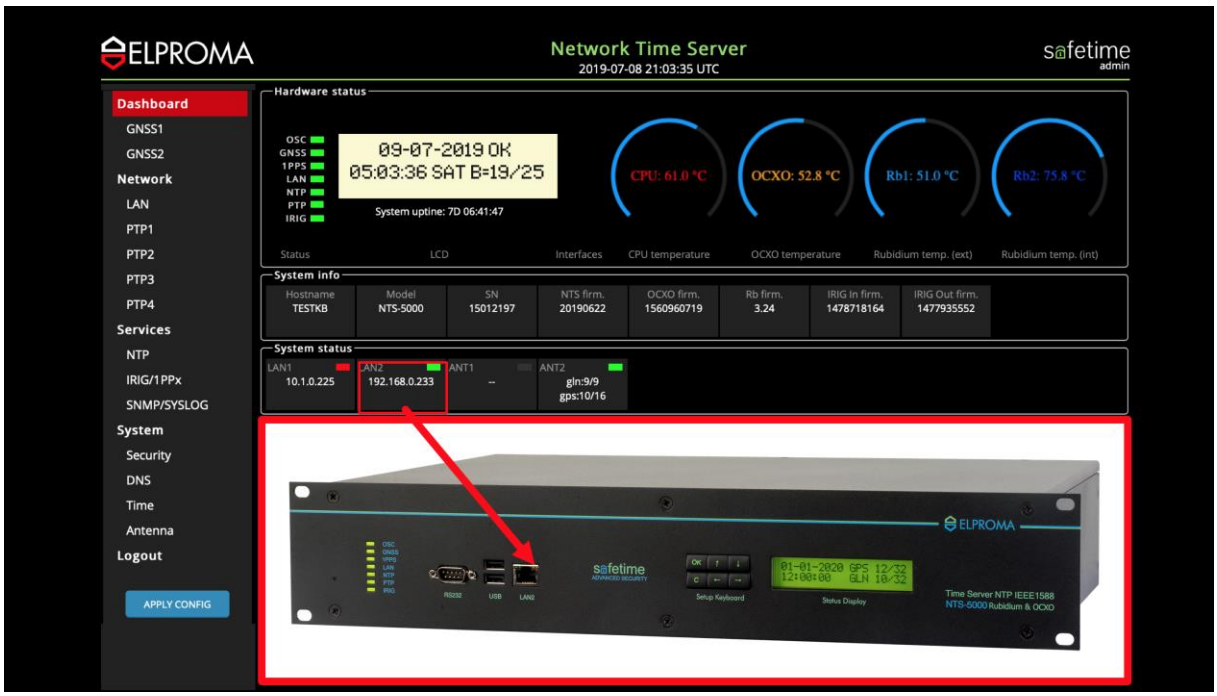
Model (e.g. NTS-5000) available on LCD after power-on. Also located on the right side of front panel



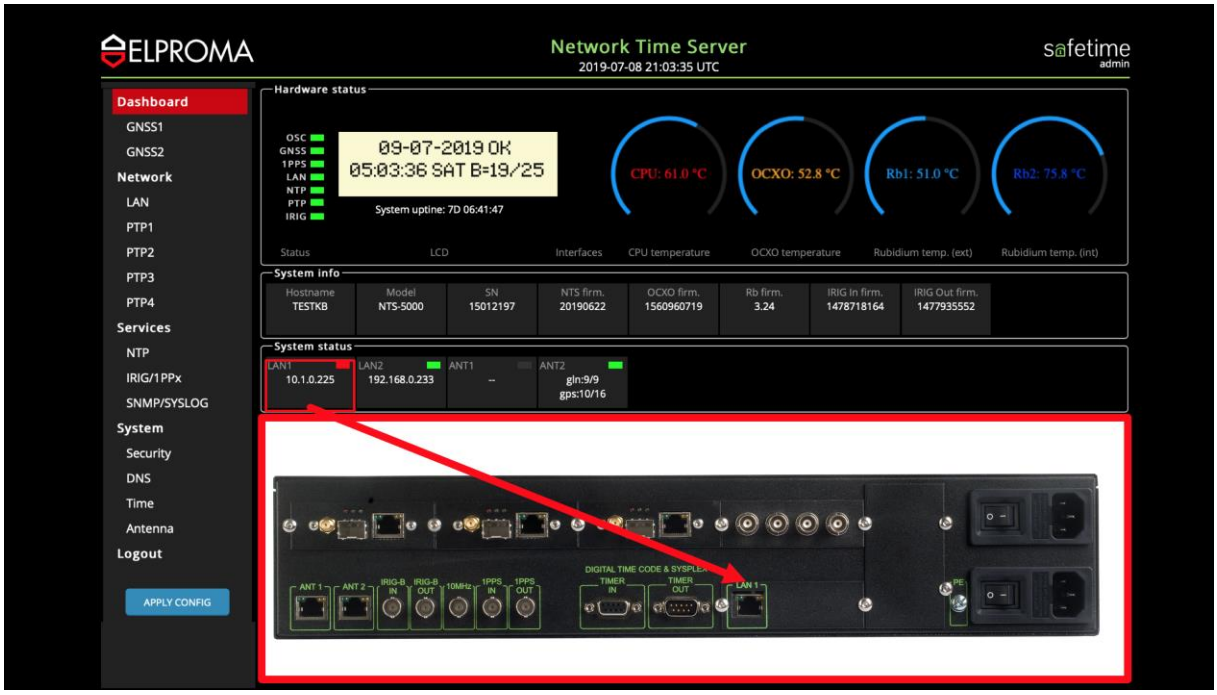
Serial number available on LCD after power-on. Also located on the back-panel S/N sticker



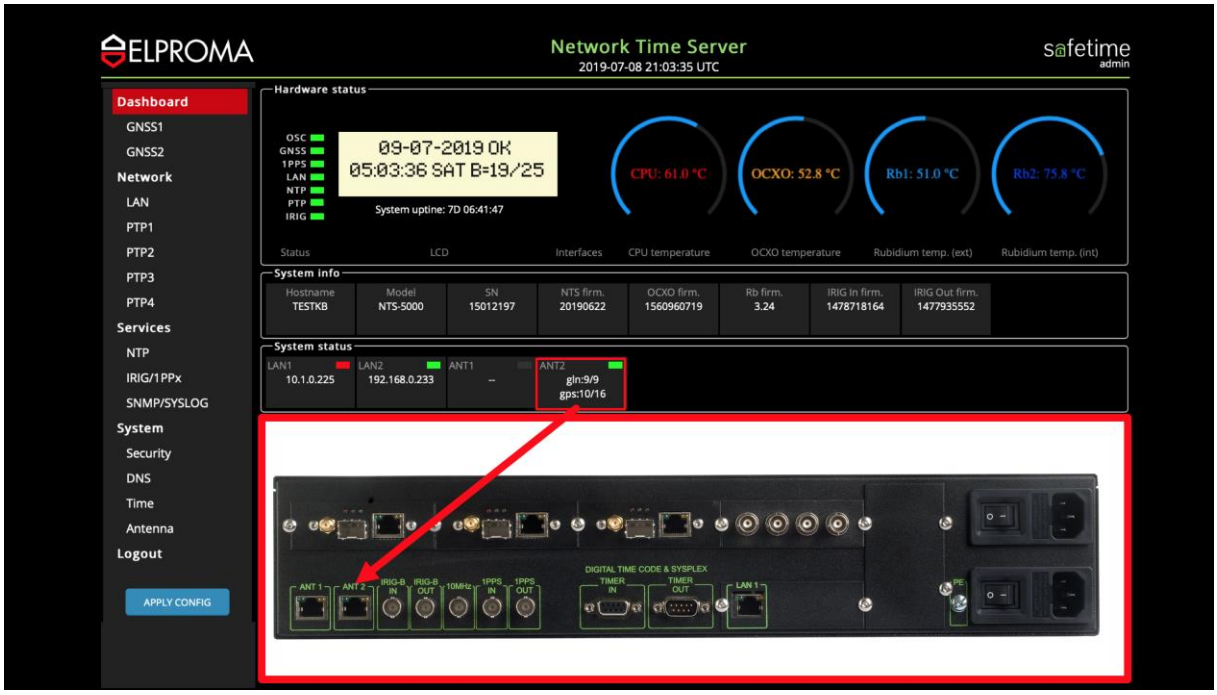
Firmware serial available on LCD after power-on. Also available as KEYBOARD command sequence



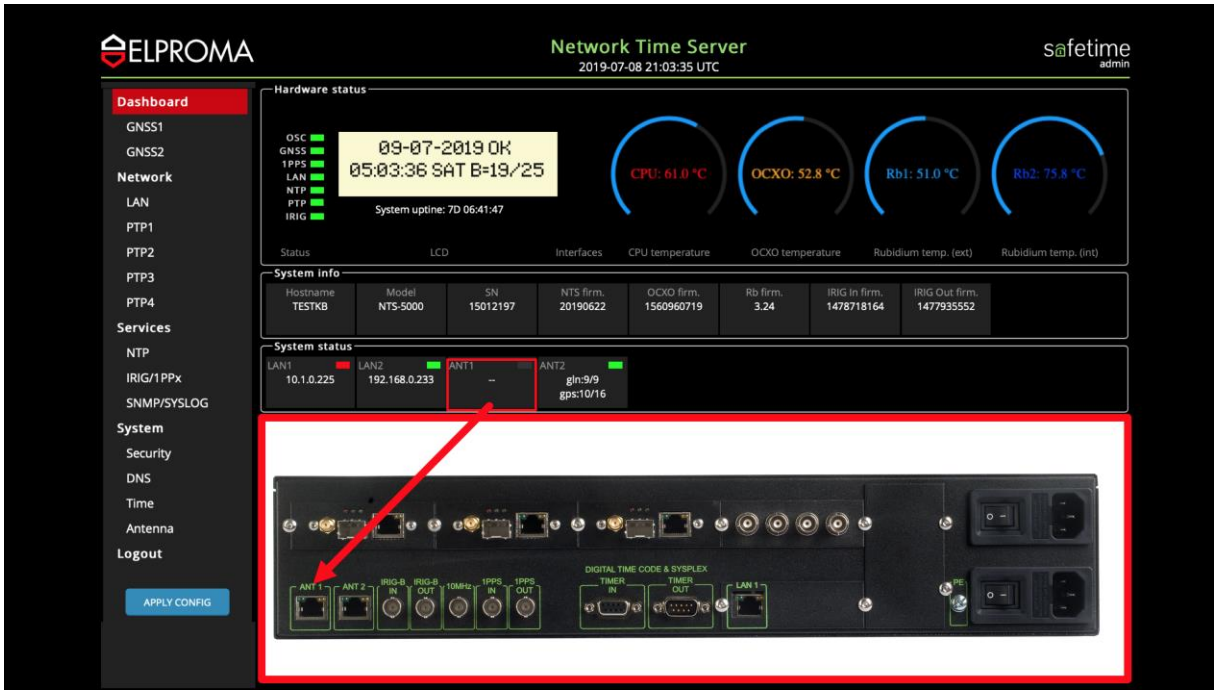
IPv4 address & LAN2 front panel LED indicator (flash green when Ethernet network cable connected)



IPv4 address & LAN1 back panel LED indicator (flash red when Ethernet network cable disconnected)

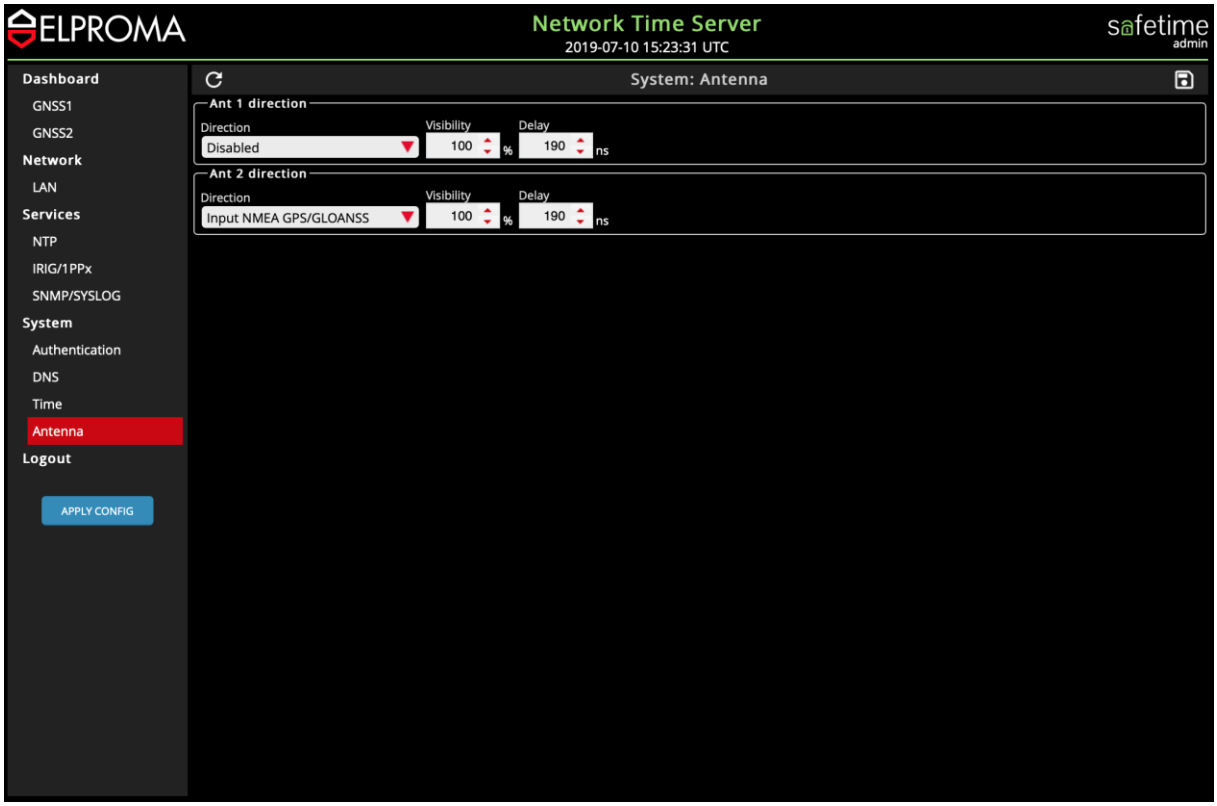


ANT2 back panel LED indicator (blank is NTS-antenna disconnected), and number of SAT is display



ANT1 back panel LED indicator (blank is NTS-antenna disconnected)

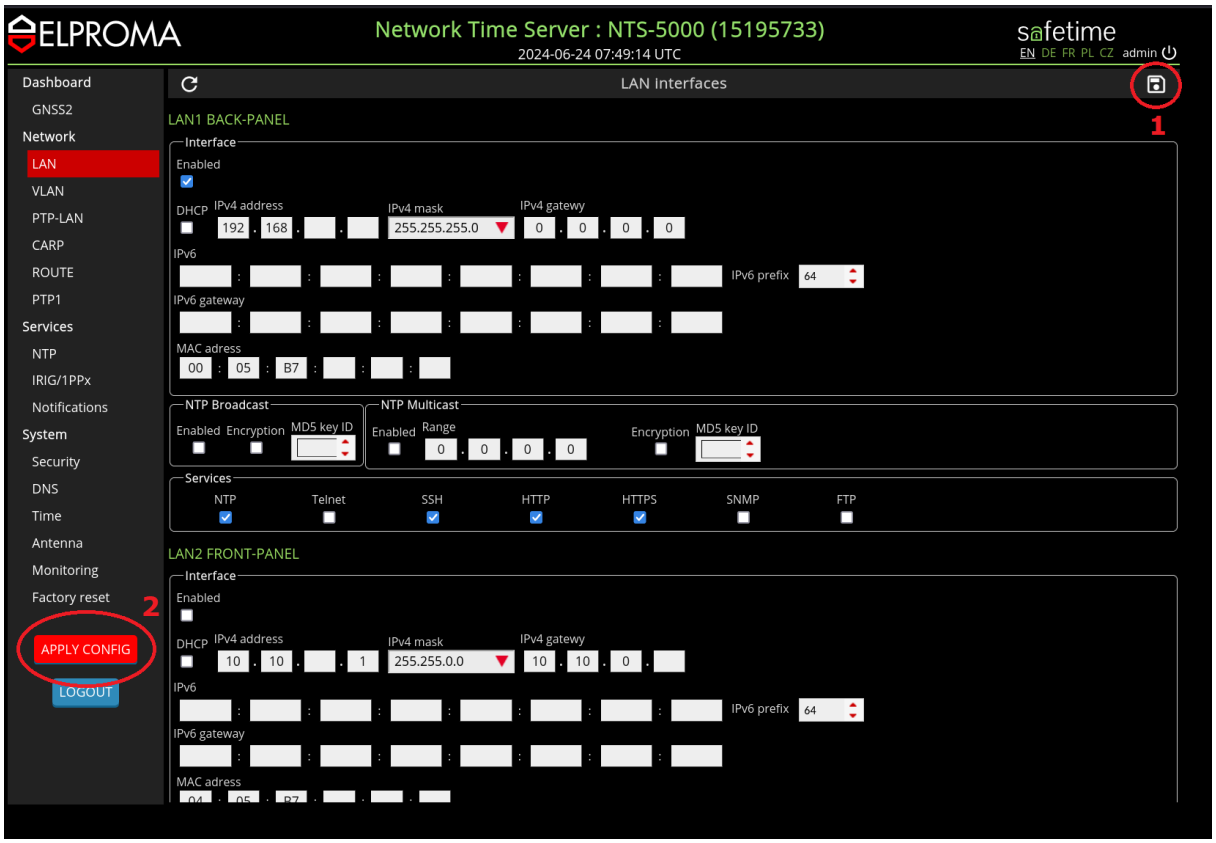
***IMPORTANT**! Please note, when NTS-antenna disconnected also do not forget to disable software setup level interface, otherwise a RED colour LED will flesh generating false alarm.*



ANT-1 is disabled at Antenna Submenu item, ANT-2 is enabled and set to text NMEA183 mode

32. Software WWW – Saving & Exit Config

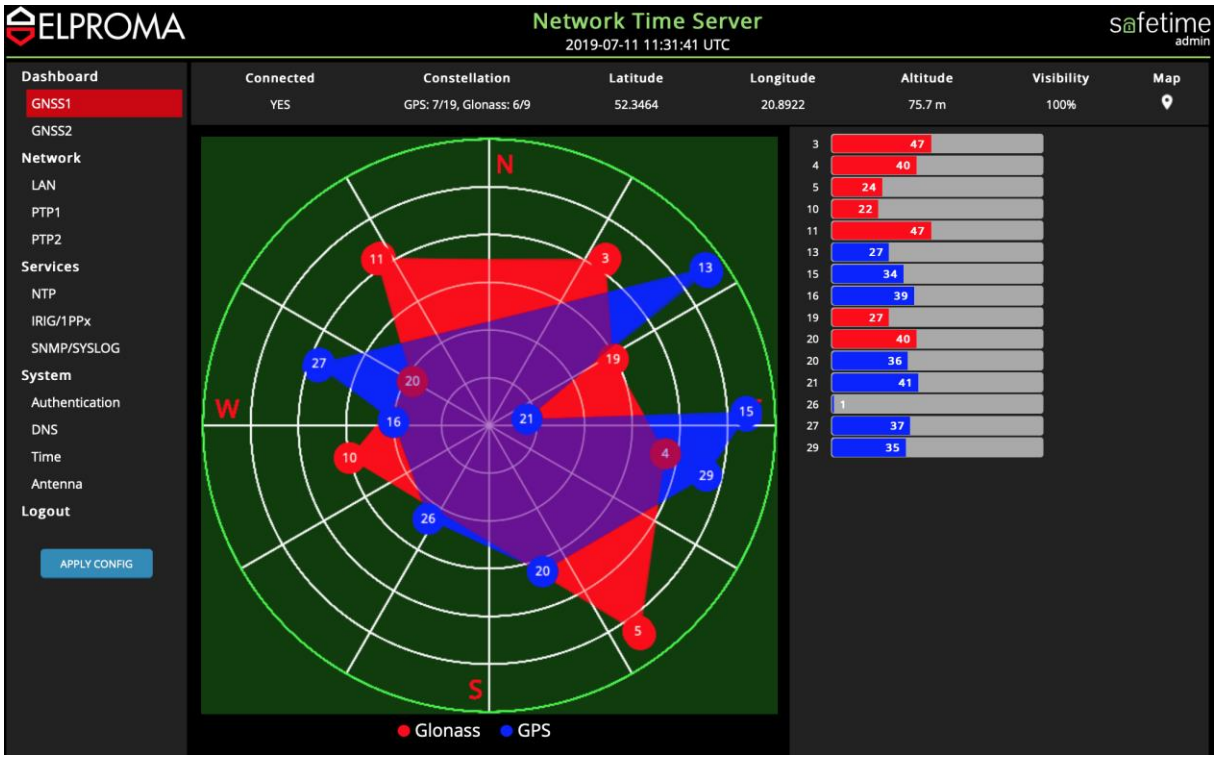
Save the settings using disk icon (1) and save it permanently by “Apply config” button (2). To quit the setup please use blue “Logout” button.



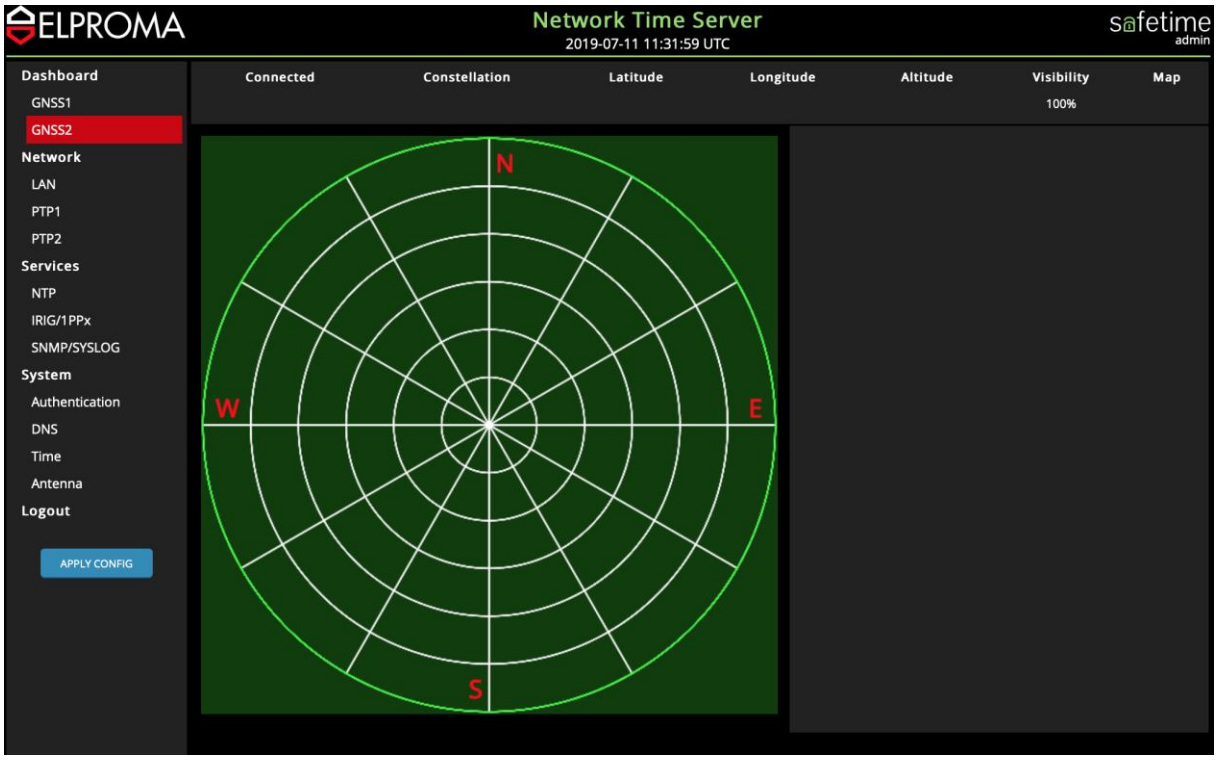
33. Software WWW – Setting GNSS & Antenna

. Single NTS-antenna System

The following screen is available if one antenna is connected (e.g. ANT-1):

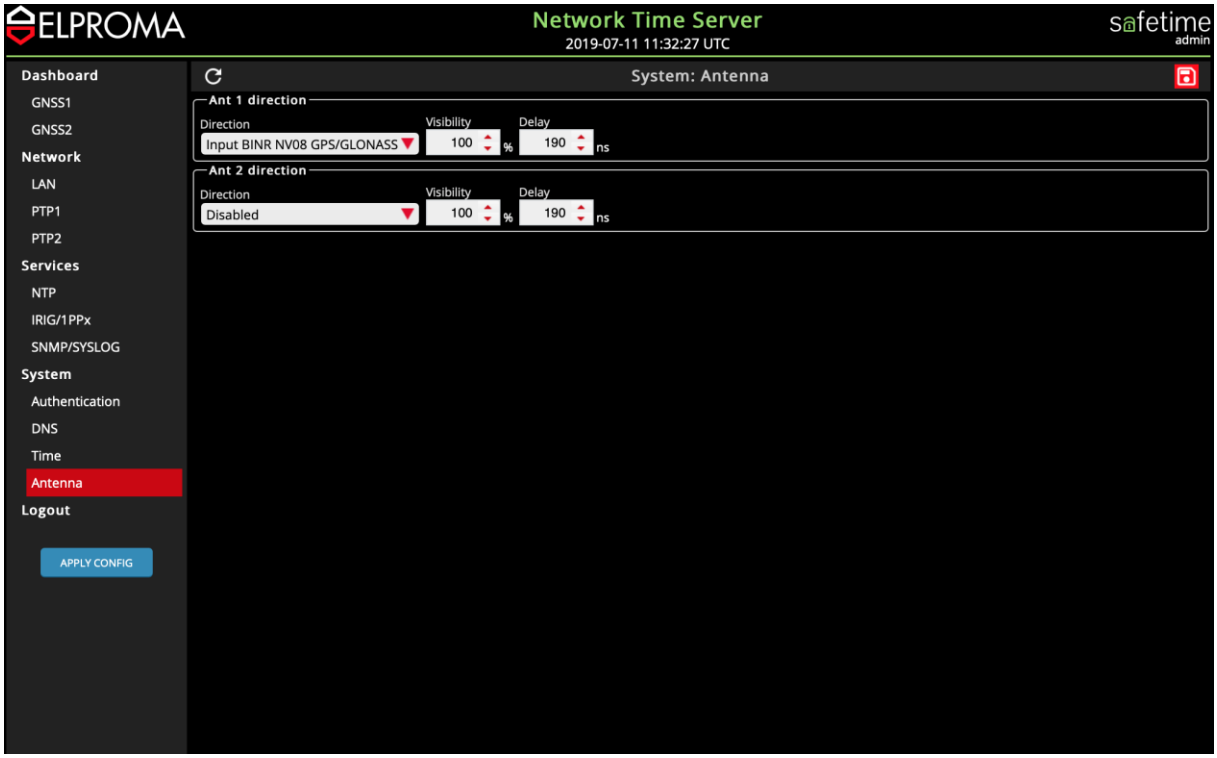


If antenna is not connected (e.g. ANT-2) the following screen appears after selecting GNSS2:

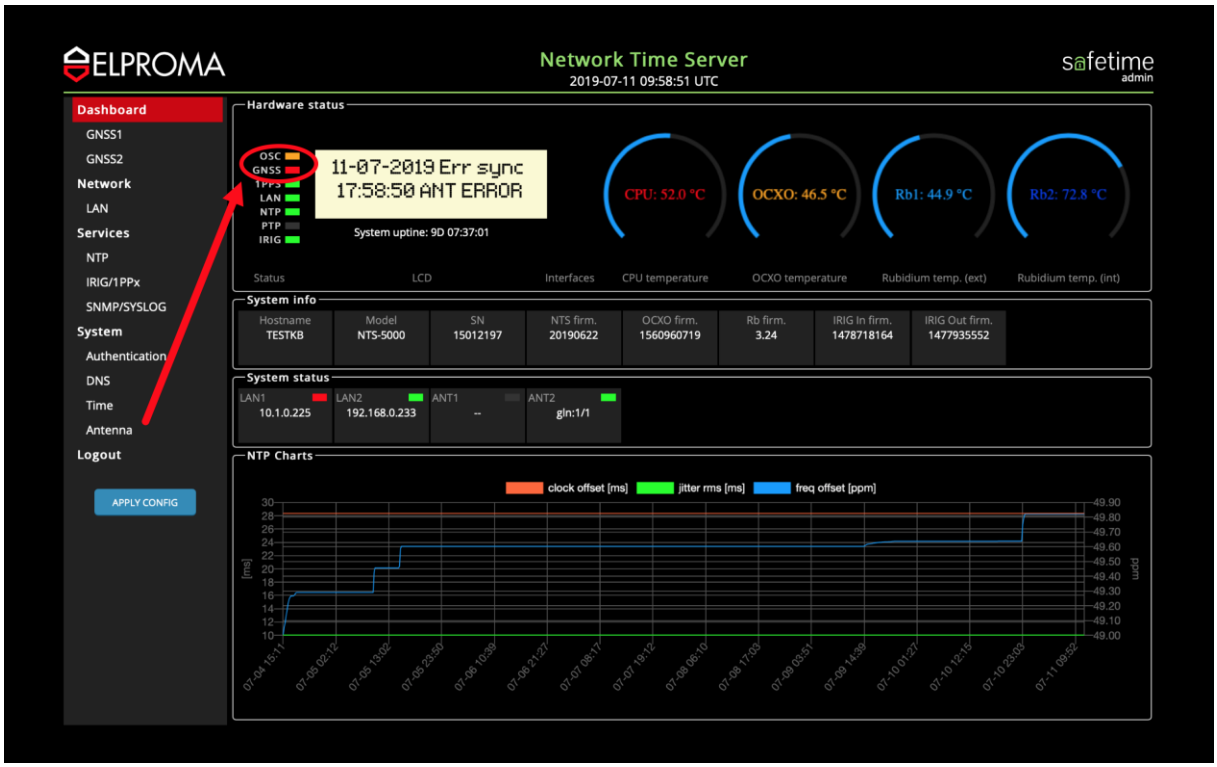


IMPORTANT NOTE!

In case of using single antenna (ANT-1 or ANT-2), disable not used interface:

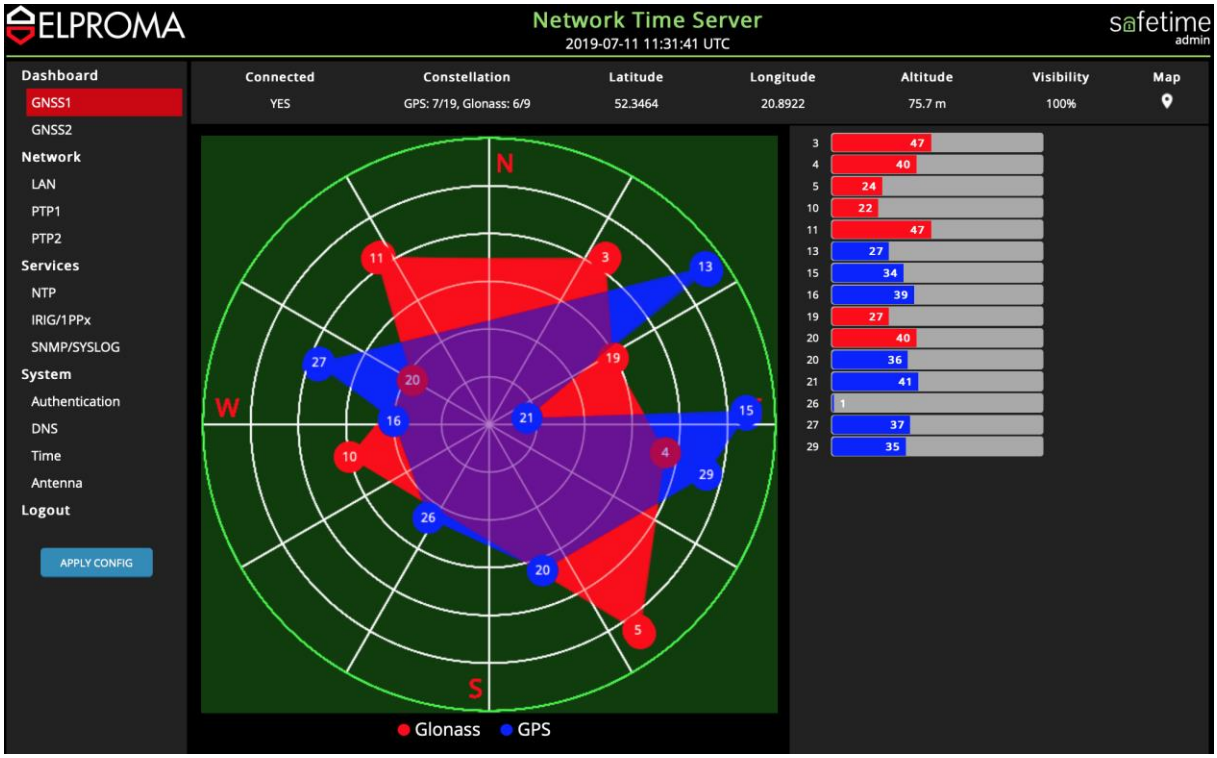


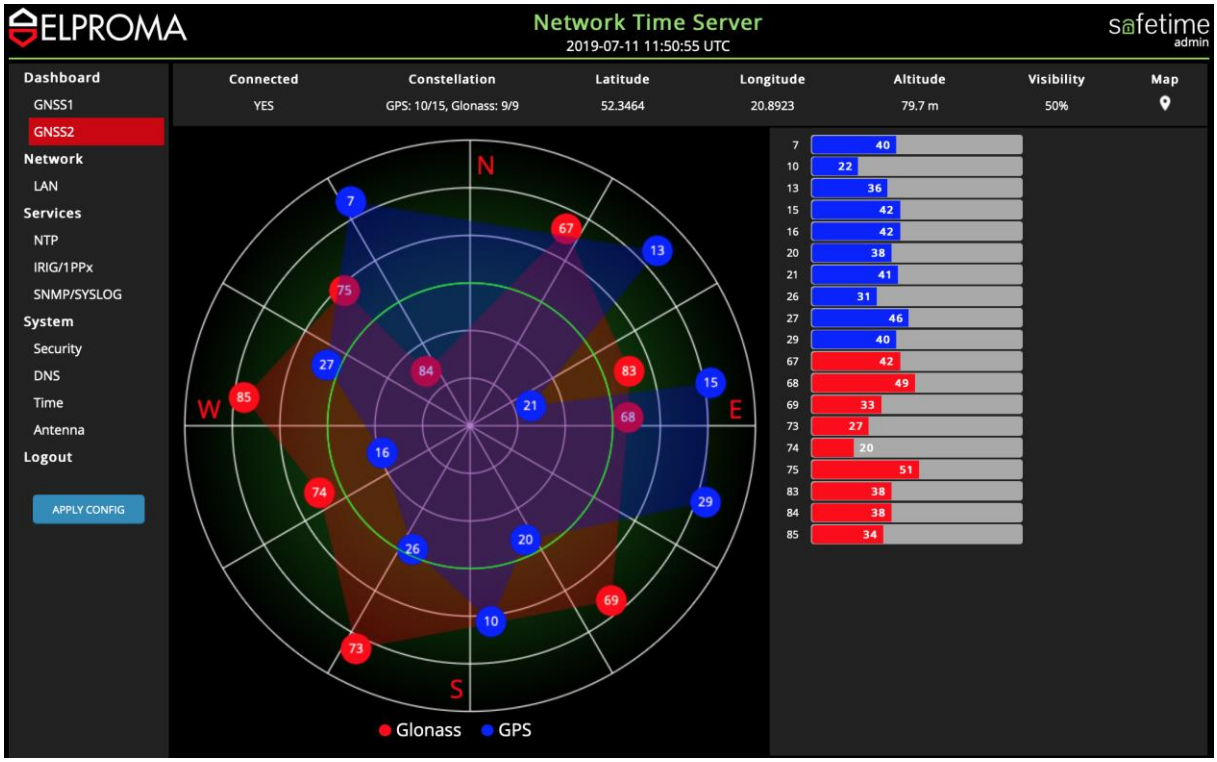
Keeping both antennas enable, when only ANT-1 (or ANT-2) is present, will trigger the front panel GNSS LED fleshing RED. This indicates a phantom problem with 2nd (not existing) antenna. Please take care to disable not used antenna I/O when only single antenna system is deployed.



. Redundant NTS-antenna System (2x antenna)

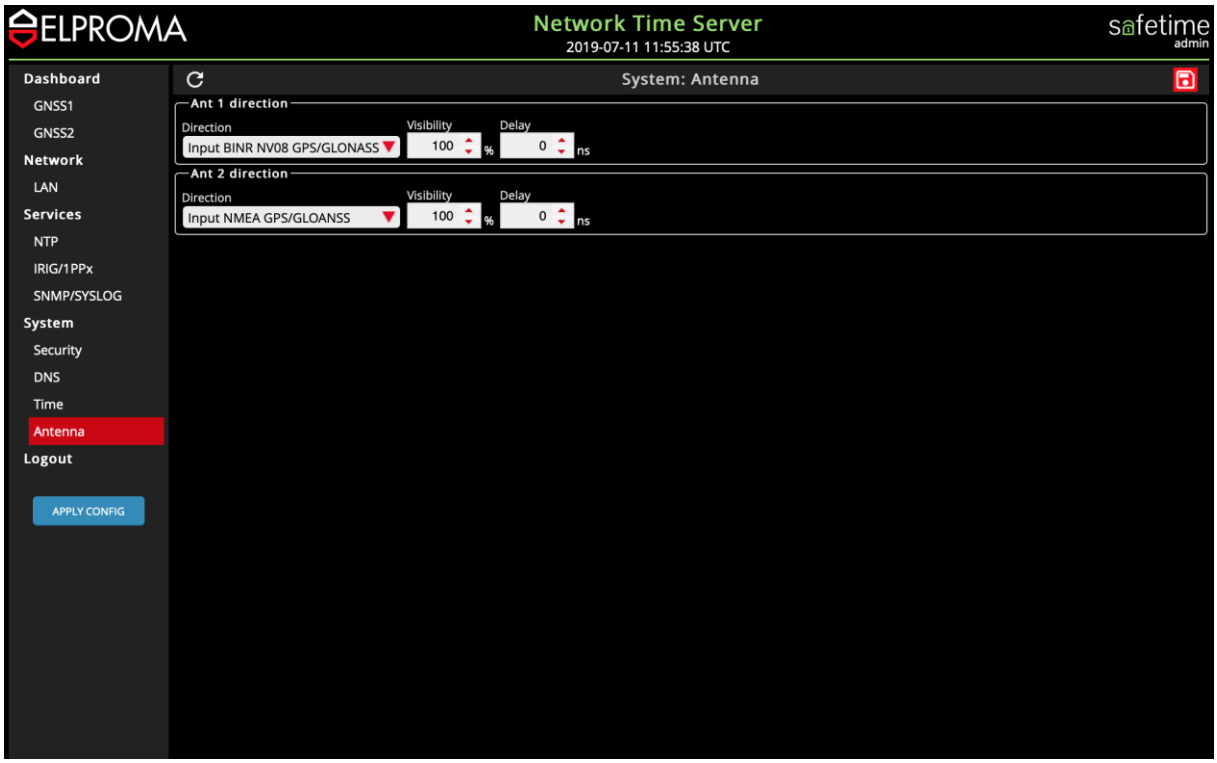
The following looks like screens appear when double antenna system (ANT-1, ANT-2) is in use:

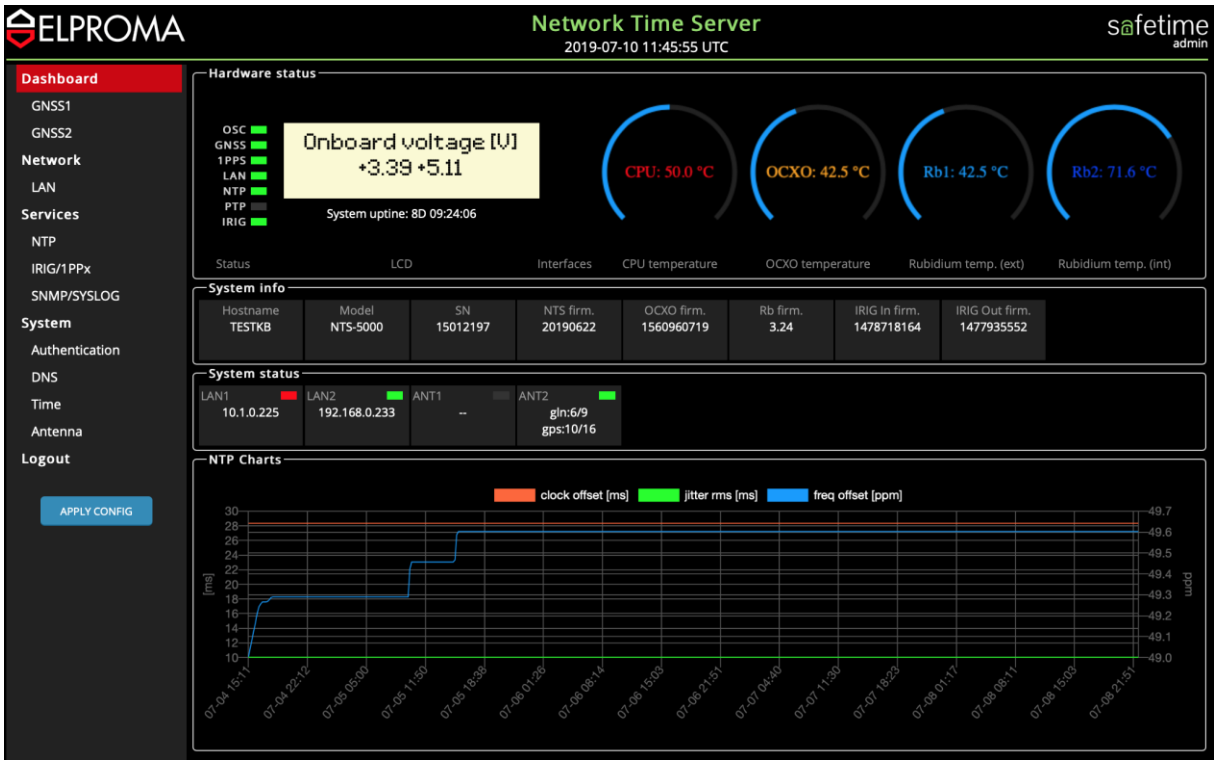




IMPORTANT NOTE!

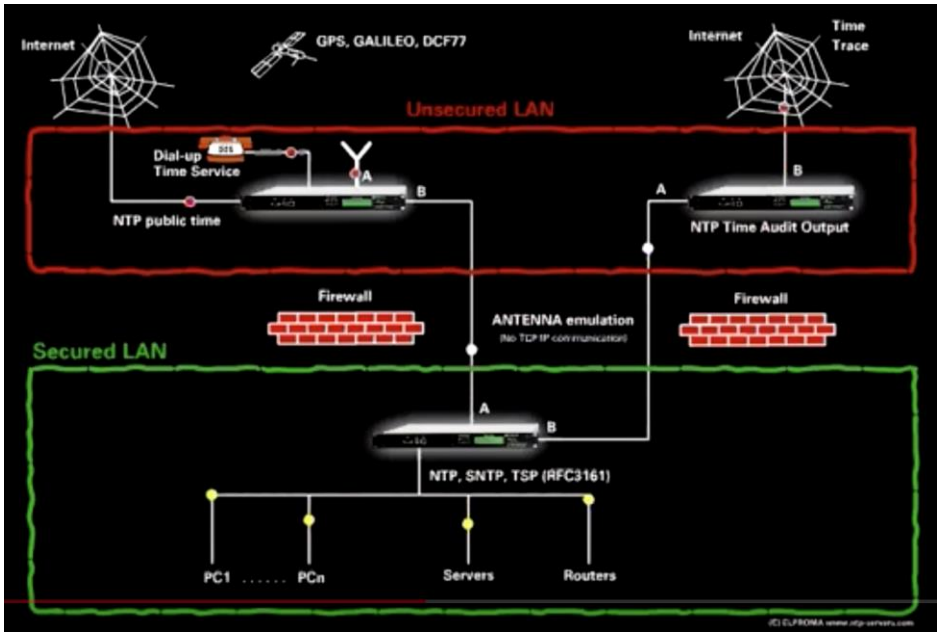
In case of using 2 antennas, please set each of them to different operation mode:
E.g. ANT-1 in BINR, and ANT-2 in NMEA mode. Never use the same MODE for both antennas.

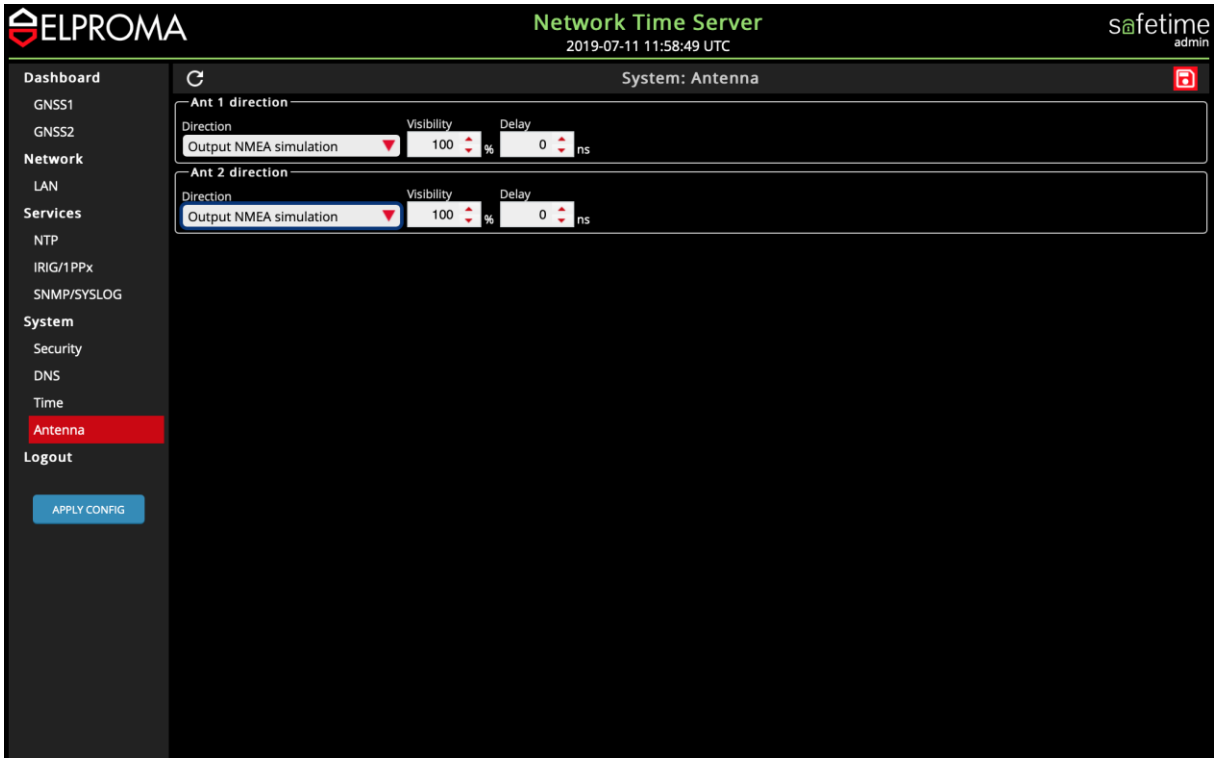

ELPROMA
Network Time Server
2019-07-11 11:55:38 UTC
safetime
admin
Dashboard
GNSS1
GNSS2
Network
LAN
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Security
DNS
Time
Antenna
Logout
APPLY CONFIG
System: Antenna
Ant 1 direction
Direction
Input BINR NV08 GPS/GLONASS
Visibility
100
%
Delay
0
ns
Ant 2 direction
Direction
Input NMEA GPS/GLOANSS
Visibility
100
%
Delay
0
ns


ELPROMA
Network Time Server
2019-07-10 11:45:55 UTC
safetime
admin
Dashboard
GNSS1
GNSS2
Network
LAN
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Authentication
DNS
Time
Antenna
Logout
APPLY CONFIG
Hardware status
OSC
GNSS
1PPS
LAN
NTP
PTP
IRIG
Onboard voltage [V]
+3.39 +5.11
System uptime: 8D 09:24:06
CPU: 50.0 °C
OCXO: 42.5 °C
Rb1: 42.5 °C
Rb2: 71.6 °C
Status
LCD
Interfaces
CPU temperature
OCXO temperature
Rubidium temp. (ext)
Rubidium temp. (int)
System info
Hostname
TESTKB
Model
NTS-5000
SN
15012197
NTS firm.
20190622
OCXO firm.
1560960719
Rb firm.
3.24
IRIG In firm.
1478718164
IRIG Out firm.
1477935552
System status
LAN1
10.1.0.225
LAN2
192.168.0.233
ANT1
--
ANT2
gln:6/9
gps:10/16
NTP Charts
clock offset [ms]
jitter rms [ms]
freq offset [ppm]
[ms]
ppm

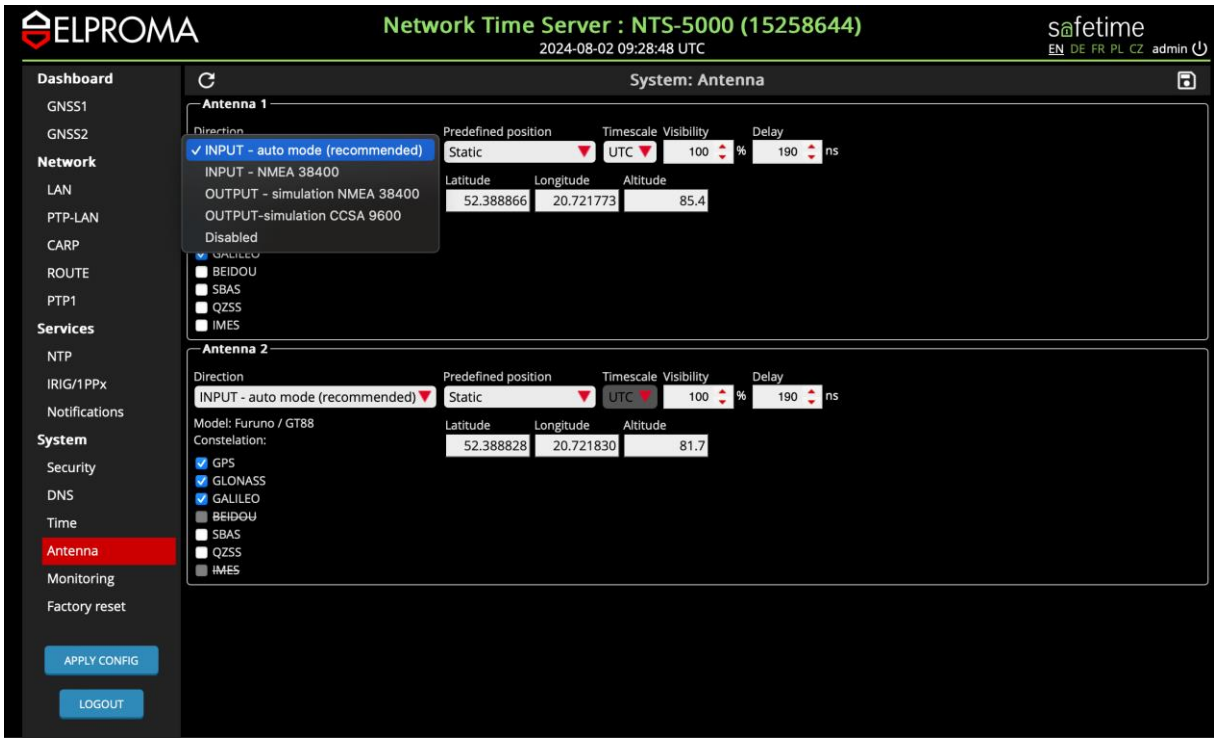
. Antenna Modes: In, Out (Emulating NMEA 183)

Each antenna (ANT-1, ANT-2) can operate in INPUT or OUTPUT mode. The output mode emulates antenna in std. GPS NMEA 183 mode, providing ref. time (PPS & ToD) from NTS-x000 to another device. This is very useful when considering over firewall connection between 2 or more timeservers. In fact this can be one of way to use a public NTP-server to provide alternative backup ref. of time into internal time servers operating inside secured network. This technique can be also be used for remote auditing purpose of internal operating network appliance NTS-x000.



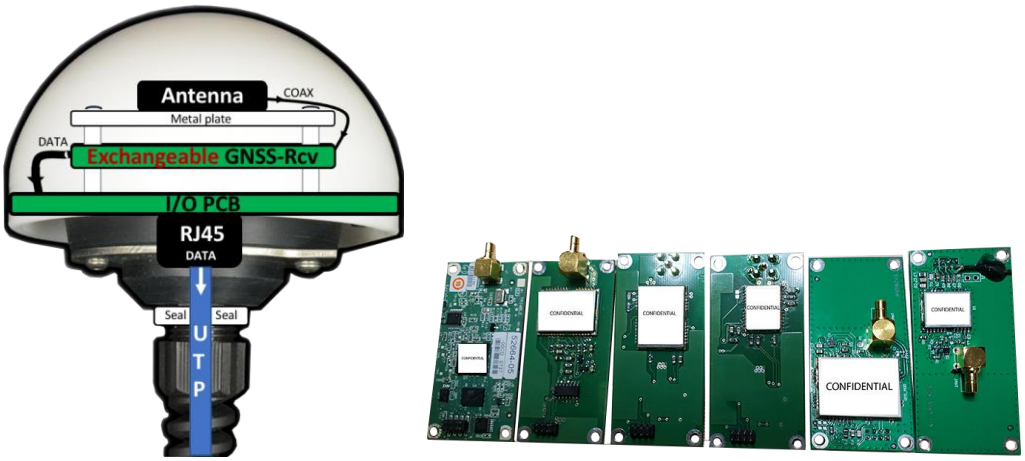


In above example, the ANT-1 interface will be set to OUTPUT (NMEA183) mode, and the ANT-2 stays operating in INPUT mode (requiring NTS-antenna to by physically connected). Please apply config changes and safe your configuration for effective use of new configuration.
Also, considering the INPUT settings, you can choose a different GNSS constellations subset.



System automatically recognizes the build in GNSS receiver. Depends on type of receiver chip your server is equipped, a new system like GALILEO, IRSS, IRIDIUM can be use too. Some of satellite sub-systems or functionalities are requiring additional licenses to pay separately.

Elproma optionally offers a various of different GNSS receivers supporting GPS, GLONASS, BEIDOU, GALILEO* o any combination of above systems. We also offer on request a multicarrier receiver supporting frequencies L1/L2/L5:

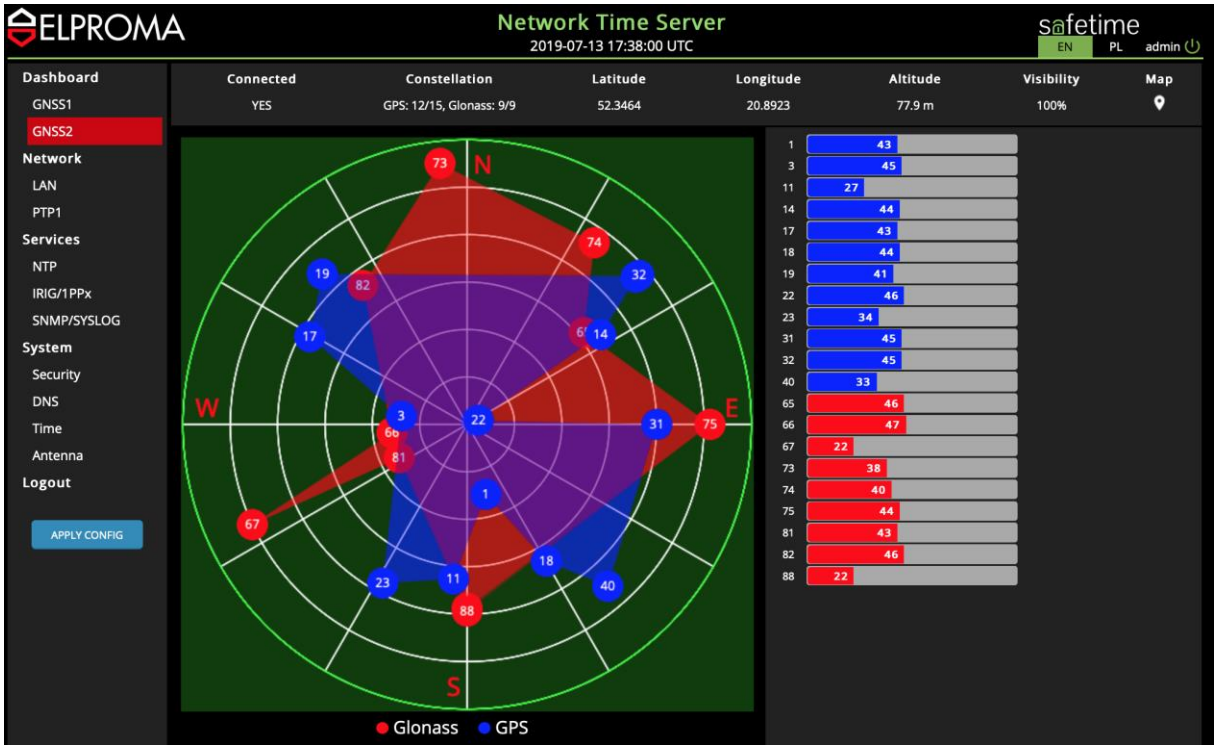


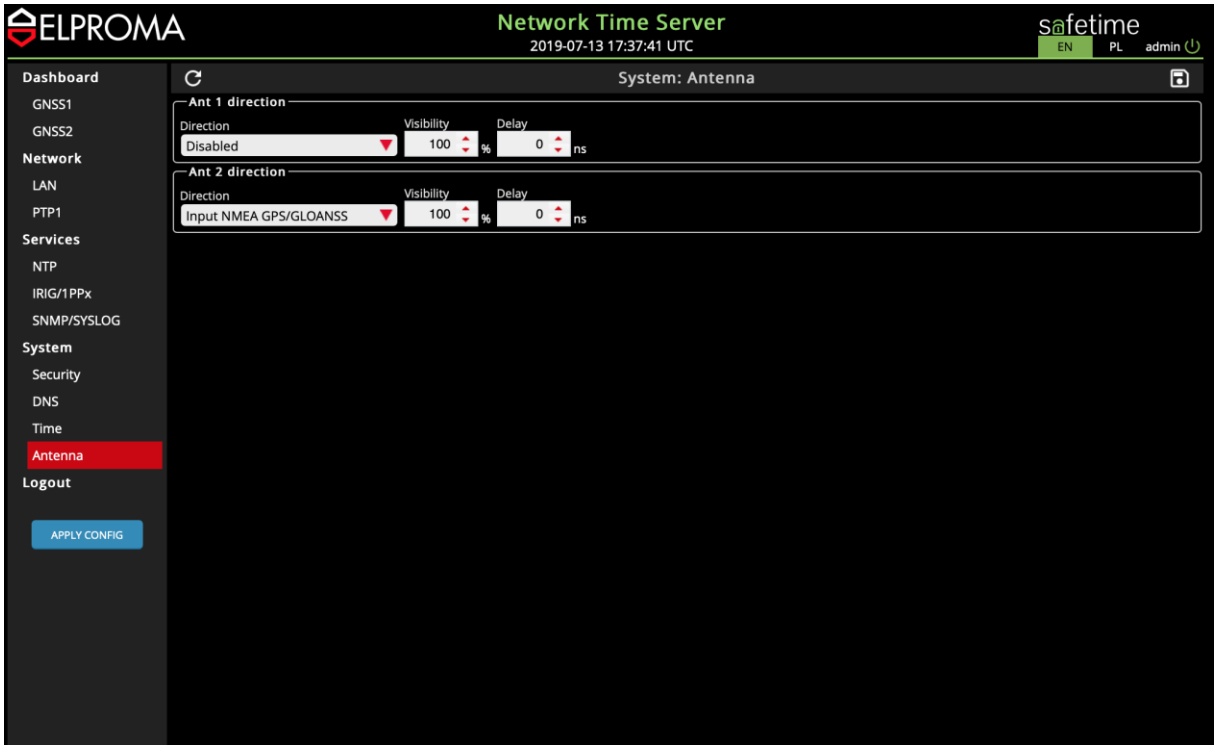
Exchangeable GNSS modules for NTS-antenna

Each module basis on different GNSS receiver from different ELPROMA qualified supplier vendor. This functionality is very useful when requirement for new satellite system evolves in time. In such case there are not needs to replace all time-server to new one. The replacing technique is crucial to ensure cyber-security and “plan B” for unexpected problem like many vendors experience.

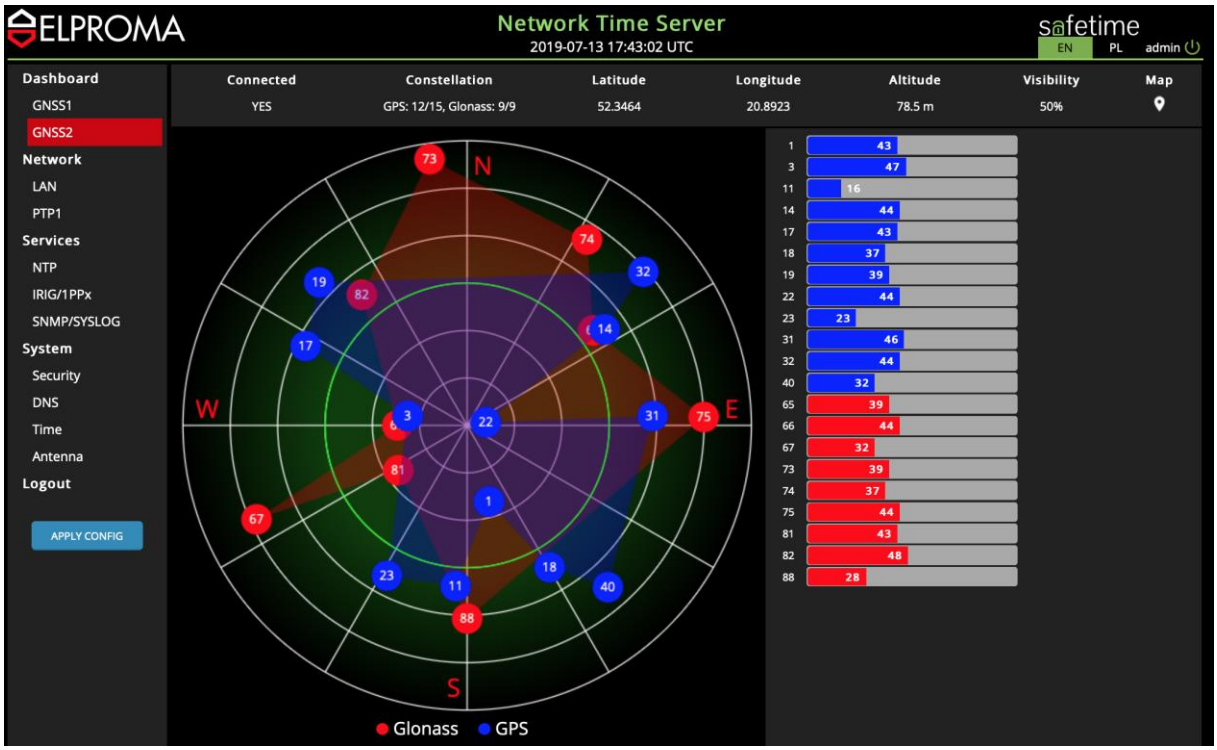
. Presenting visibility of GNSS satellites

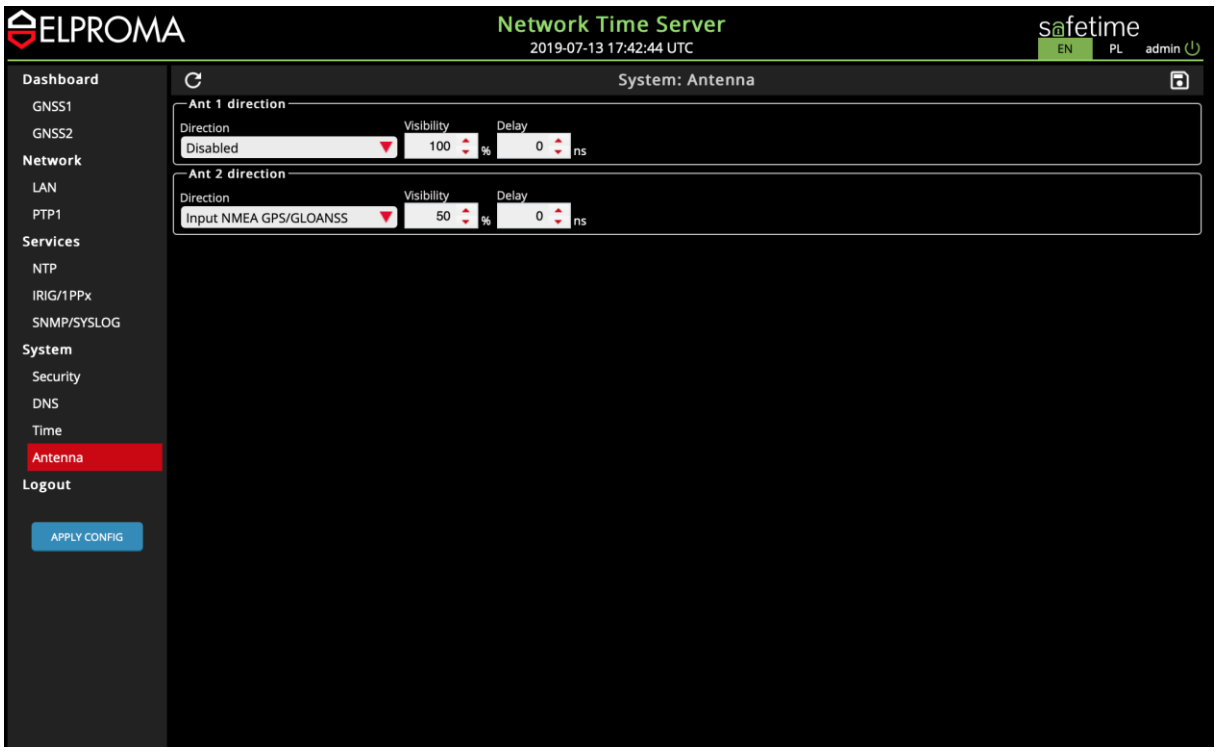
Sometimes, it is just simply not possible to locate your antenna perfectly to let it view all 360 degree of the sky. In such case, you might like to indicate this fact by setting your own visibility filter on radar. The 100% visibility looks following:



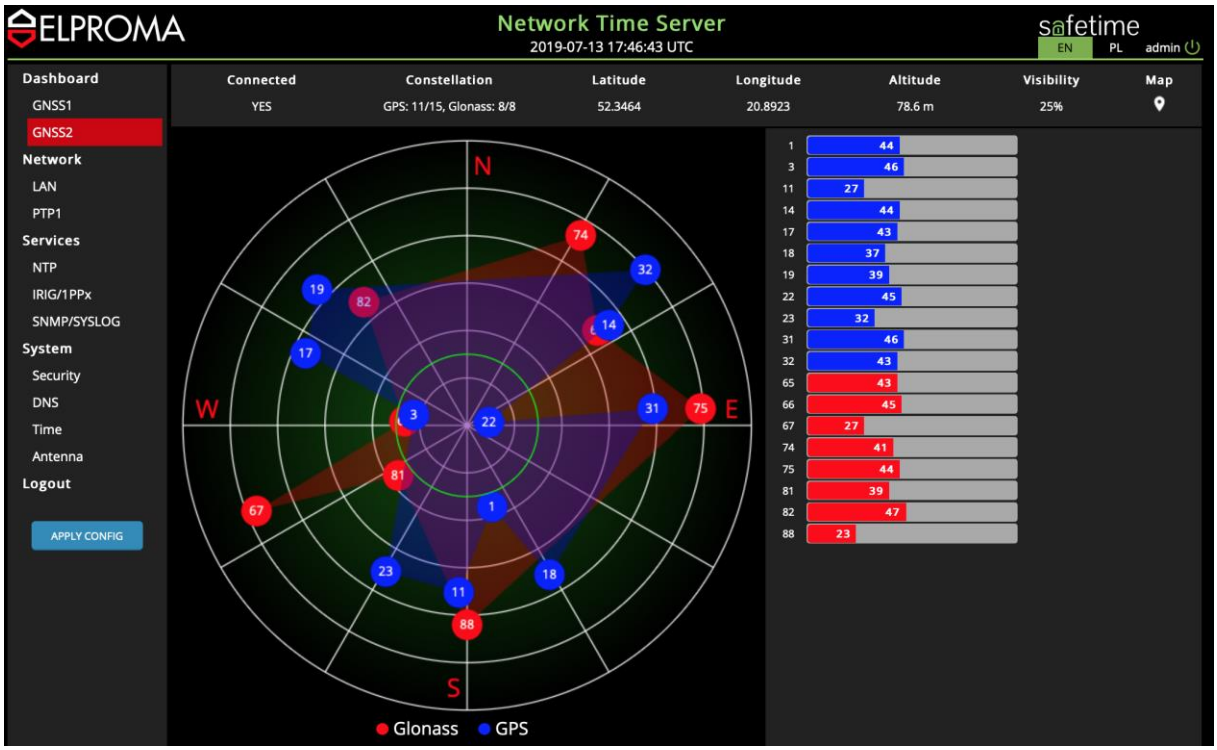


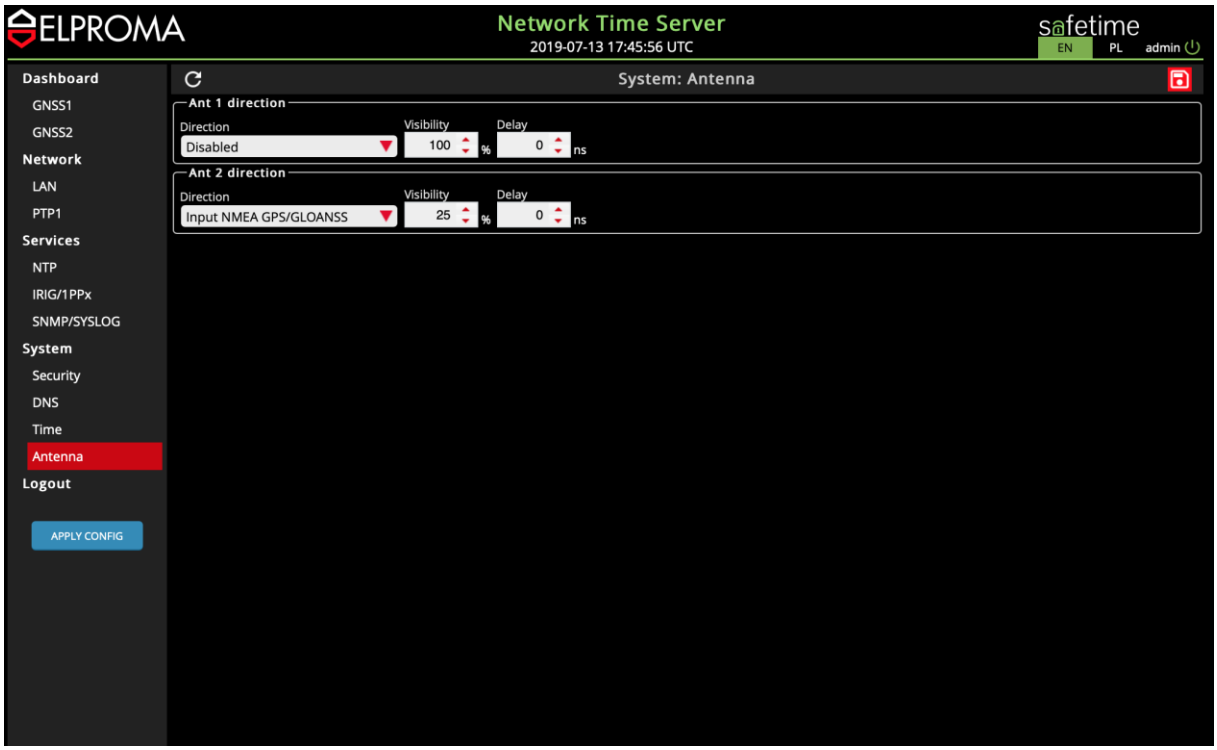
The 50% visibility gives following effect when green colour field indicator moves to centre:





The 25% visibility gives following effect when green colour field indicator moves to centre:

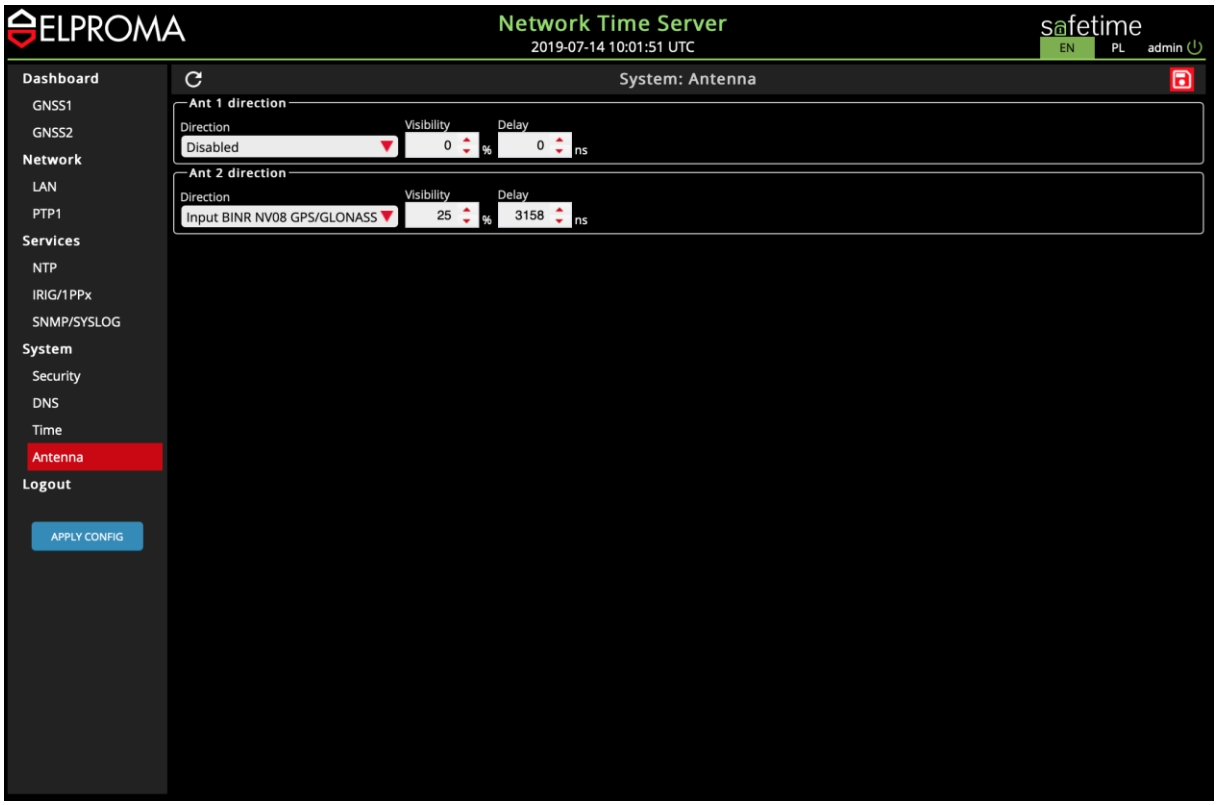




. Compensating cable length delay

IMPROTANT NOTE! The cable compensation works only for BIN antenna mode. The NMEA mode currently does not support cable delay compensation.

The NTS-antenna includes built-in GNSS receiver. It computes position and time based on the position. However, the signal must travel through a potentially long UTP (STP) cable before it reaches the NTS-x000 time server. The typical delay for most UTP (STP) cables is 1.5417 ns per foot. For a 30 ft cable, the delay would be 1.5417×30 = 46.25 ns. If uncorrected, the NTS-x000 estimates of UTC would be 46.25 ns later than a properly calibrated unit. For the SI metric system please assume a cable delay is 4.5 ns each cable meter. Therefore, for a max. cable length of 700m the compensation delay should be set to 3.15 [us] (microsecond). The final delay compensation you can store at server WWW setup:



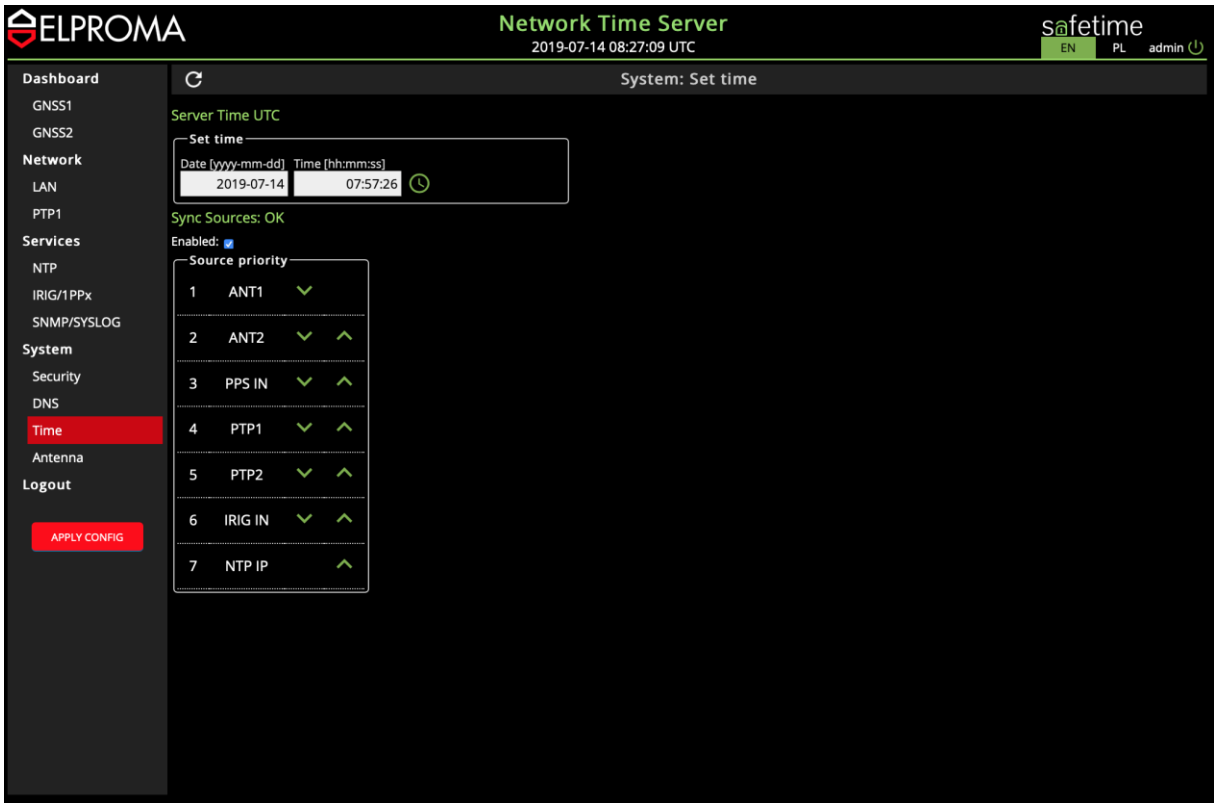
Above example present delay compensation 450ns for 100-meter UTP cat. 5 cable used between NTS-antenna and time server NTS-x000.

NOTE! You will need to save your configuration and apply changes in setting first.

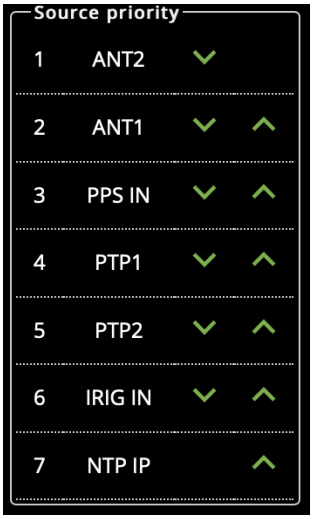
. Setting Synchronization priority time resources

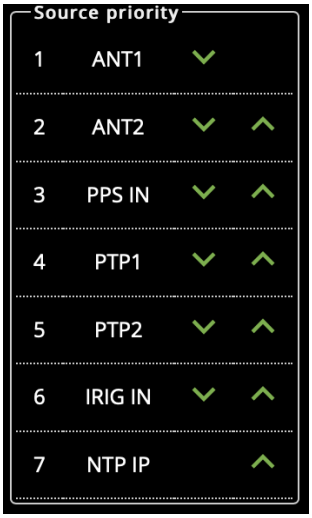
All Elproma servers support simultaneously both ANT-1 and ANT-2. In fact, it receives simultaneously data from all /O inputs providing ref. sources of UTC time. Switching between the ref. sources does not impact the server time output (note! This is a valid assuming all references are operating same time scale as UTC). However, only one reference is taken in time following user-definable PRIORITY TABLE and all other sources stays ready backup.

You can choose using TIME menu item, whatever ANT-1 or ANT-2 will keep priority in synchronization:



You can swap between antennas priority ANT-1/ANT-2 by clicking green upper/down arrow of each item:



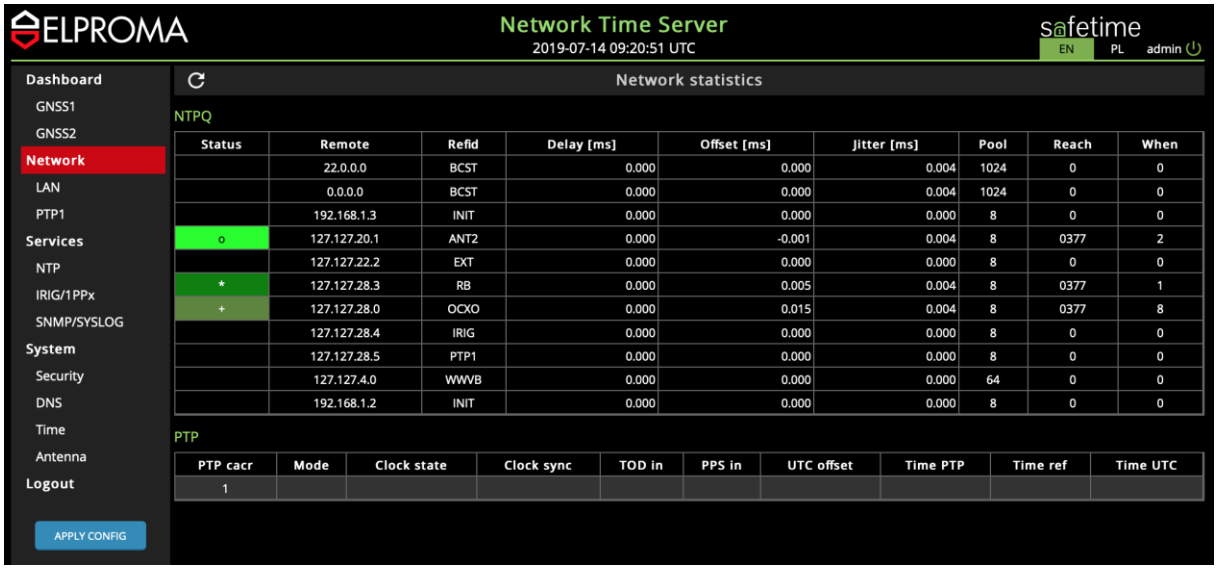


. Monitoring synchronization status of antenna

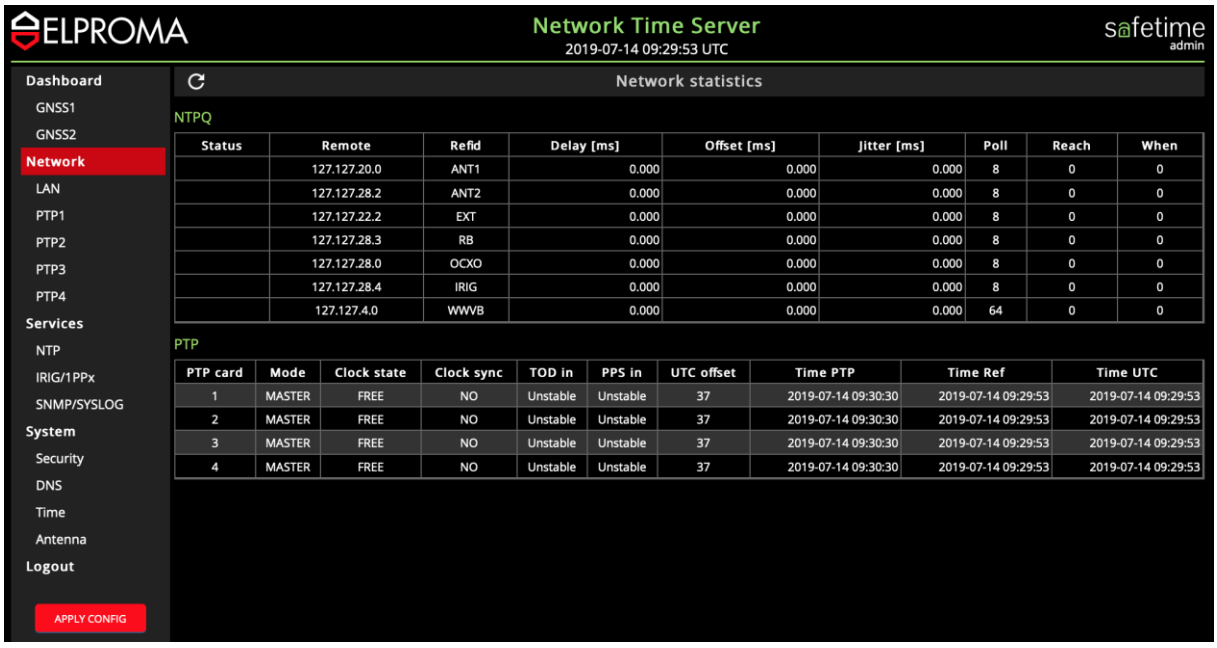
(please ref. to below chapter)

34. Software WWW – Setting Network

To configure network interface please connect your time server to PC using LAN1-LAN2. The NETWORK menu presents all sync. resources with its current priority and status. The 1st column marks “o”, “*” indicates current source of time. Other candidates are market “+” or “-“. Table presents also other data useful to examine performance and status of syncing.

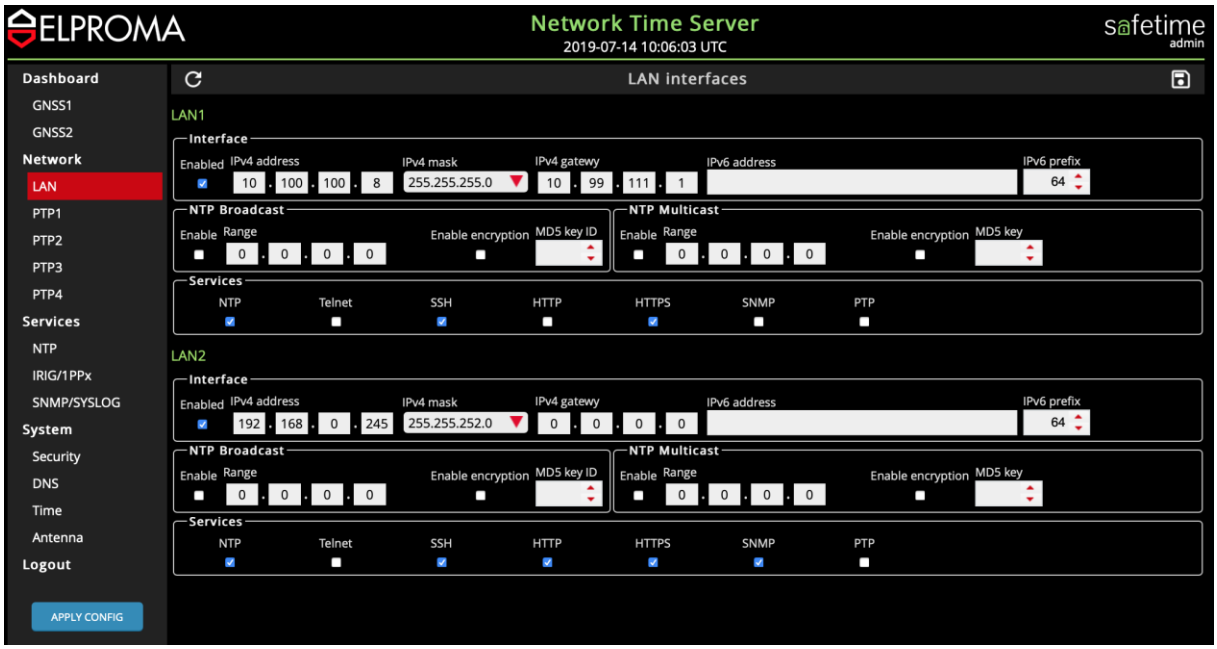


If your server is equipped with Expander 1-4 PTP IEEE1588 cards, the bottom part of screen includes a list expander cards and its data:



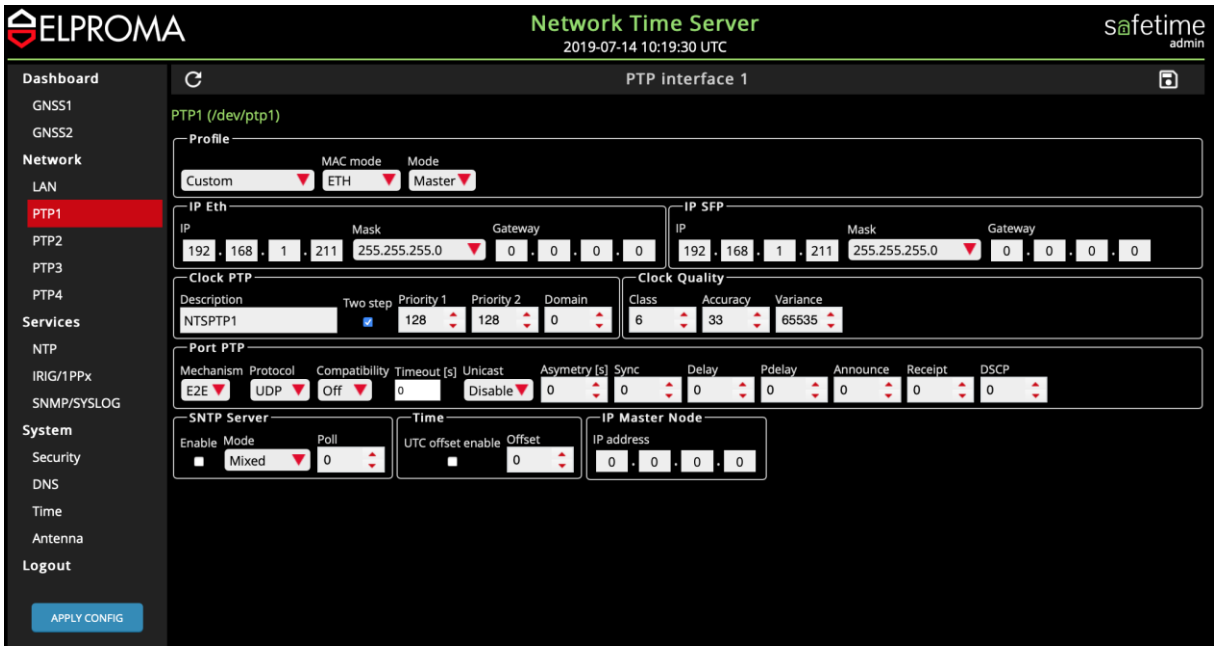
. LAN1-LAN2 (std.) – Platform 0

IMPORTANT NOTE!
Configuring Time Server is requiring exclusive access by single interface at time.
Only single LAN in time can include GATEWAY (LAN1 or LAN2).
LAN1-LAN2 interfaces are 10/100Mbps and they support software stamping NTP and PTP.



. LAN3-LAN10 (optional Expander 1-4 for NTS-5000/TC) Platform 0

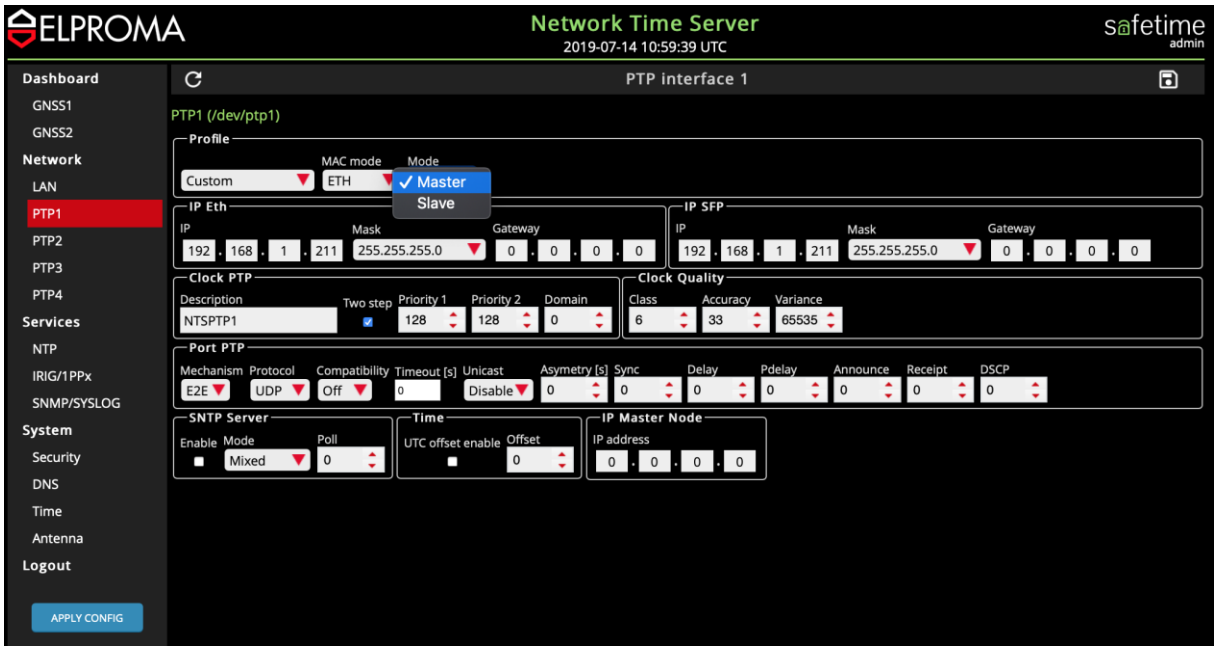
IMPORTANT NOTE!
Configuring LAN3-LAN10 is only possible via LAN1 or LAN2 interface at time.
Each LAN can include own GATEWAY (LAN3- LAN10).
LAN3-LAN10 interfaces are 1GE and they support hardware stamping PTP IEEE1588



. PTP IEEE1588 configuration

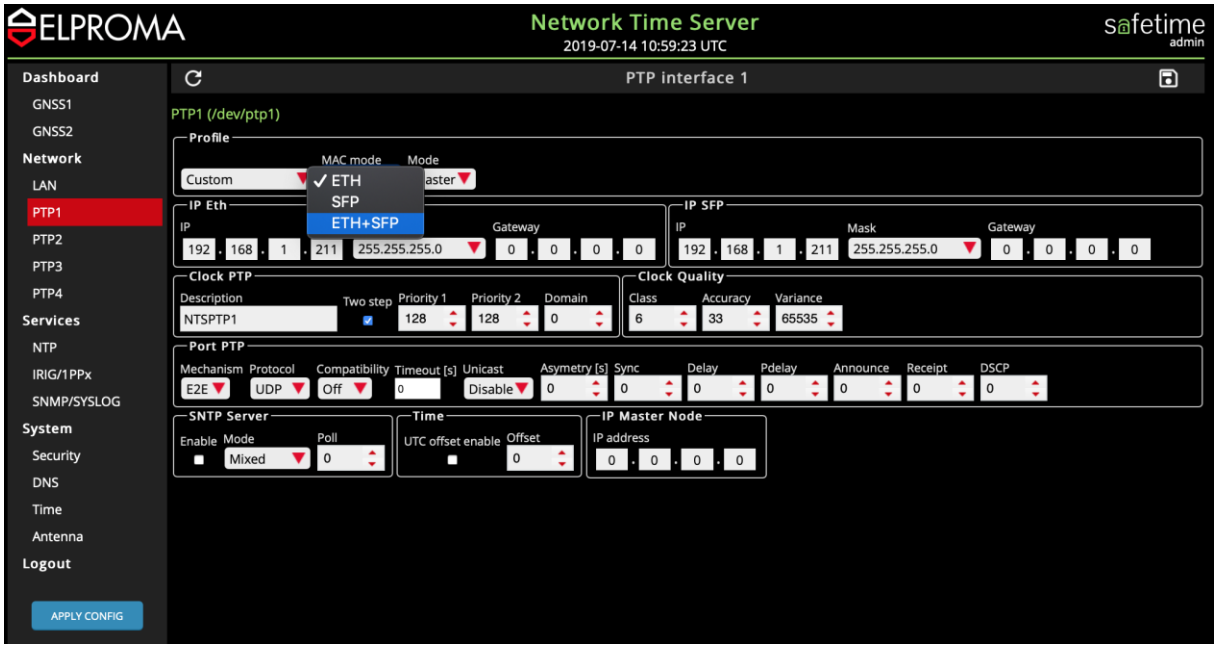
NTS-5000 and NTS-TC can be equipped with additional network interfaces, supporting hardware stamping PTP IEEE1588. There are max. 4x NIC (Expander 1-4 cards), each includes 2x LAN (1GE) supported by Rj45 and SFP interface. Expander cards 1-4 are available only for Platform 0. In Platform 2 they have been replaced by LAN2, LAN3 and LAN4, LAN5 as an option

For Platform 0 Expander 1-2 can operate both: grandmaster & slave PTP IEEE1588. Expander 3-4 are only able to operate as grandmaster. All cards are automatically recognized by NTS-5000/NTS-TC system and added to main menu. Master/Slave is set for all expander, so if you choose to operate Expander1 card slave, both LAN3 and LAN4 will operate slave too. To choose MASTER or SLAVE mode (LAN3-LAN6) select from profile menu:

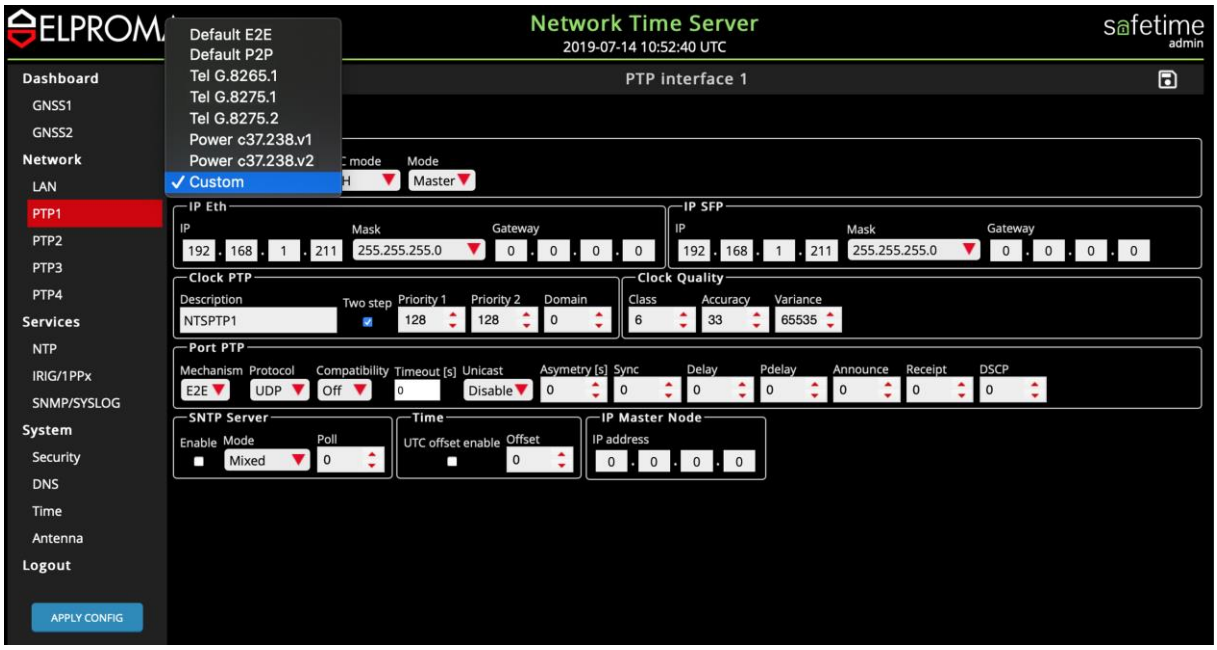


For Platform 2 each LAN 2-5 can operate as MASTER or SLAVE (SLAVE is depending on the firmware version)

Choose specific interface ETH or SFP you want to configure for each Expander 1-4 car: PTP1.. PTP4. (platform 0)



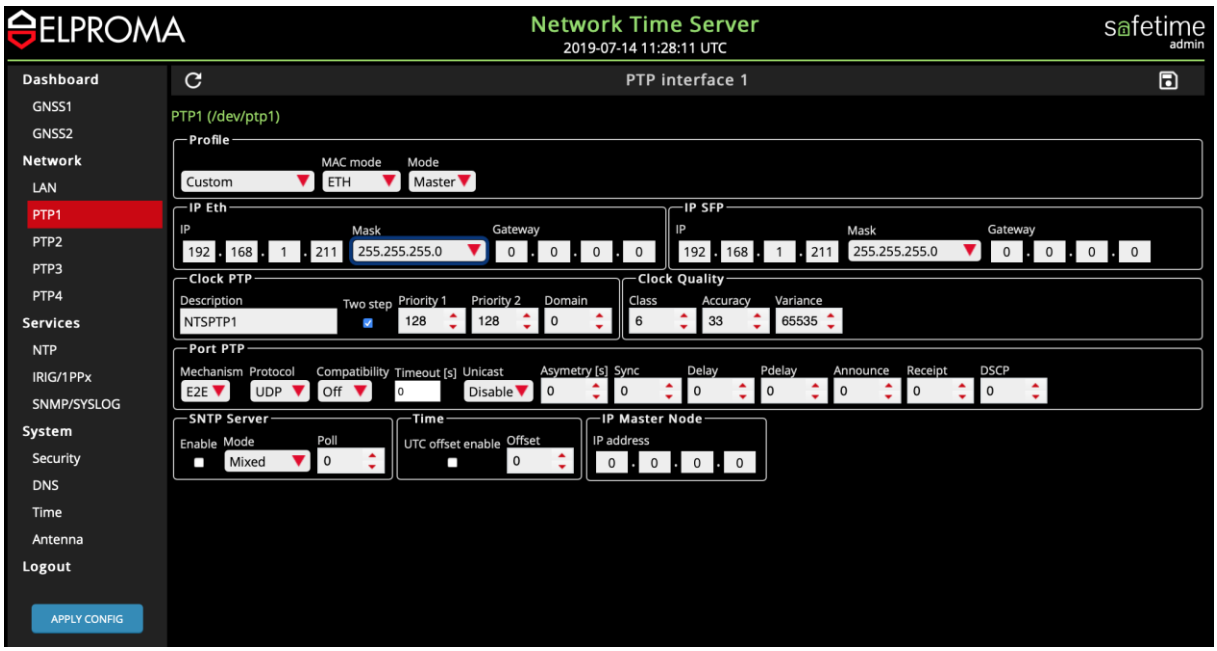
Choose predefined PTP IEEE1588: 2008 profiles from menu or define our own custom one:



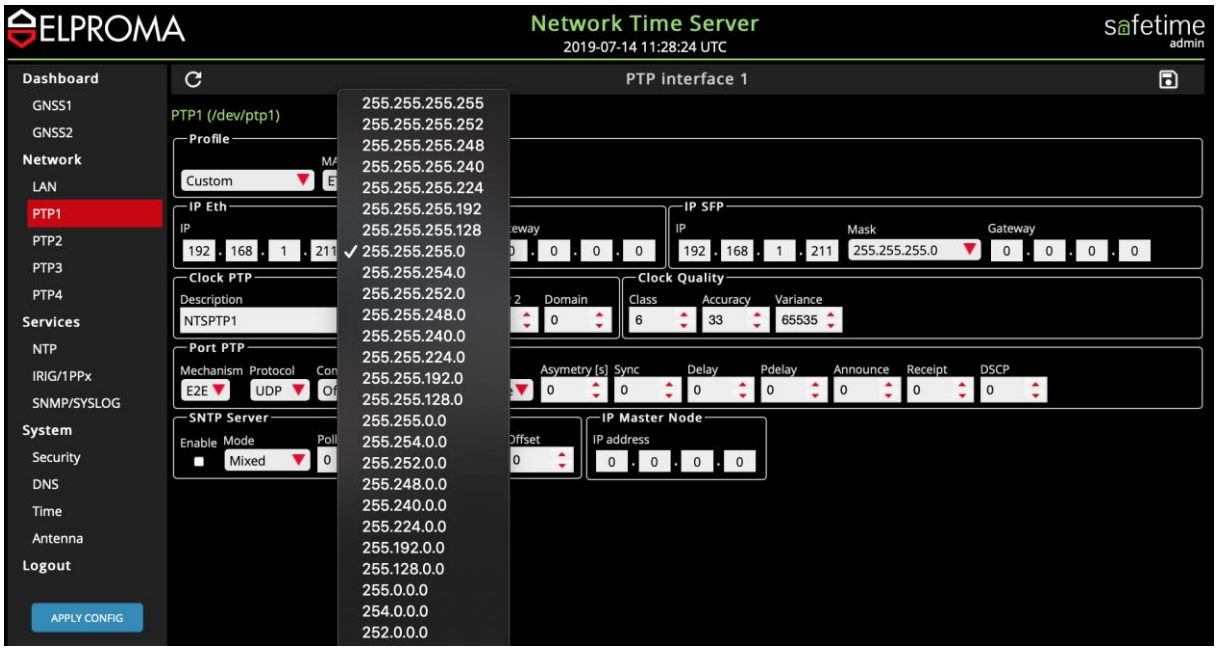
Currently supported PTP IEEE1588 profiles are:

Default E2E, Default P2P, Telecom (ITU-I G8265.1, ITU-I G8275.1, ITU-I G8275.2), Power (IEEE C37.238 v1, v2 – covering compliance of IEC 61850-9-3 Power Utility Profile) and Custom (you do configure manually each parameter)

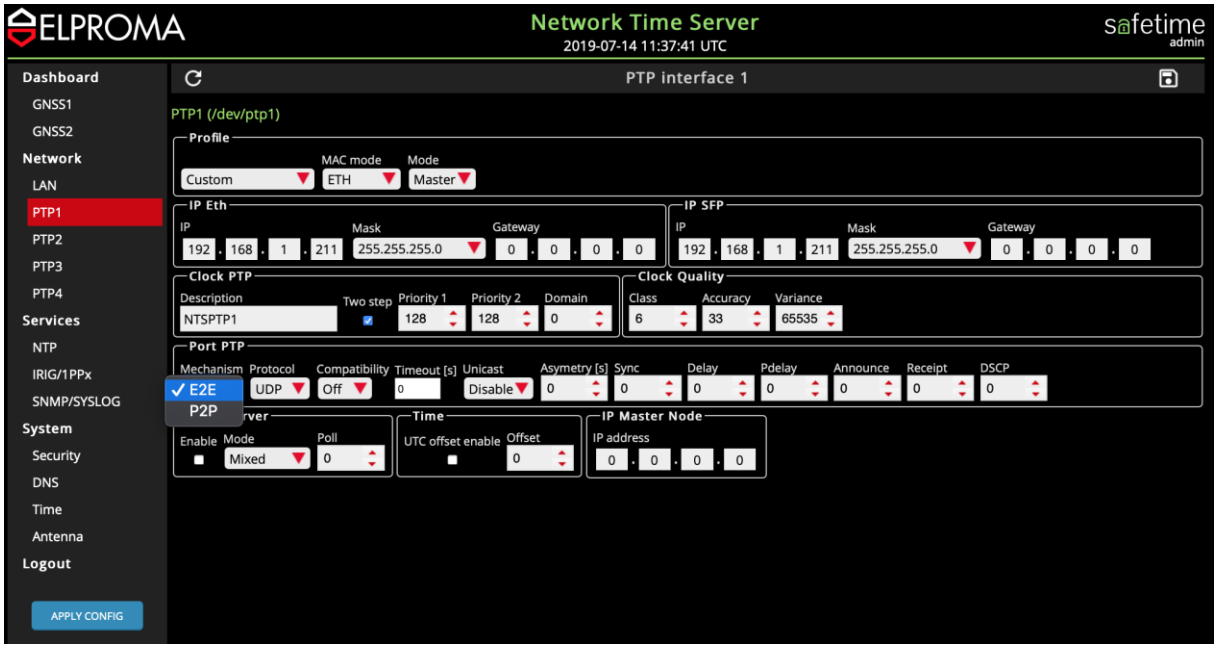
Now you can set specific IPv4/IPv6 address to each PTP interface (ETH or SFP) separately:

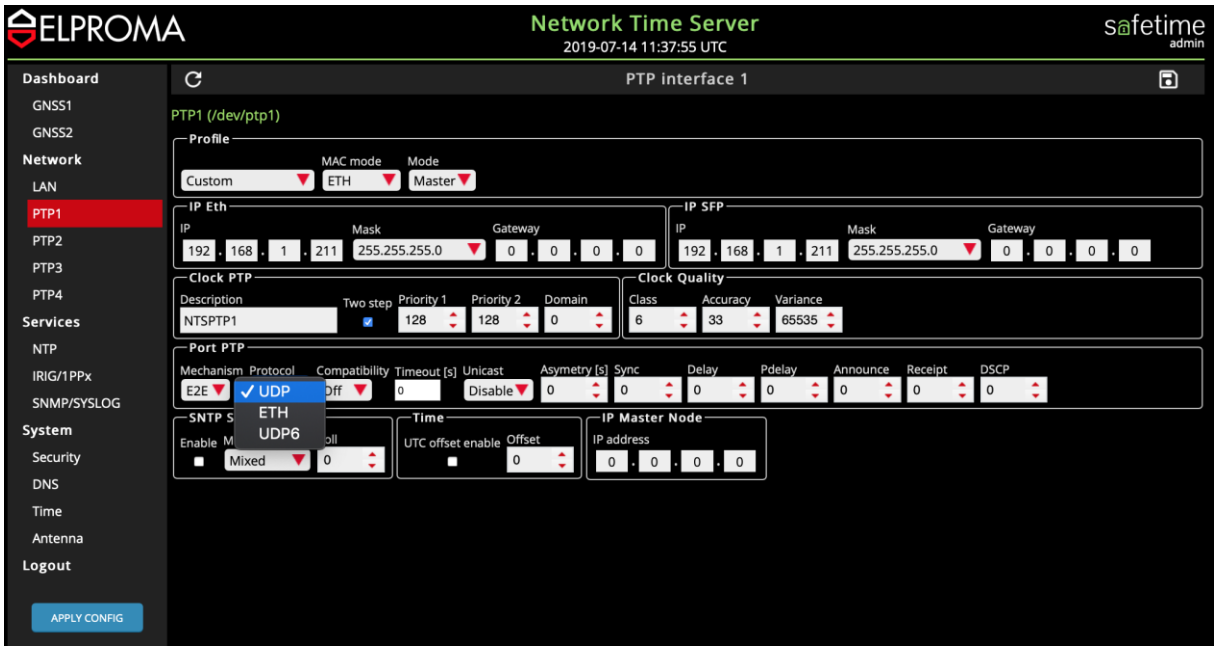


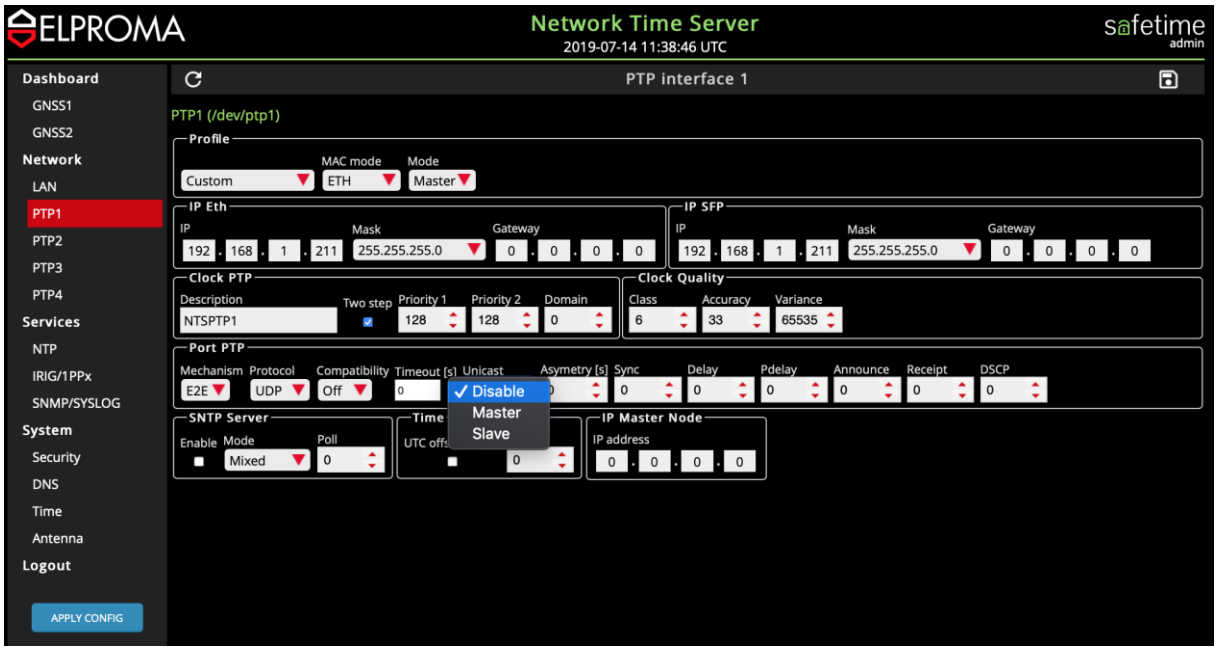
Some predefined values will help prevent against errors (e.g. subnet MASK):

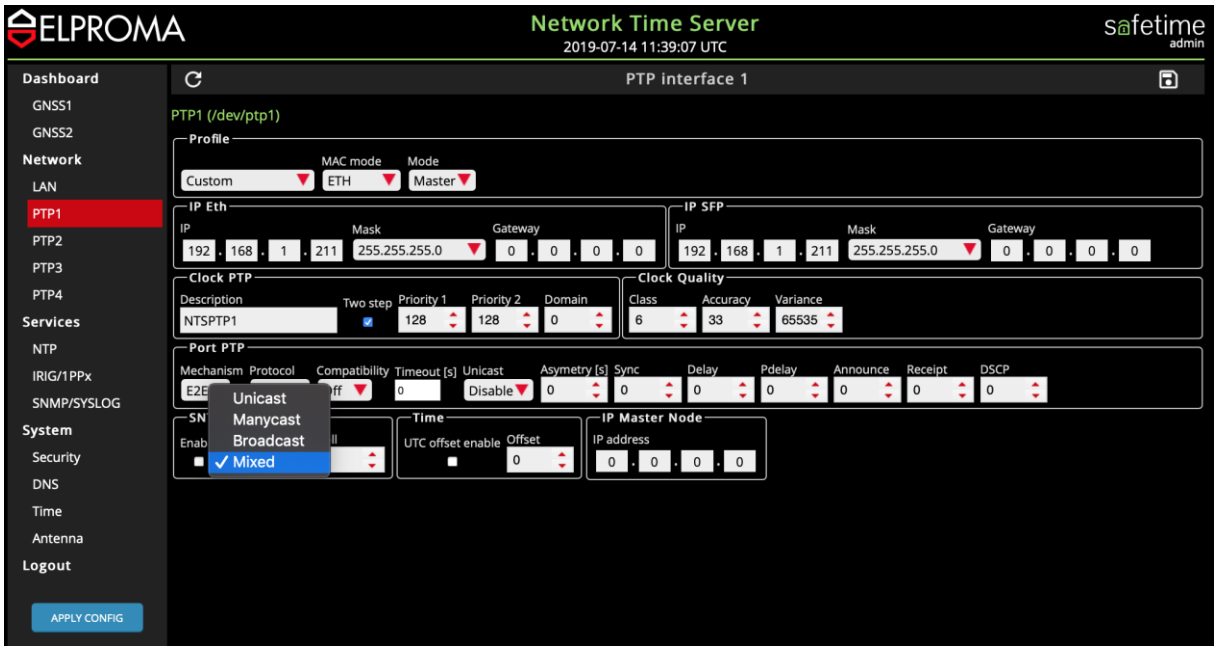


The other PTP data can be set:




ELPROMA
Network Time Server
2019-07-14 11:37:55 UTC
safetime
admin
Dashboard
GNSS1
GNSS2
Network
LAN
PTP1
PTP2
PTP3
PTP4
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Security
DNS
Time
Antenna
Logout
APPLY CONFIG
PTP interface 1
PTP1 (/dev/ptp1)
Profile
Custom
MAC mode
ETH
Mode
Master
IP Eth
IP
192 . 168 . 1 . 211
Mask
255.255.255.0
Gateway
0 . 0 . 0 . 0
IP SFP
IP
192 . 168 . 1 . 211
Mask
255.255.255.0
Gateway
0 . 0 . 0 . 0
Clock PTP
Description
NTSPTP1
Two step
Priority 1
128
Priority 2
128
Domain
0
Clock Quality
Class
6
Accuracy
33
Variance
65535
Port PTP
Mechanism
E2E
Protocol
UDP
ETH
UDP6
Compatibility
Off
Timeout [s]
0
Unicast
Disable
Asymetry [s]
0
Sync
0
Delay
0
Pdelay
0
Announce
0
Receipt
0
DSCP
0
Enable
Mixed
Poll
0
Time
UTC offset enable
Offset
0
IP Master Node
IP address
0 . 0 . 0 . 0

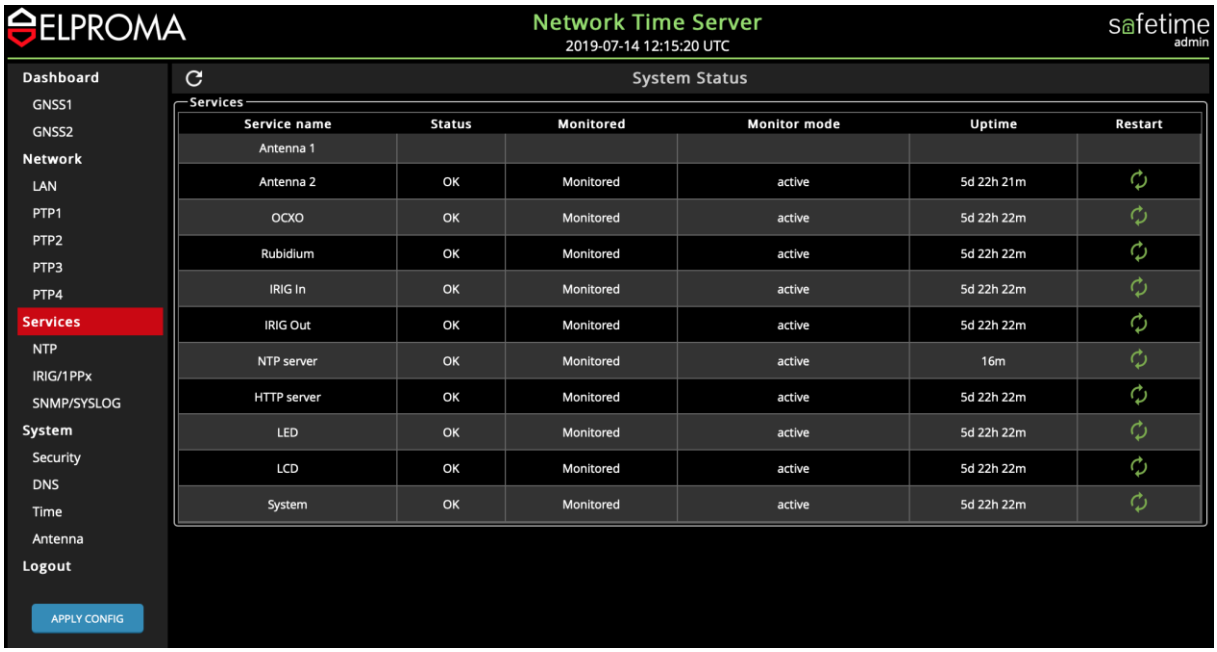

ELPROMA
Network Time Server
2019-07-14 11:38:46 UTC
safetime
admin
Dashboard
GNSS1
GNSS2
Network
LAN
PTP1
PTP2
PTP3
PTP4
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Security
DNS
Time
Antenna
Logout
APPLY CONFIG
PTP interface 1
PTP1 (/dev/ptp1)
Profile
Custom
MAC mode
ETH
Mode
Master
IP Eth
IP
192 . 168 . 1 . 211
Mask
255.255.255.0
Gateway
0 . 0 . 0 . 0
IP SFP
IP
192 . 168 . 1 . 211
Mask
255.255.255.0
Gateway
0 . 0 . 0 . 0
Clock PTP
Description
NTSPTP1
Two step
Priority 1
128
Priority 2
128
Domain
0
Clock Quality
Class
6
Accuracy
33
Variance
65535
Port PTP
Mechanism
E2E
Protocol
UDP
Compatibility
Off
Timeout [s]
0
Unicast
Disable
Master
Slave
Asymetry [s]
Sync
0
Delay
0
Pdelay
0
Announce
0
Receipt
0
DSCP
0
SNTP Server
Enable
Mode
Mixed
Poll
0
IP Master Node
IP address
0 . 0 . 0 . 0


ELPROMA
Network Time Server
2019-07-14 11:39:07 UTC
safetime
admin
Dashboard
GNSS1
GNSS2
Network
LAN
PTP1
PTP2
PTP3
PTP4
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Security
DNS
Time
Antenna
Logout
APPLY CONFIG
PTP interface 1
PTP1 (/dev/ptp1)
Profile
Custom
MAC mode
ETH
Mode
Master
IP Eth
IP
192 . 168 . 1 . 211
Mask
255.255.255.0
Gateway
0 . 0 . 0 . 0
IP SFP
IP
192 . 168 . 1 . 211
Mask
255.255.255.0
Gateway
0 . 0 . 0 . 0
Clock PTP
Description
NTSPTP1
Two step
Priority 1
128
Priority 2
128
Domain
0
Clock Quality
Class
6
Accuracy
33
Variance
65535
Port PTP
Mechanism
Protocol
Compatibility
Timeout [s]
0
Unicast
Disable
Asymetry [s]
0
Sync
0
Delay
0
Pdelay
0
Announce
0
Receipt
0
DSCP
0
Unicast
Manycast
Broadcast
Mixed
Time
UTC offset enable
Offset
0
IP Master Node
IP address
0 . 0 . 0 . 0

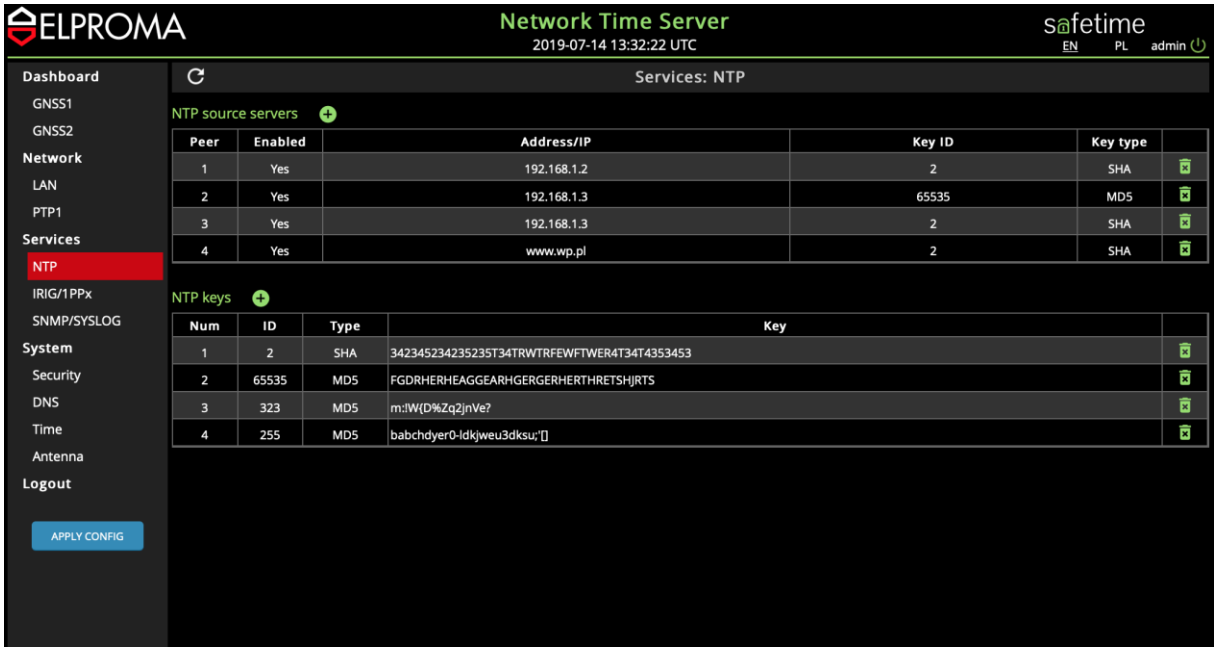
35. Software WWW – Services

. NTP backup servers

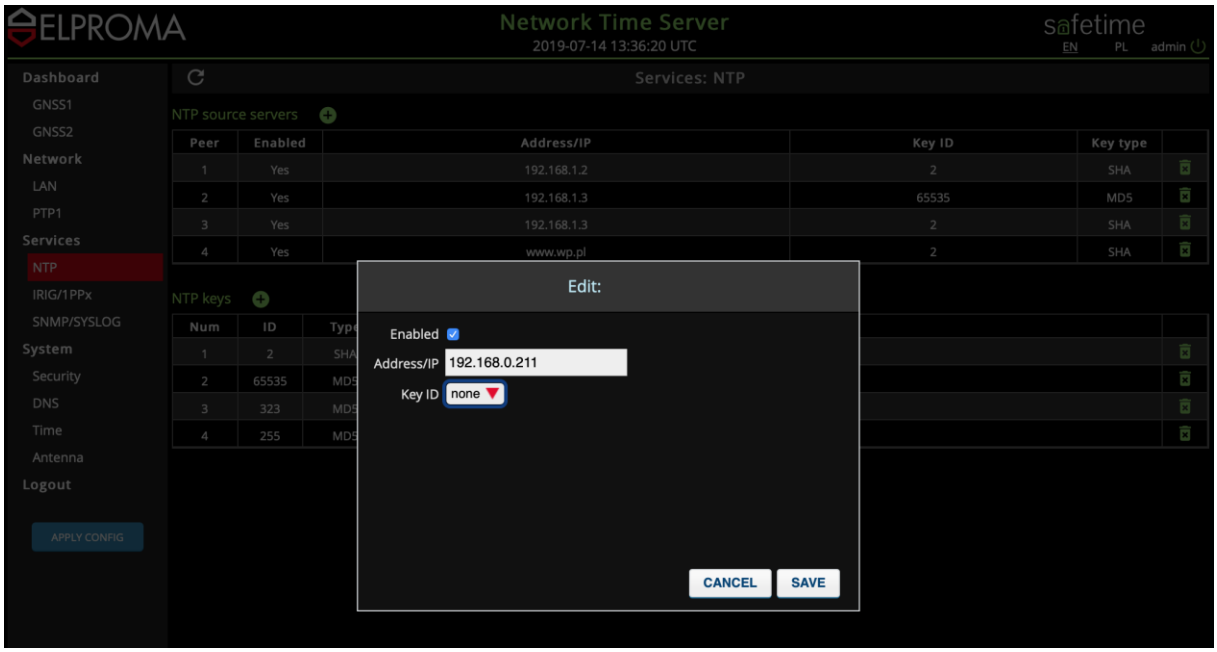
The NTS-x000 is state of the art technology server. It is designed to ensure robust synchronization, cybersecurity and easy maintenance. Therefore, each of its modules operates autonomously. This is possible due to fact, that each functional module is independent, and microprocessor controlled. You can trace and monitor status of each independent service, but you can also reset each of them.



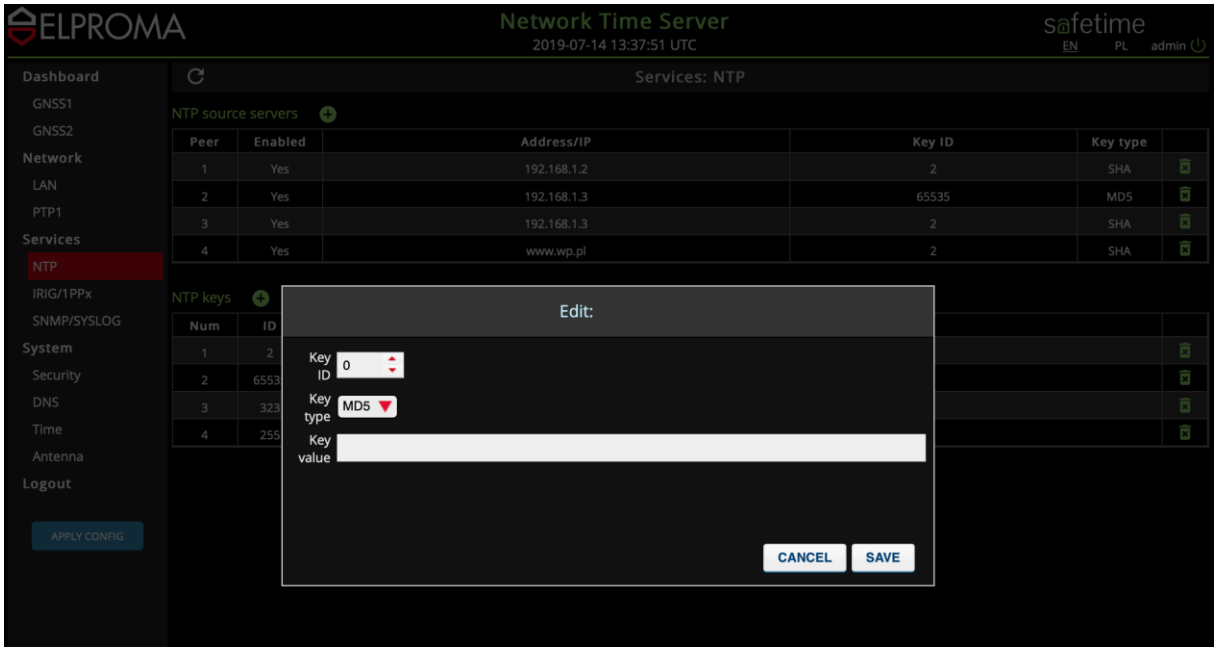
You can define up to 10 of backup NTP time servers. They can be used when missing stratum 0 ref.



To add new NTP-server please click (+) icon located on the top of table and provide IPv4 address:

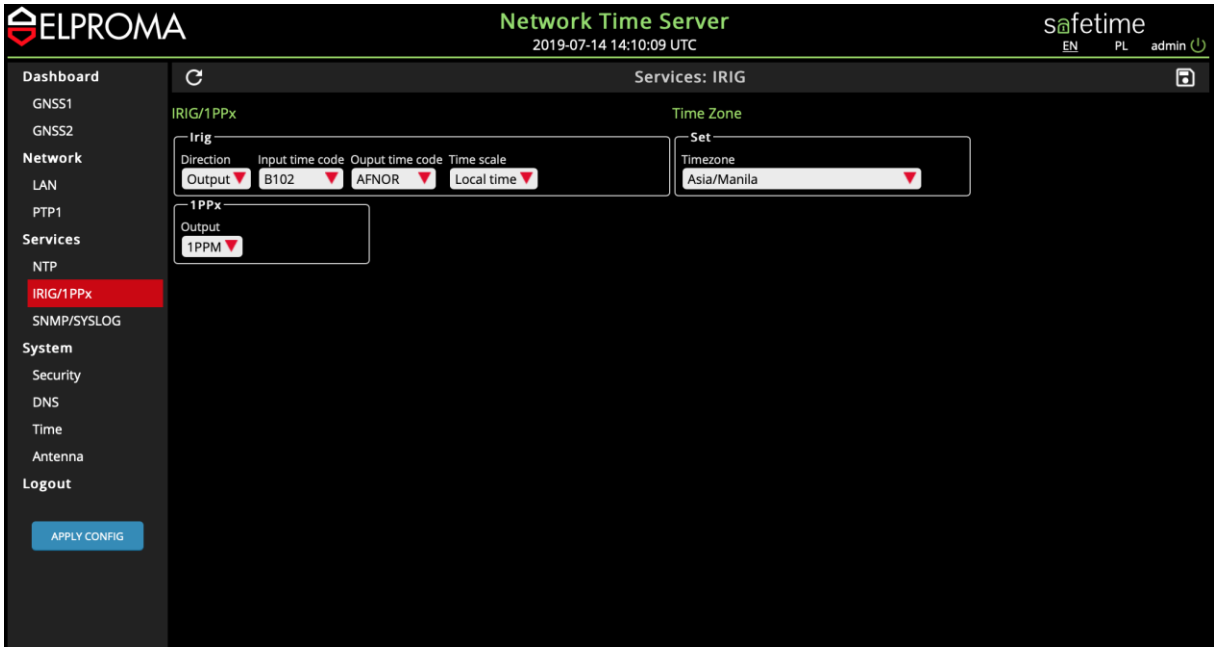


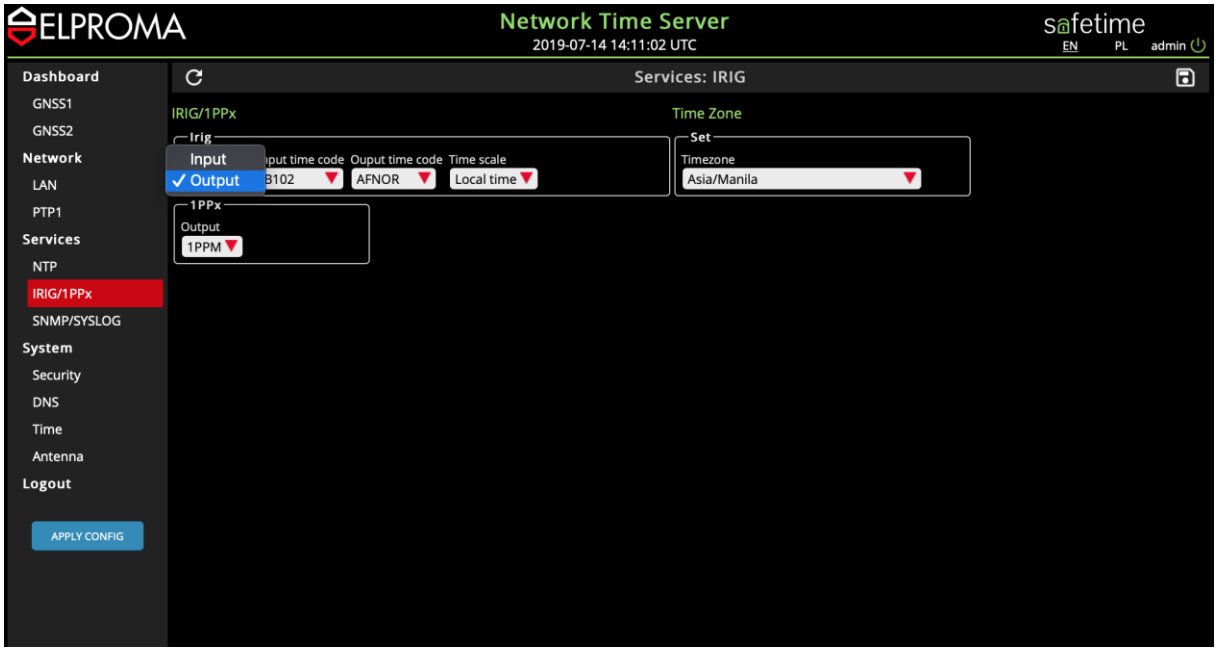
You can also add/remove authentication keys (used when NTP-authentication is necessary):



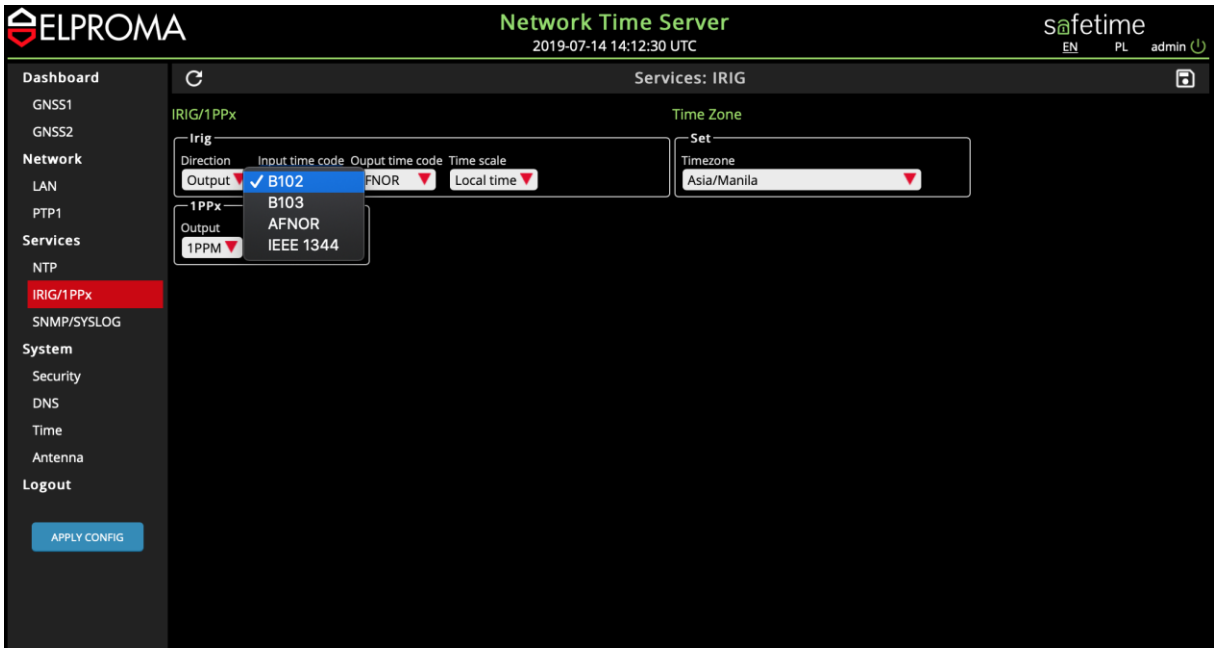
. IRIG-B/PPS-x Management

You can define direction, coding, time-code format and time-scale for IRIG-B interface:

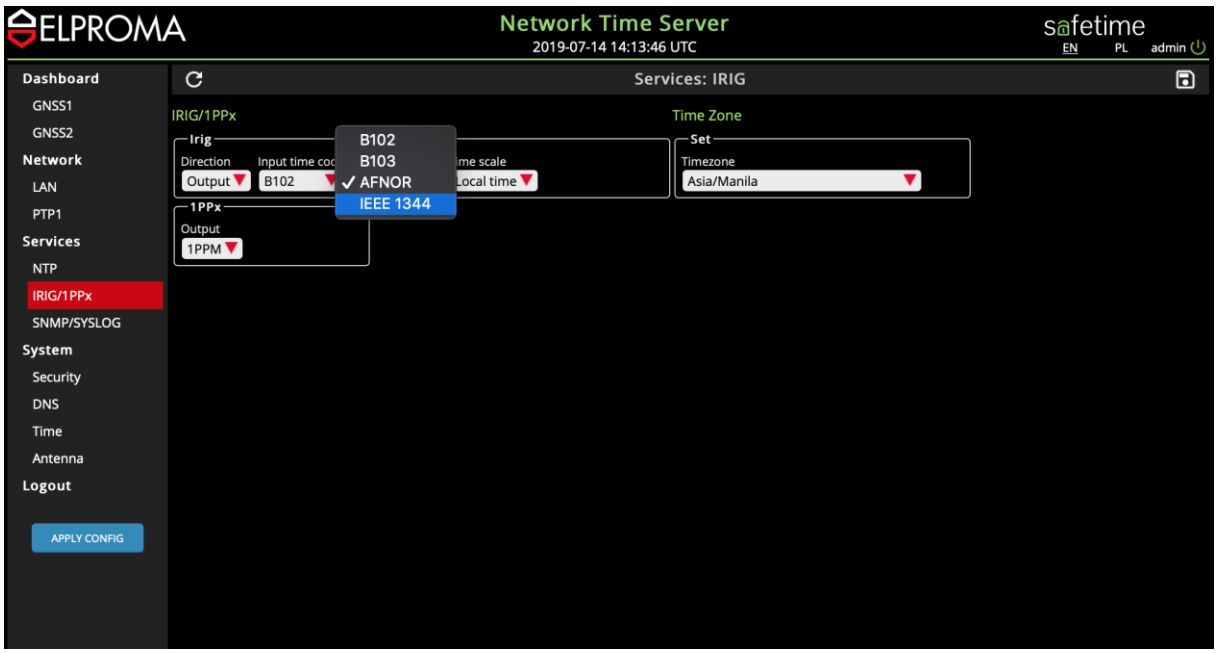




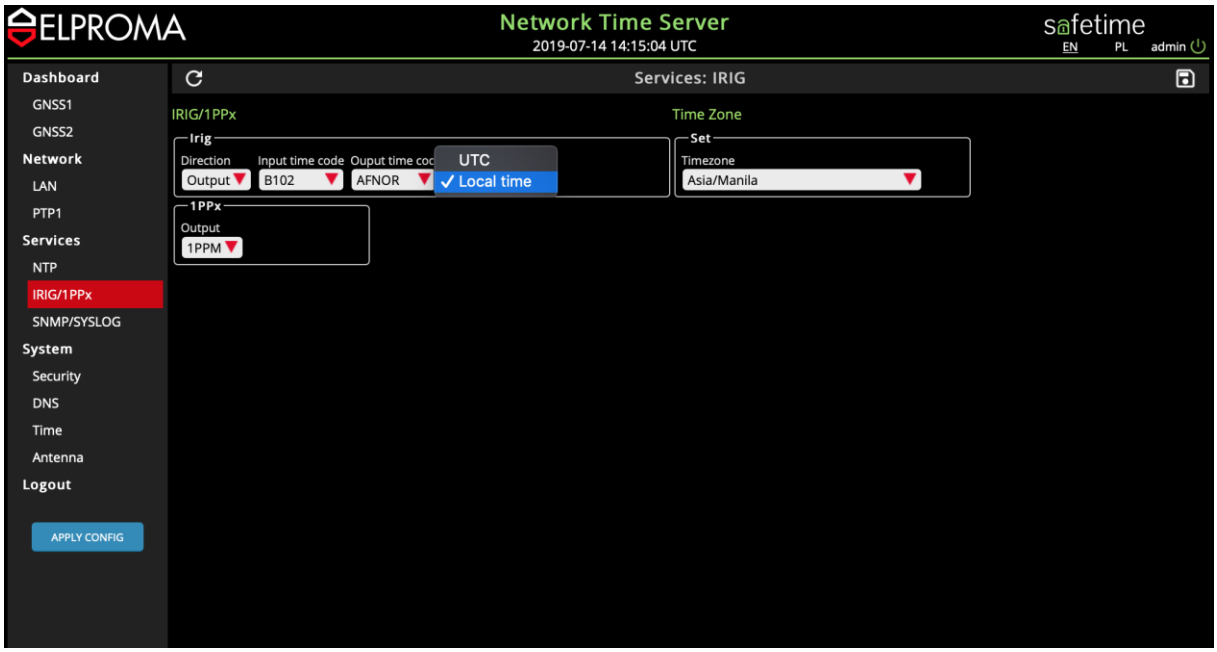
Setting IRIG-B input time-code:



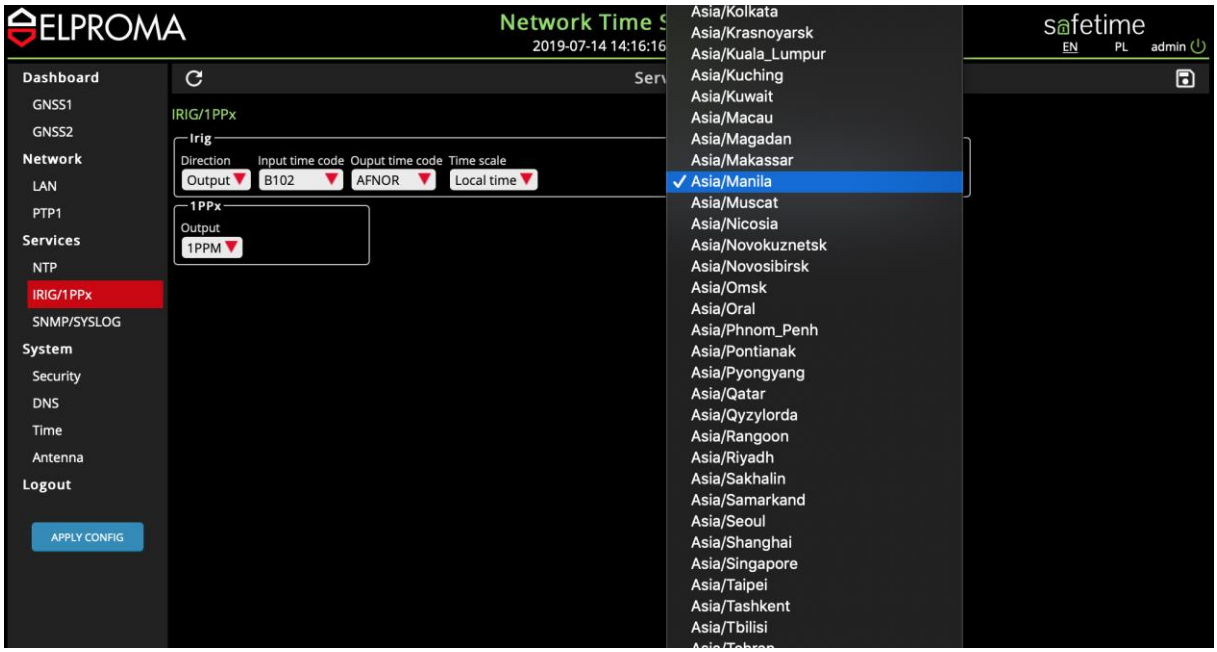
Setting IRIG-B output time-code:



IRIG-B can be defined to operate LOCAL TIME or UTC:

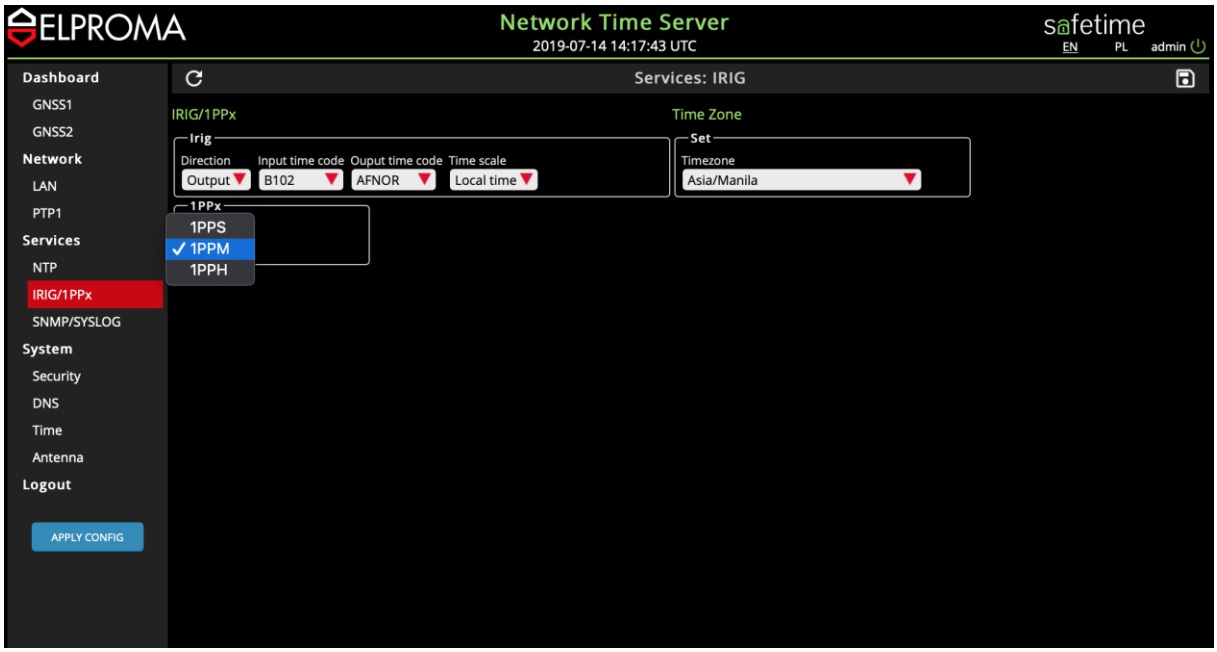


If you choose LOCAL TIME setting, you should also specify your localization for it:

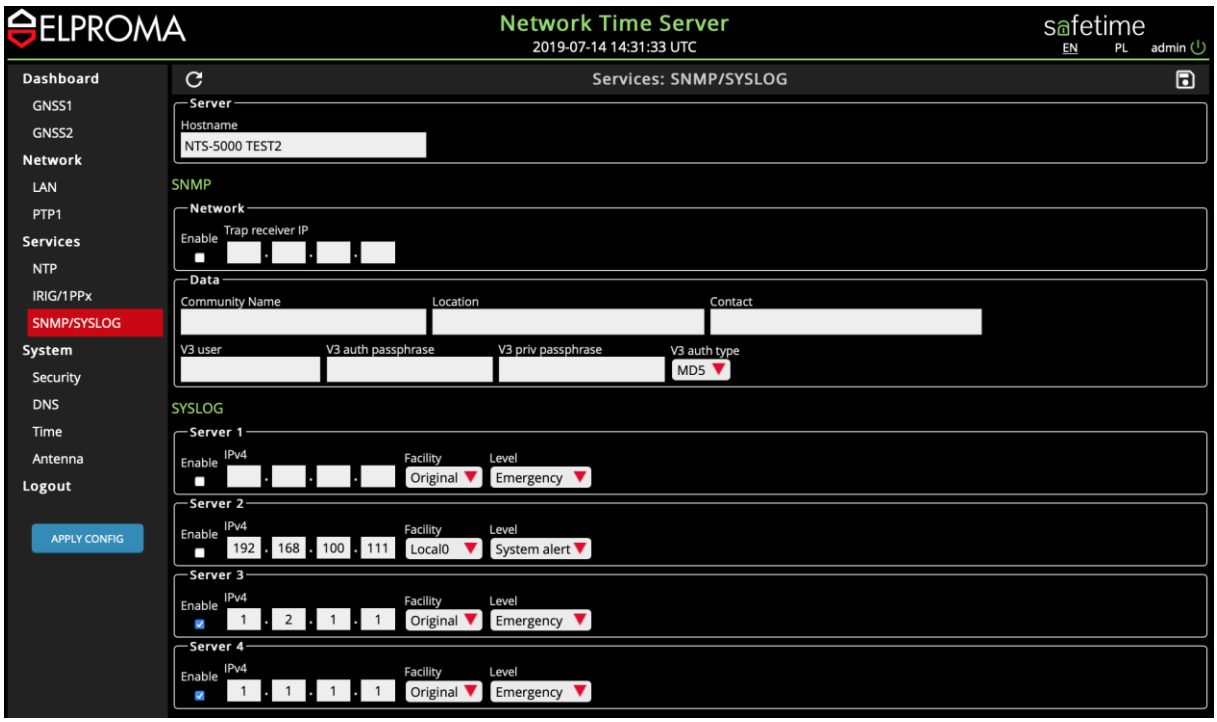


You can also decide on PPS output frequency standard:

- PPS (Pulse Per Second)
- PPM (Pulse Per Minute)
- PPH (Pulse Per Hour)

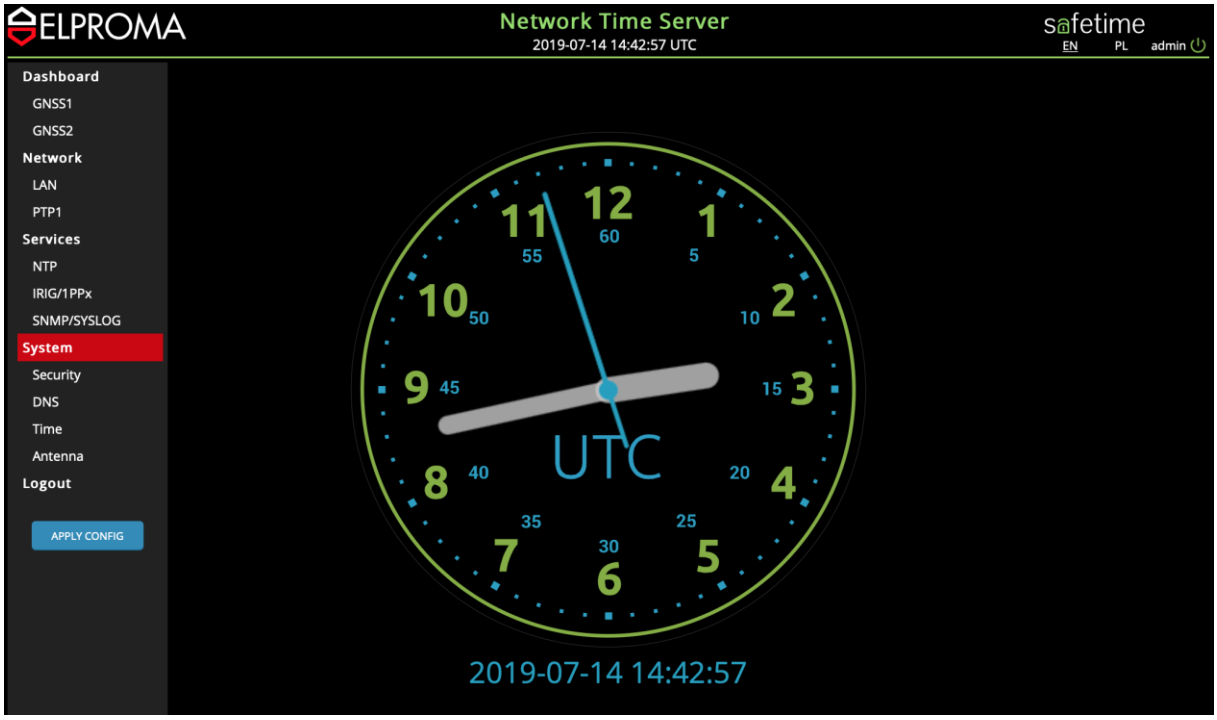

ELPROMA
Network Time Server
2019-07-14 14:17:43 UTC
safetime
EN PL admin
Dashboard
GNSS1
GNSS2
Network
LAN
PTP1
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Security
DNS
Time
Antenna
Logout
APPLY CONFIG
Services: IRIG
IRIG/1PPx
Time Zone
Irig
Direction
Output
Input time code
B102
Ouput time code
AFNOR
Time scale
Local time
Set
Timezone
Asia/Manila
1PPx
1PPS
1PPM
1PPH

. SYSLOG/SNTP

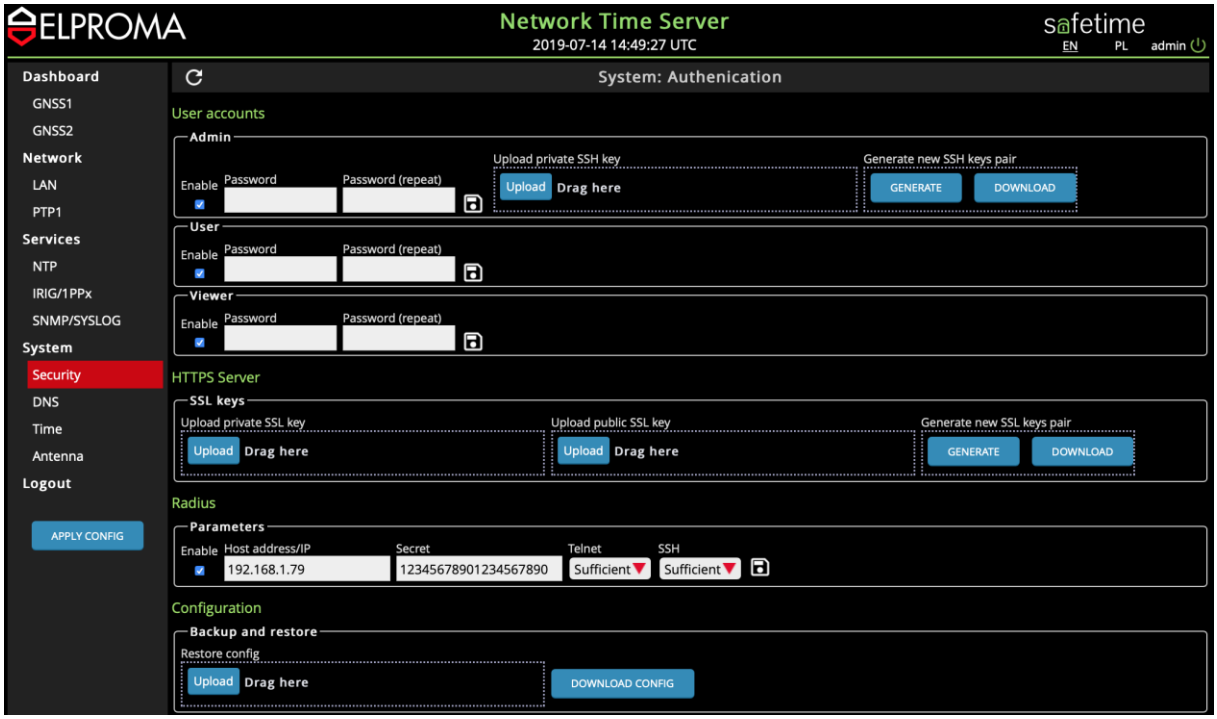

ELPROMA
Network Time Server
2019-07-14 14:31:33 UTC
safetime
EN PL admin
Dashboard
GNSS1
GNSS2
Network
LAN
PTP1
Services
NTP
IRIG/1PPx
SNMP/SYSLOG
System
Security
DNS
Time
Antenna
Logout
APPLY CONFIG
Services: SNMP/SYSLOG
Server
Hostname
NTS-5000 TEST2
SNMP
Network
Enable
Trap receiver IP
Data
Community Name
Location
Contact
V3 user
V3 auth passphrase
V3 priv passphrase
V3 auth type
MD5
SYSLOG
Server 1
Enable
IPv4
Facility
Original
Level
Emergency
Server 2
192 168 100 111
Local0
System alert
Server 3
1 2 1 1
Server 4
1 1 1 1

36. Software WWW – System Security & DNS

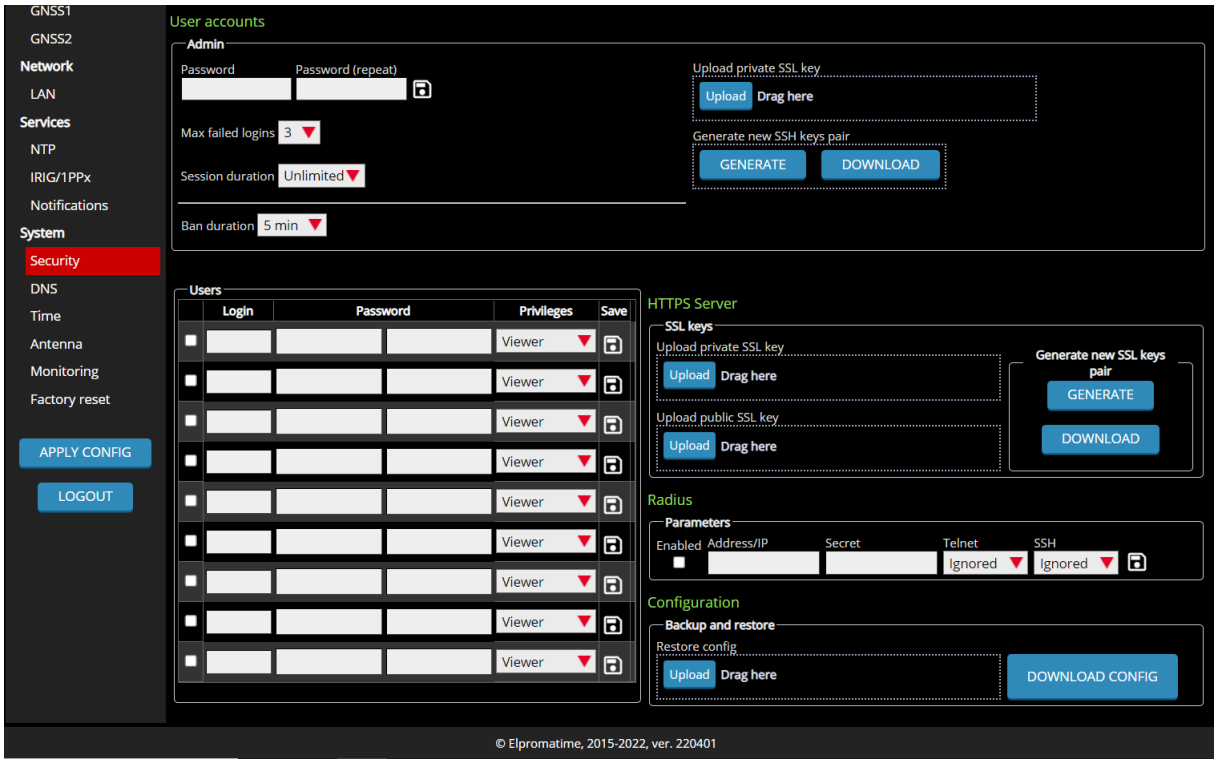
Following screen presents system time CLOCK frequently used by admins as information dashboard:



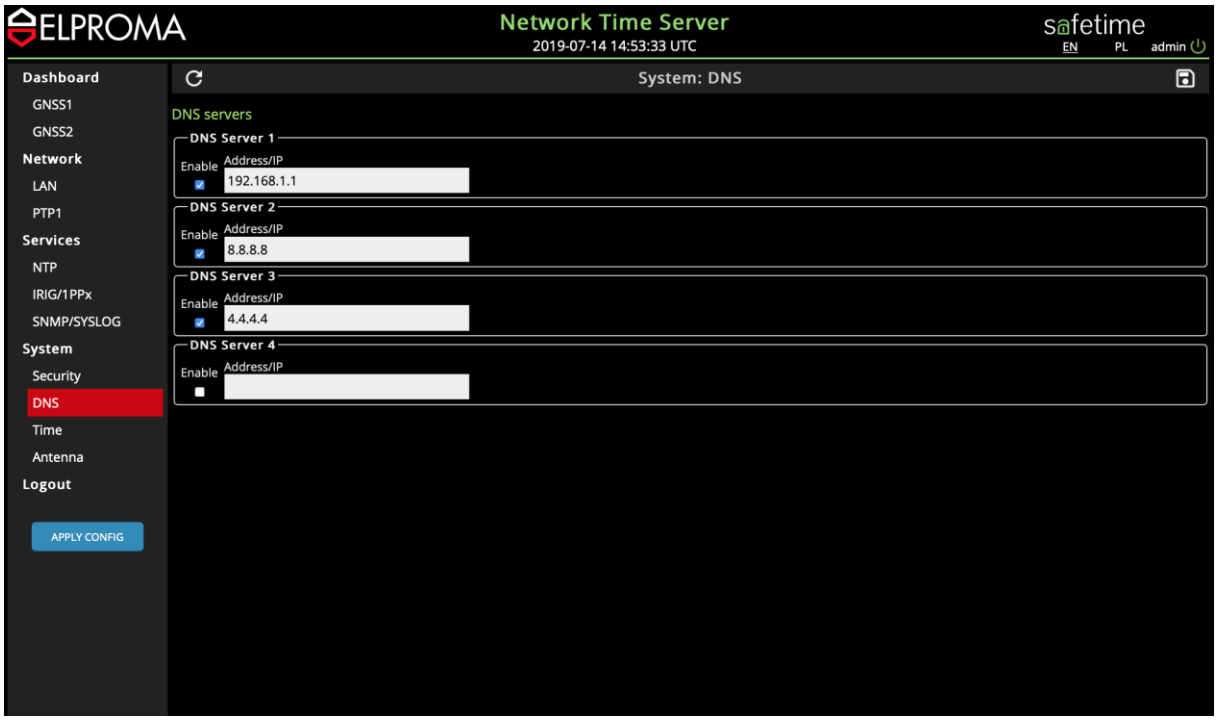
You can generate, upload or download SSL, SSH keys and manage HTTPS, Radius and configuration



You can define multiple users accessing time server:



You can define up to 4x DNS servers:



Setup SSH

37. Software SSH - Setup LAN1-LAN2

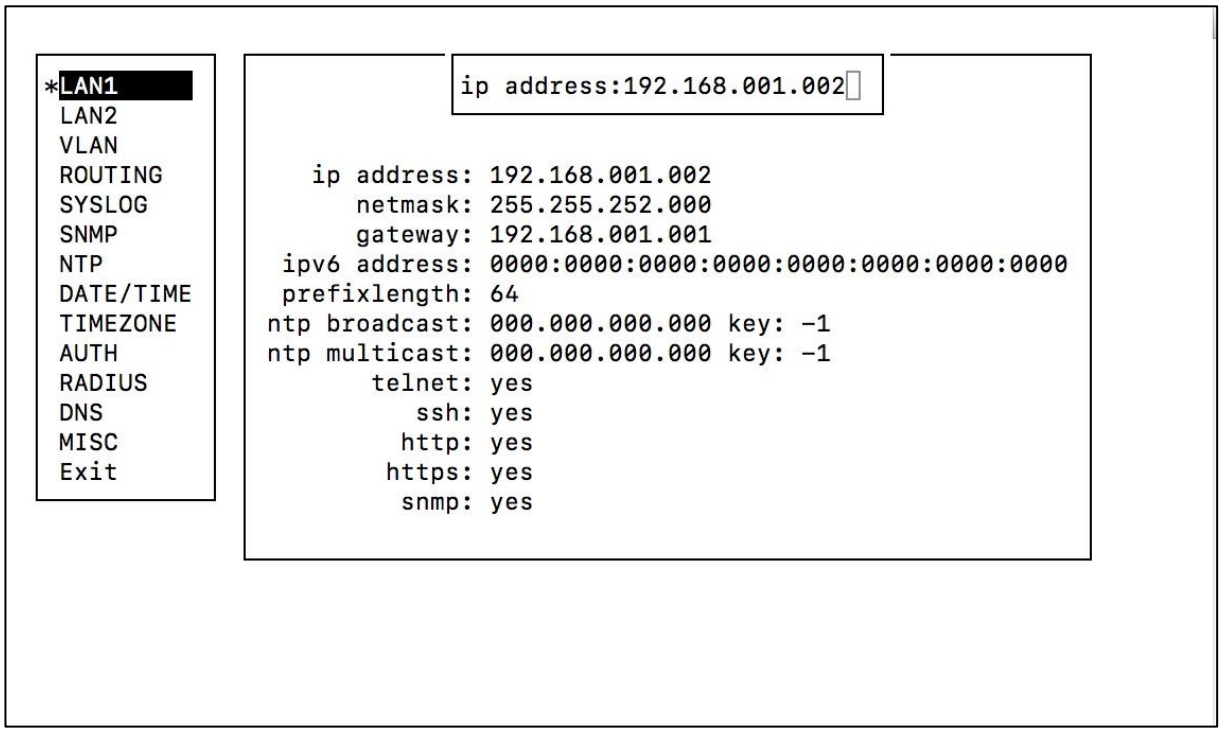
This chapter will let you configure std. LAN1 and LAN2 interfaces (100/10 Mbps) of NTS-x000 family products. All below presented operations of configuration are similar NTS-3000, NTS-4000, NTS-5000 but this chapter will describe details based on example of server NTS-5000.

The factory default (user and password) is:

Username: **admin**
Password: **12345**

To start configuration, please configure all LAN interfaces by simply placing:

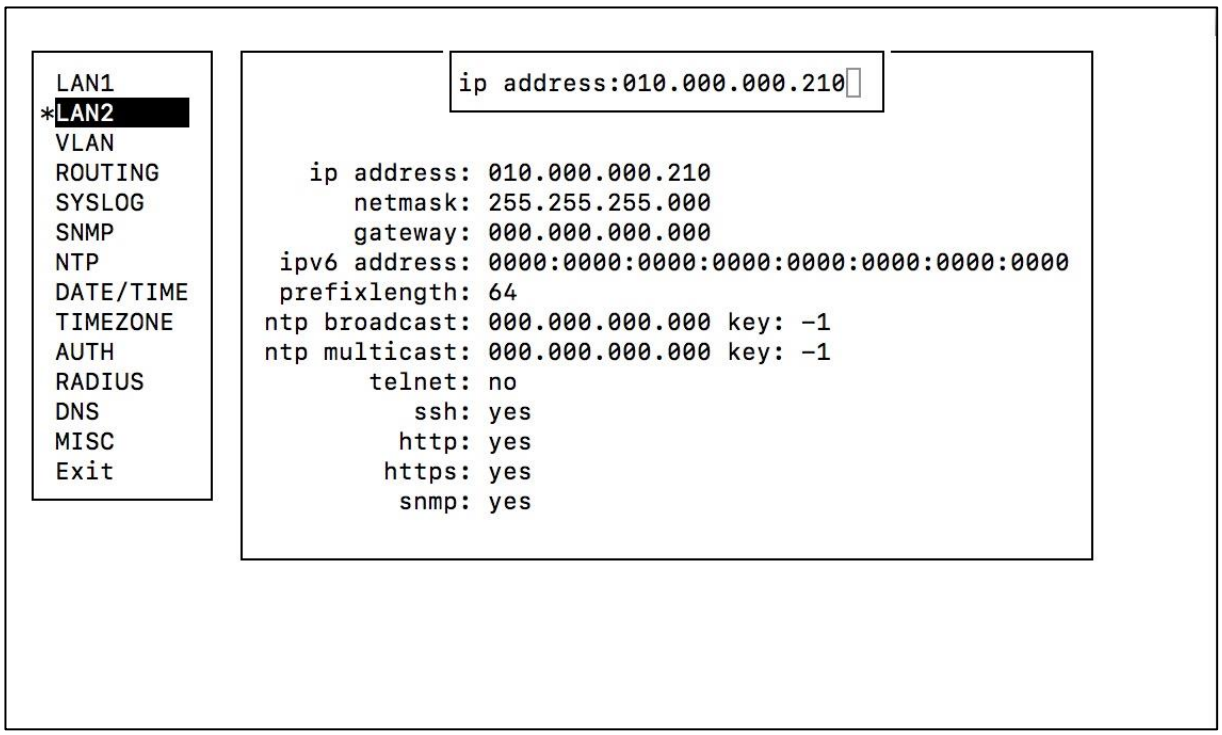
IP
MASK
DEFAULT GETEWAY



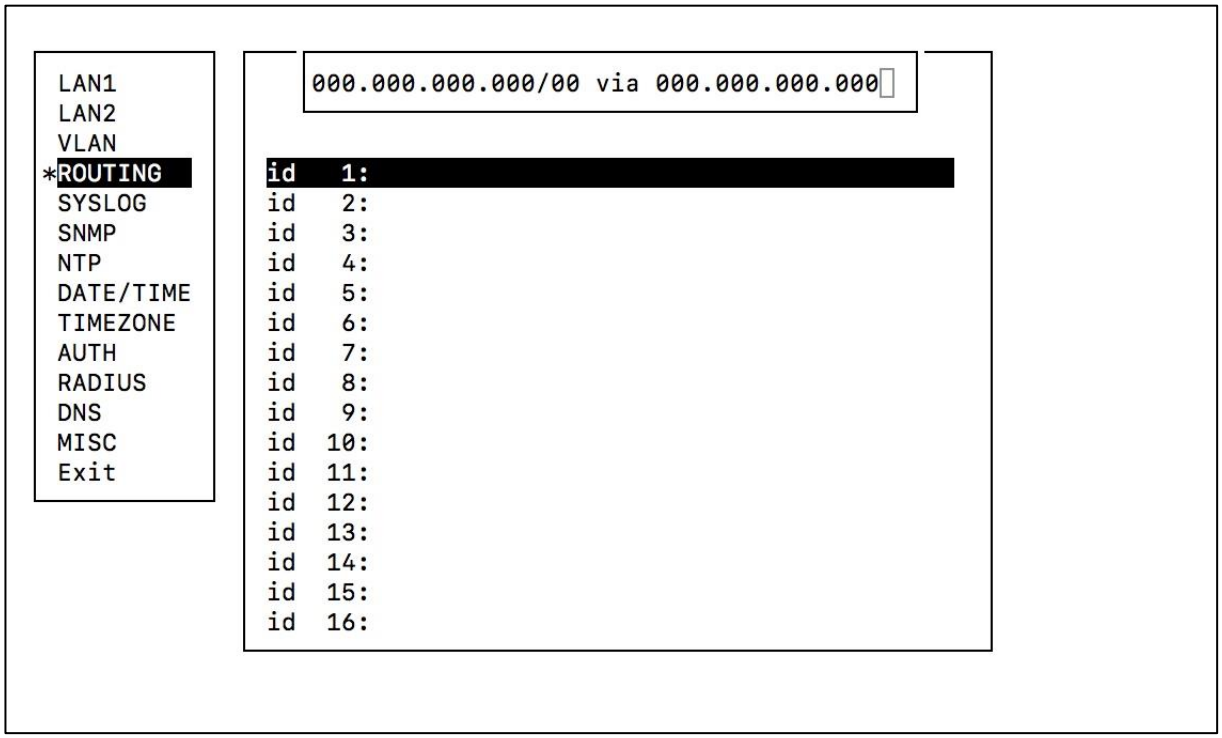
In addition, you can specify what mode you want to work on specific LAN interface. You can enable extra *broadcast* and *multicast* modes running in the background of standard client/server mode, but we suggest to finish basic configuration first before you go to more advanced options. Therefore, please leave those options for the moment now by simply filling fields 0.

Now it's time to decide what other remote services you like to keep active for future accessing. You access each LAN separately:

- Enable/Disable access via Telnet
- Enable/Disable access via SSH
- Enable/Disable access via HTTP
- Enable/Disable access via HTTPS
- Enable/Disable access via SNMP (MIB2)



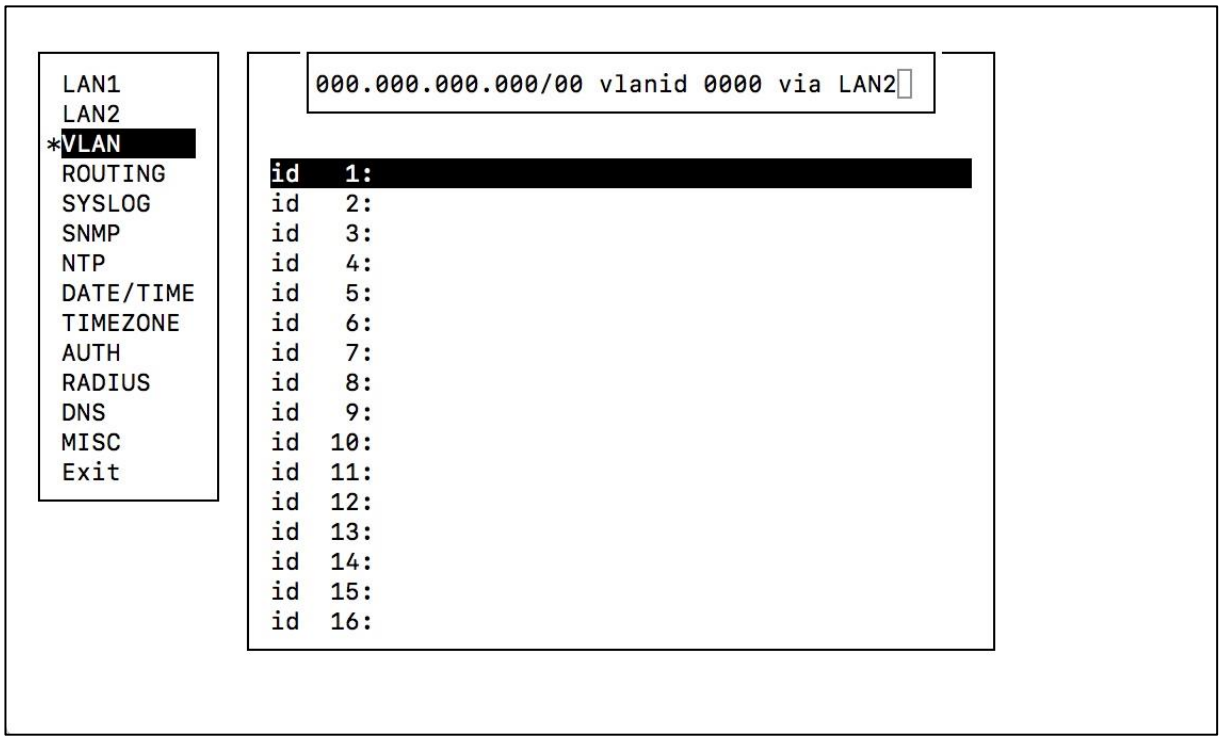
Now you should repeat above steps for LAN2. It is strongly recommended to use only 1 of 2 (LAN1 or LAN2) GATEWAYS. So, if you have chosen GATEWAY for LAN1, please do not use GATEWAY for LAN2, and vice versa. It is because using 2 GATEWAYS simultaneously might cause risk of redirecting IP return packages to wrong GATEWAY output. This is well known problem for Unix and FreeBSD. To prevent such unexpected behave we recommend setting static routing.



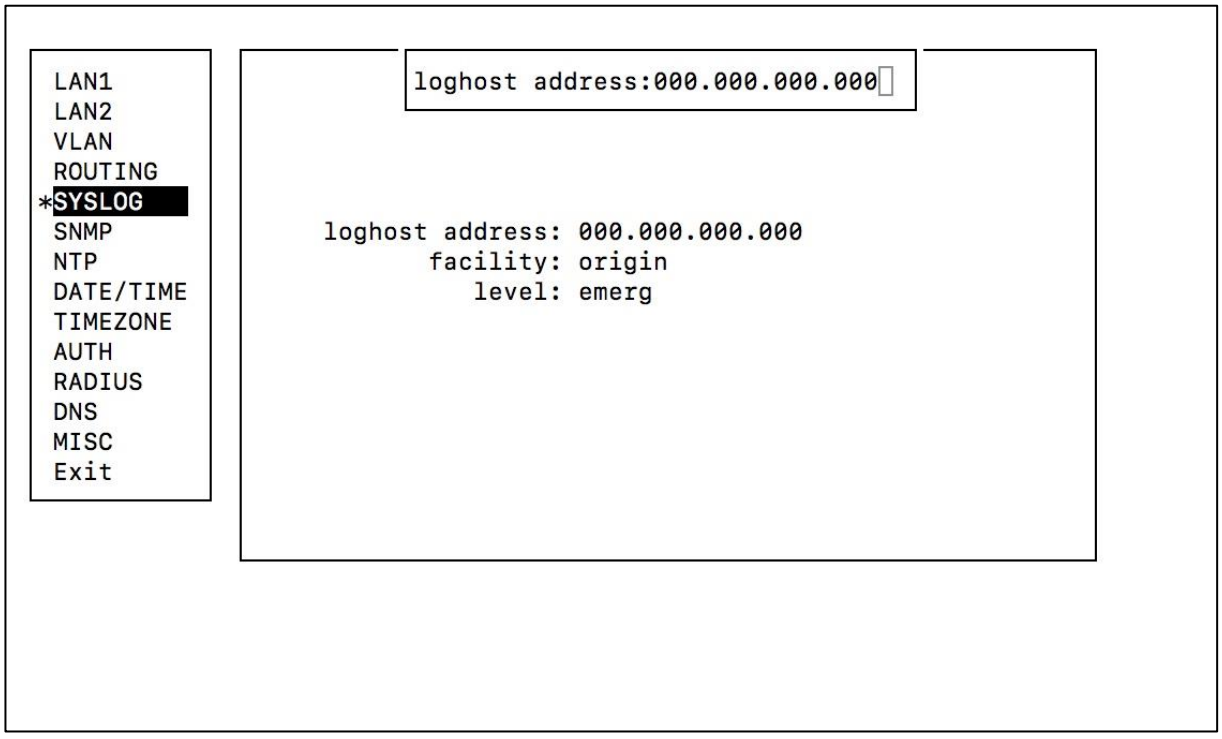
A static routing is useful when considering **stub network**, or pocket network. This is a somewhat casual term describing a computer network, or part of an internetwork with no knowledge of other networks, that will typically send much or all of its non-local traffic out via a single path, with the network aware only of a default route to non-local destinations. As a practical analogy, think of an island which is connected to the rest of the world through a bridge and no other path is available either through air or

sea. Continuing this analogy, the island might have more than one physical bridge to the mainland, but the set of bridges still represents only one logical path.

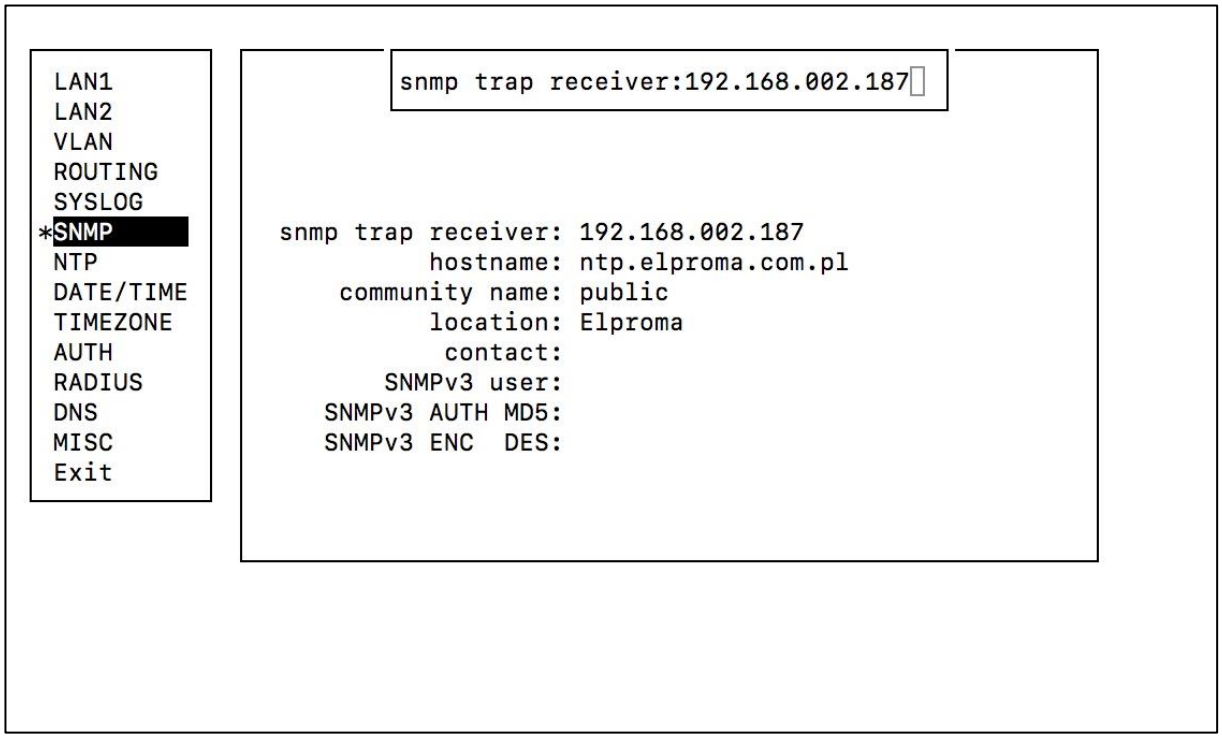
NTS-x000 can use VLAN's when linked to CISCO (for information contact ELPROMA).



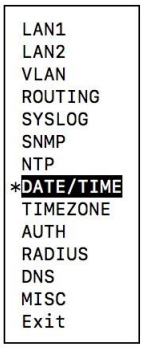
You can also specify SYSLOG server for future tracing functionality. You can configure facility and verbosity of NTS server messages, to ease log segregation on your syslog server. Please read syslog documentation for details about logs gathering.

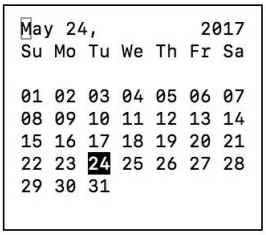


If your network supports SNMP, you can configure special MIB2 traps to implement exceptional facts you can be interesting in. It is very easy to set traps on such way that you will be informed by mail or mobile phone (SMS) on any unexpected situation may occur inside NTS server like e.g. losing GNSS antenna signal etc. Also you can trace all IP statistics using your favourite SNMP client (ie. *Mrtg*)

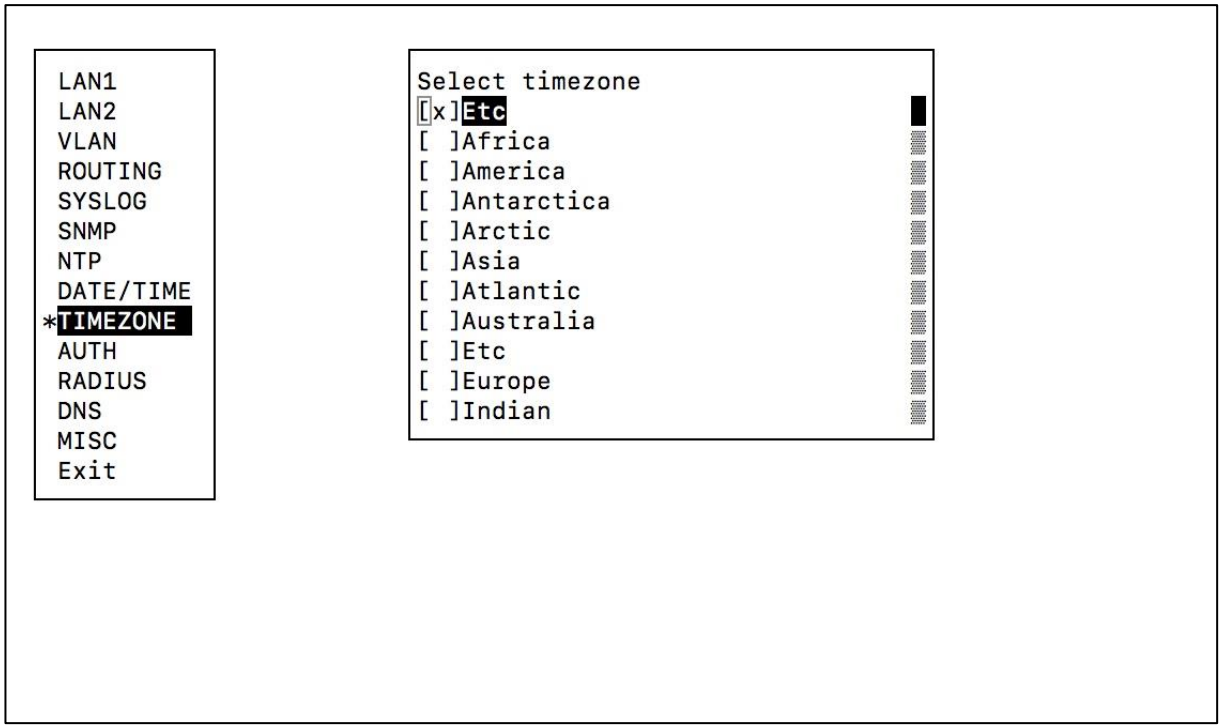


Another step is to define up to 10x NTP backup servers for single NTS server unit. In this mode NTS server reminds Stratum 1 if GPS antenna works fine or any other time source (PPS_IN, Rubidium/NTS-5000only, OCXO). But in case of missing accurate time source NTS server checks backup servers list. If NTP accepts any of them the NTS server reduce its stratum to N-1 (where N is a Stratum of approved server taken out of backup list). We advise to specify only Stratum 1 servers on NTS server backup list. This does not let reduce NTS server Stratum below 2. The backup NTP servers should be configured for authorized NTP transmission. For this reason, there is another field key pointing position in encryption list with MD5 keys. But in this step we still advice to continuous Setup without encrypted associations. Safety and protection will be discussed shortly in this manual.

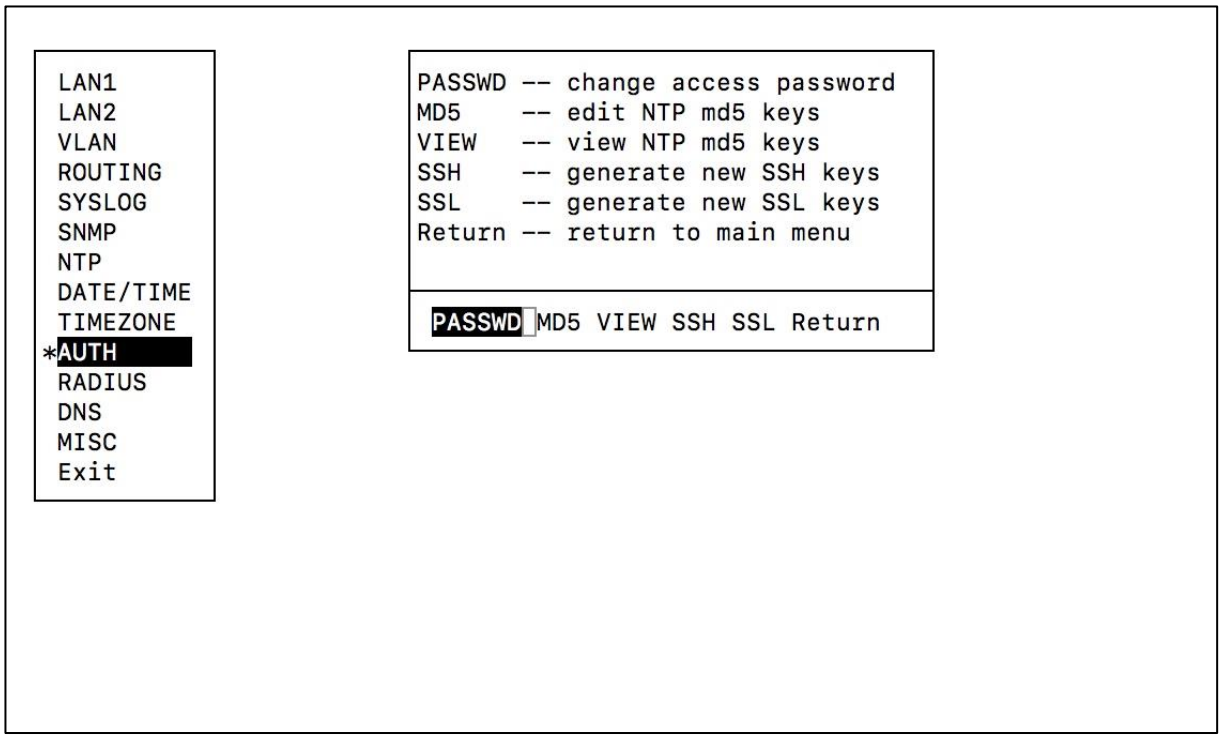




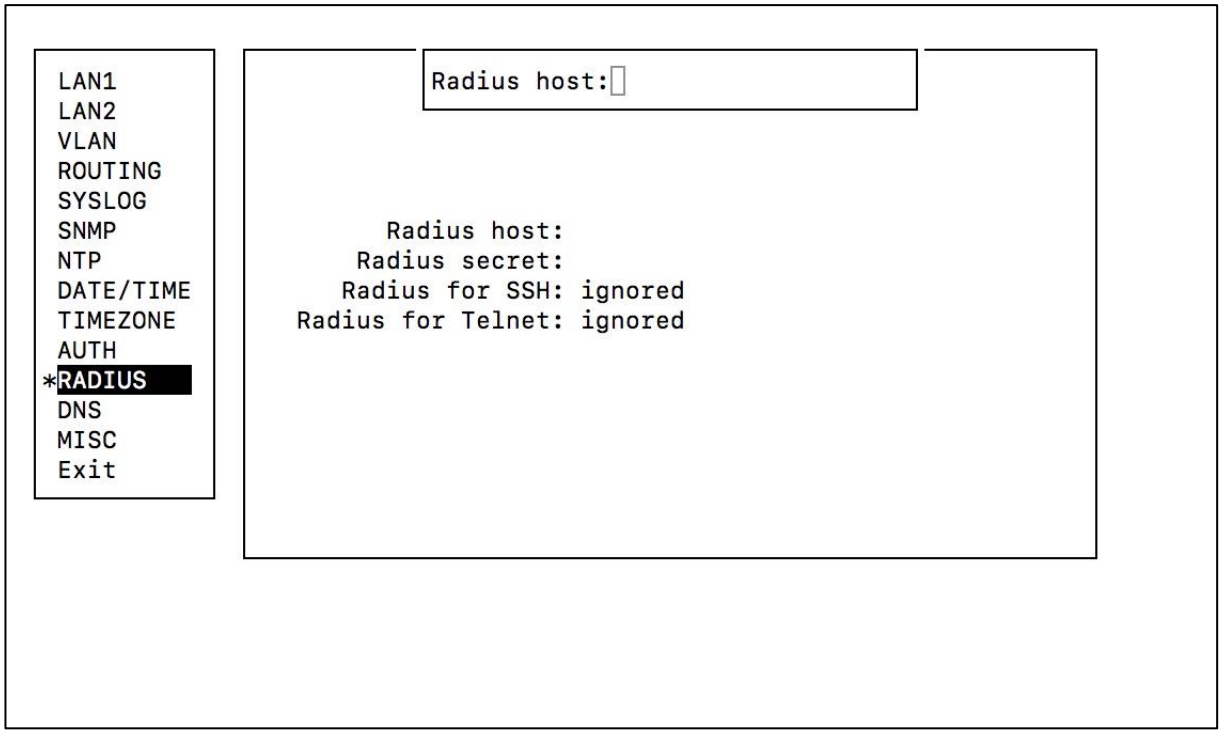
Setting DATE/TIME is a tool to pre-set LOCAL clocks time. It always use to be UTC however some customers use this option to maintaining other than UTC timescales (GPS). This can be useful option to maintain local zone time too.

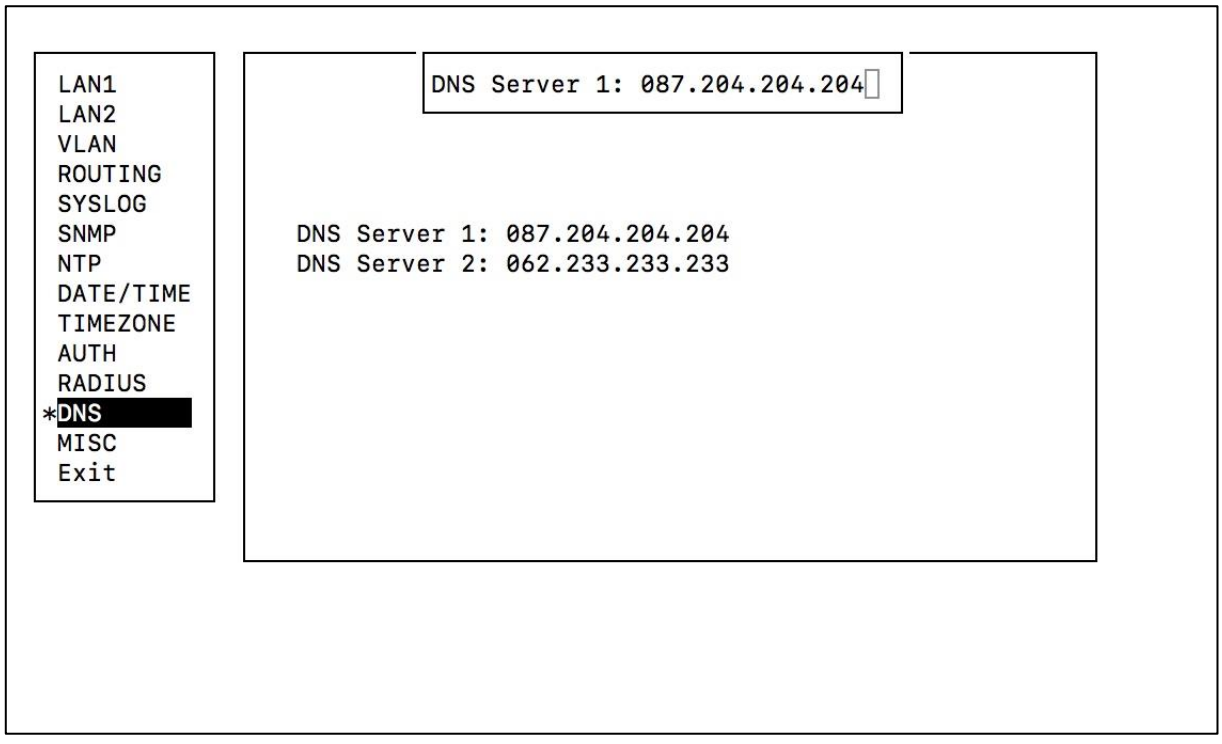


Time Zone service lets set LCD time to local time. It has information meaning only and timeserver works and supports universal UTC timescale.

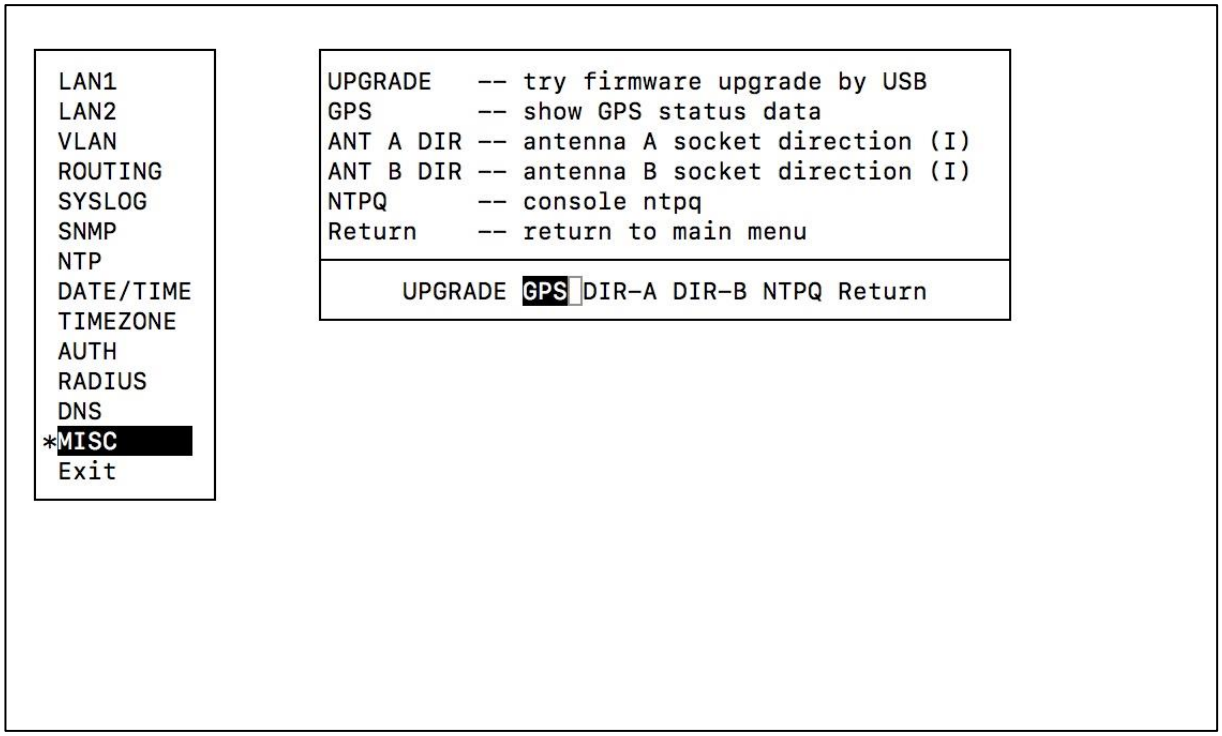


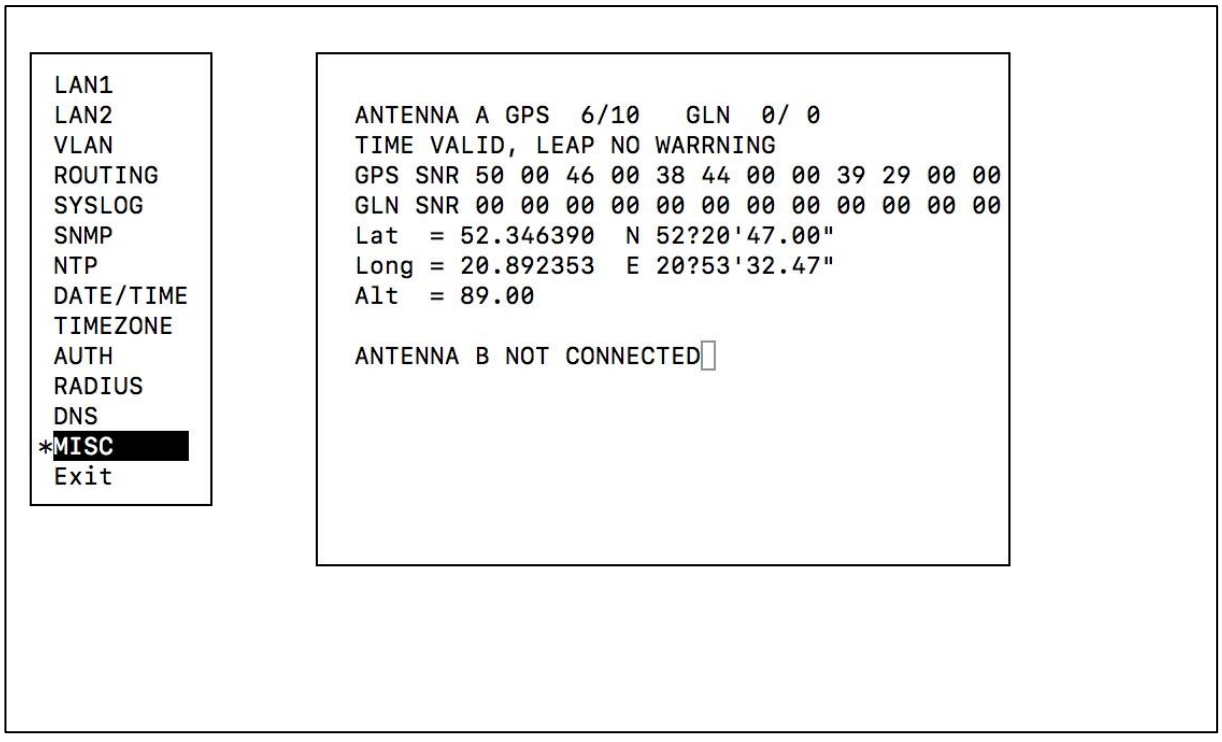
AUTH includes set of settings related to security and authentication including MD5 and SSH/SSL keys.



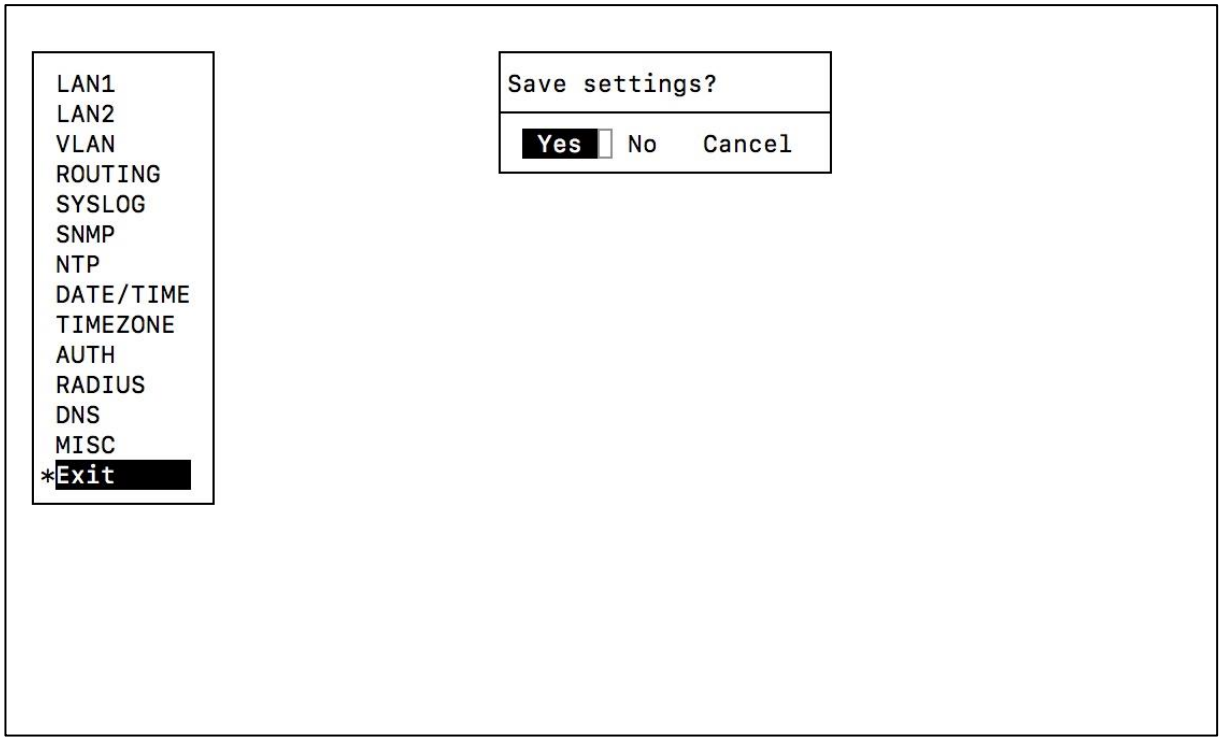


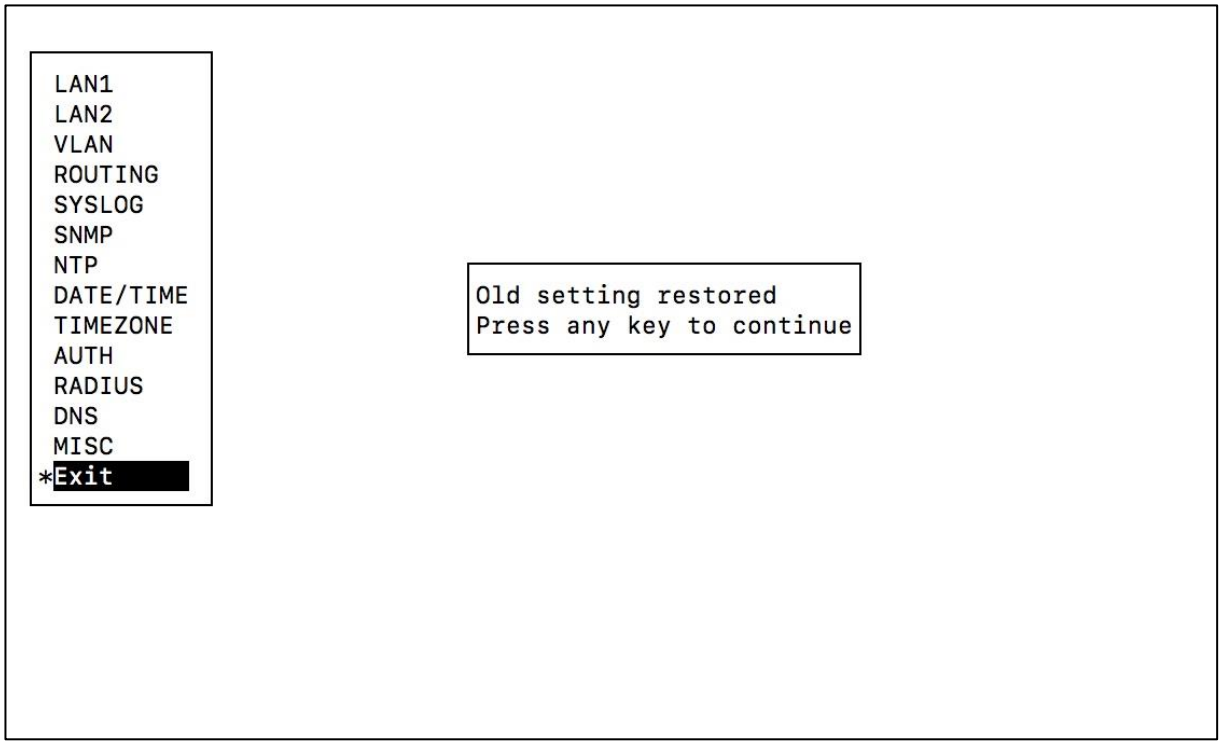
Upgrade. To perform firmware upgrade you should put USB memory stick with new firmware into port on front panel and then activate this option. **GPS.** With this function you can monitor GNSS receiver messages on line, just as they came. You can check receiver location and GPS status bits. **ANT A/B DIR.** This functions give you ability to send time signal in NMEA/PPS format to another NTS series unit. Just configure one antenna socket as an output (O) and connect it with 1 to 1 twisted pair cable with RJ-45 TIA-568B connectors to antenna input (I) of second NTS.





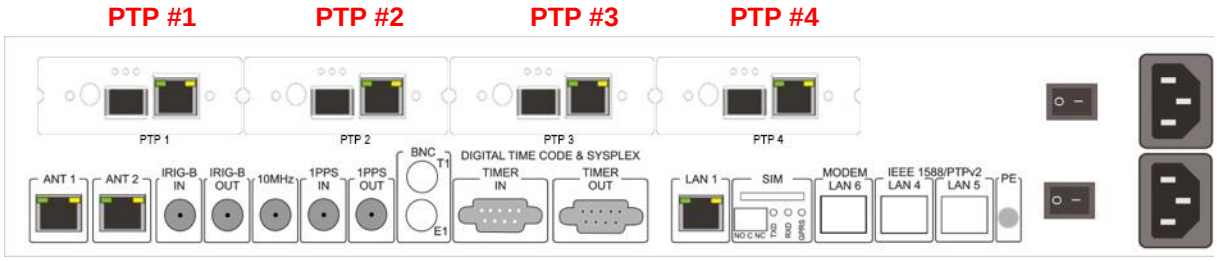
Once setup is done you have to exit with save option. Do not turn off power when NTS is saving settings (appropriate message appear on LCD). The NTS–5000 supports SETUP available via SSH and TELNET service or serial console port located on front panel (DTE configuration, 9600 baud, 8 data bits, no parity, 1 stop bit).


LAN1
LAN2
VLAN
ROUTING
SYSLOG
SNMP
NTP
DATE/TIME
TIMEZONE
AUTH
RADIUS
DNS
MISC
*Exit
Save settings?
Yes No Cancel

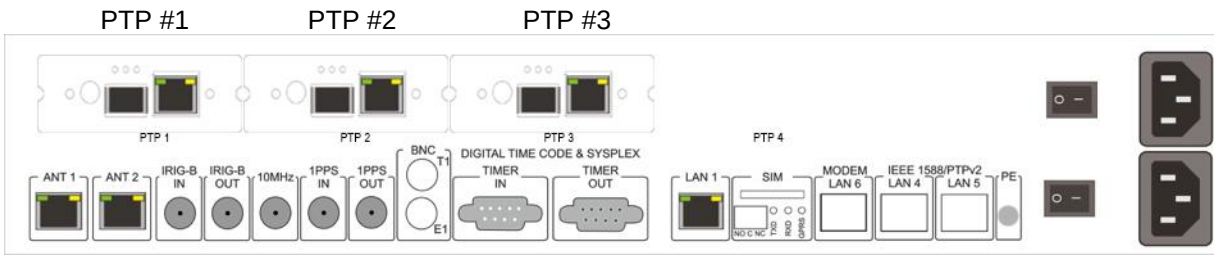

LAN1
LAN2
VLAN
ROUTING
SYSLOG
SNMP
NTP
DATE/TIME
TIMEZONE
AUTH
RADIUS
DNS
MISC
*Exit
Old setting restored
Press any key to continue

38. Software SSH - Setup LAN3-LAN10

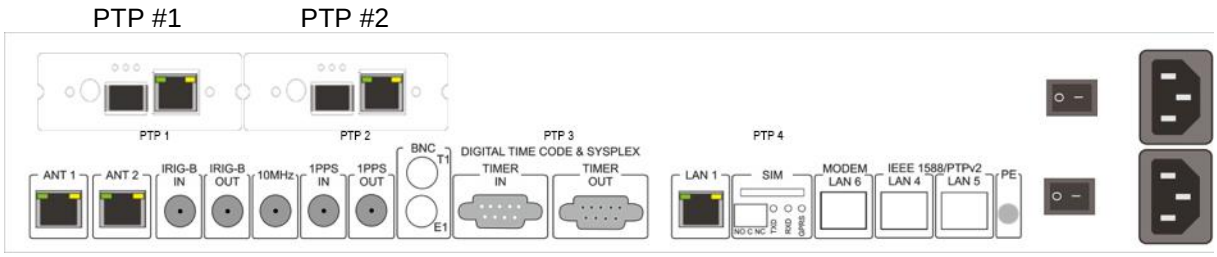
This chapter includes information dedicated to NTS-5000/NTS-5000LITE PTP IEEE1588 hardware extensions. The NTS-5000/NTS-5000LITE can be equipped with 1-4 optional hardware PTP modules located at back panel of server. NTS-5000 is delivered with built-in (mounted) and calibrated PTP IEEE1588 interfaces. Therefore, all hardware PTP interfaces must be ordered and assembled at factory. If you have ordered less that required PTP interfaces, please contact Elproma technical support.



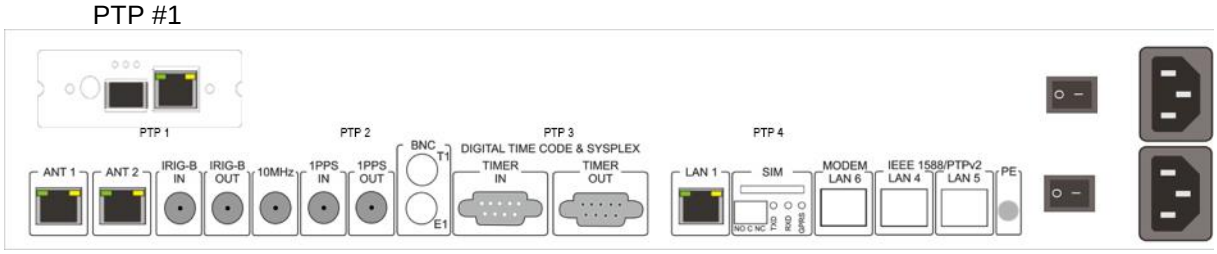
NTS-5000 Back Panel w/ high precision x4 interfaces: PTP1, PTP2, PTP3, PTP4



NTS-5000 Back Panel w/ high precision x3 interfaces: PTP1, PTP2, PTP3

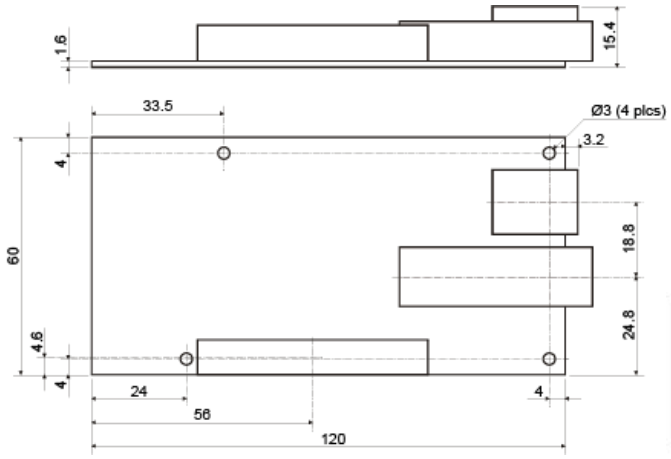


NTS-5000 Back Panel w/ high precision x2 interfaces: PTP1, PTP2

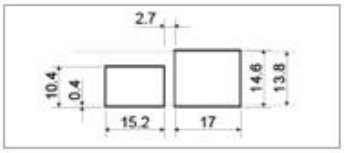


NTS-5000 Back Panel w/ high precision single PTP1 interface

Ultra-high precision nanosecond [ns] PTP/IEEE1588 extension card



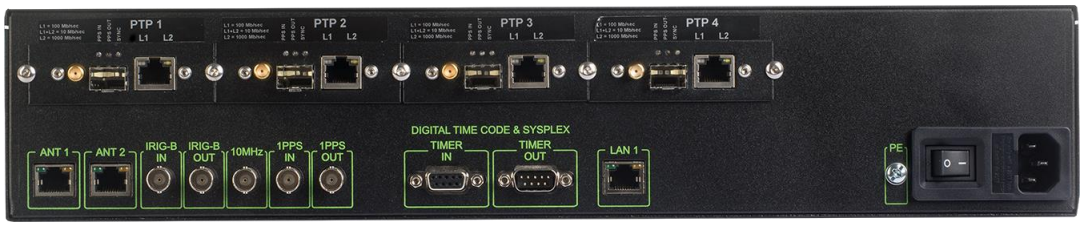
PTP1-PTP4 hardware extension board (top view)



PTP1-PTP4 panel view

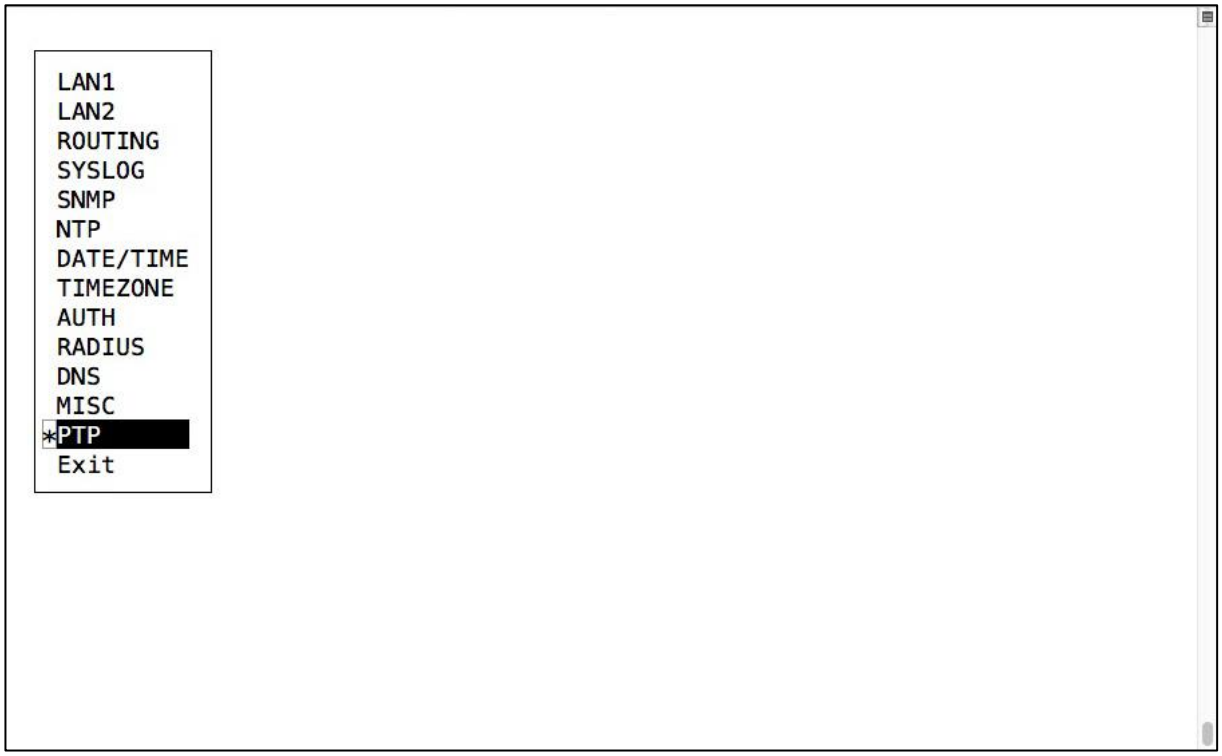
PTP1-PTP4 hardware extension cards at NTS-5000 (front view)

PTP1-PTP4 hardware extension cards at NTS-5000 (top view)



NTS-5000/NTS-5000LITE back panel view

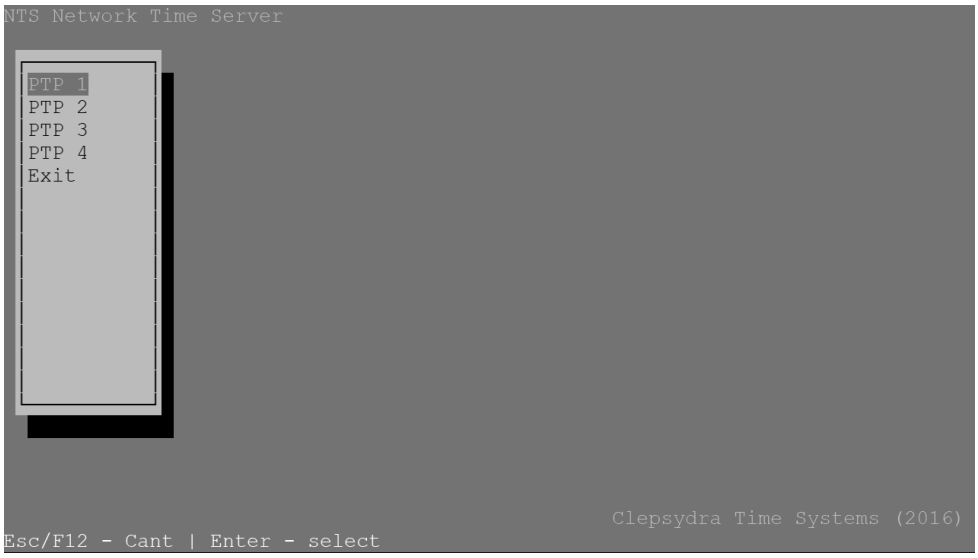
The 1-4 hardware PTP cards must be factory pre-installed. The firmware software setup automatically recognised them and a new menu item PTP is displayed a last line before Exit item:



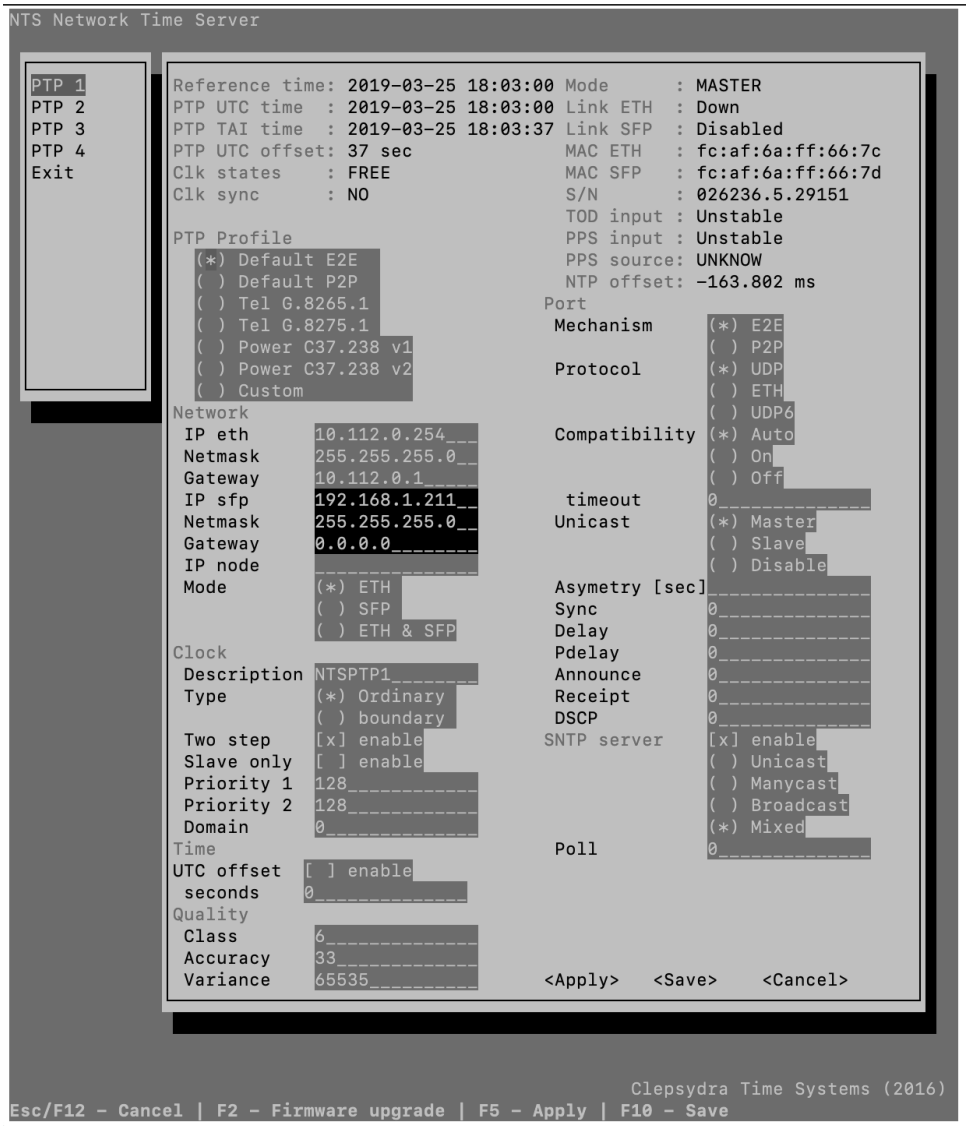
The std. UID and Password for setup are:

Username: **admin**
Password: **12345**

Platform 0: Depends how many Extender 1-4 cards are installed inside NTS-5000, the submenu will looks like:

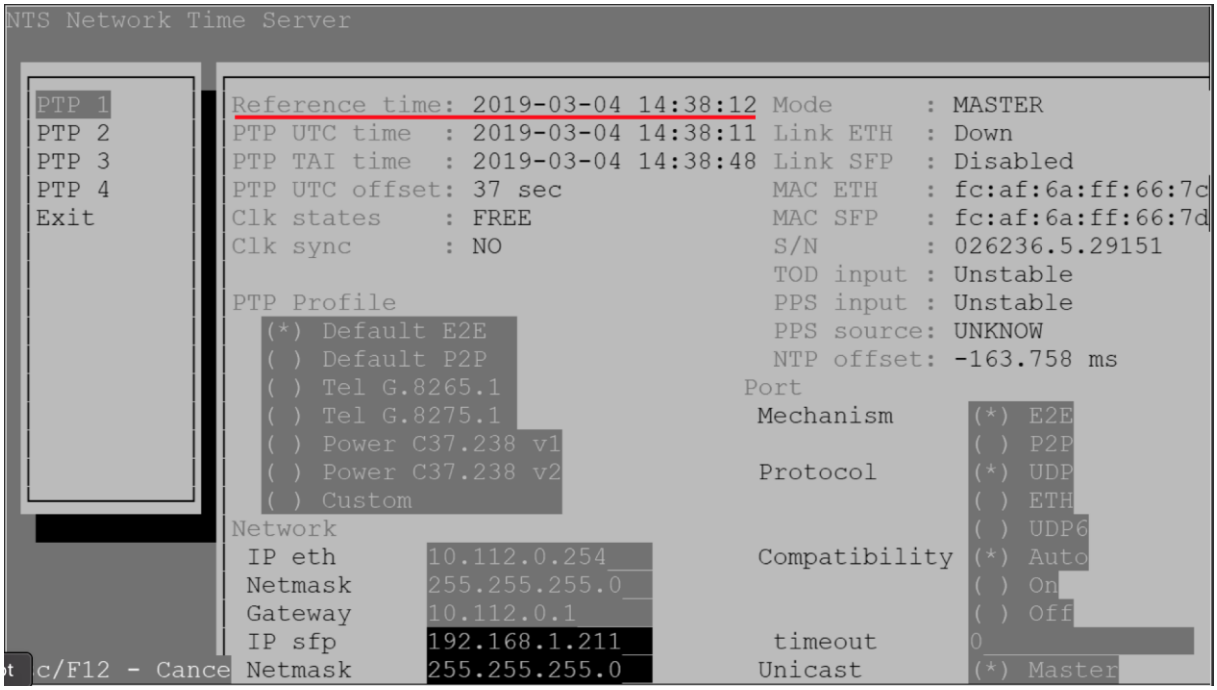


View of PTP Expander card configuration. This card operates autonomously:

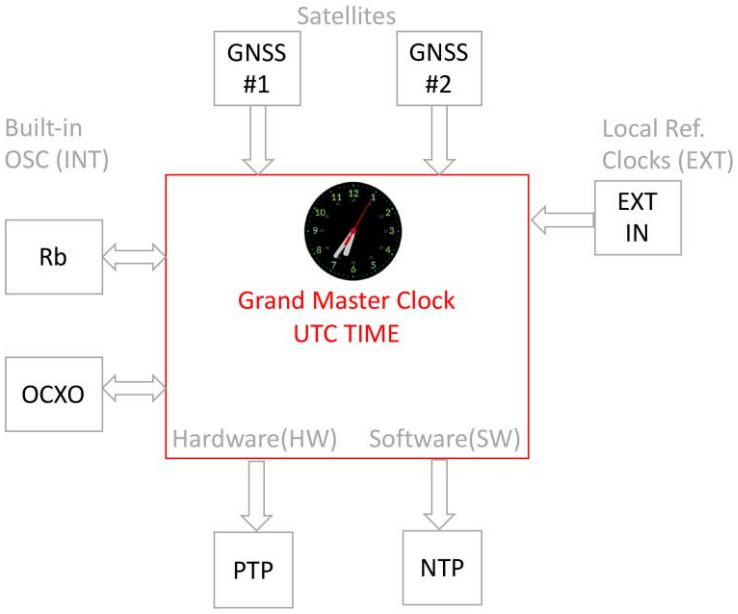


The meaning of parameters is:

Reference time

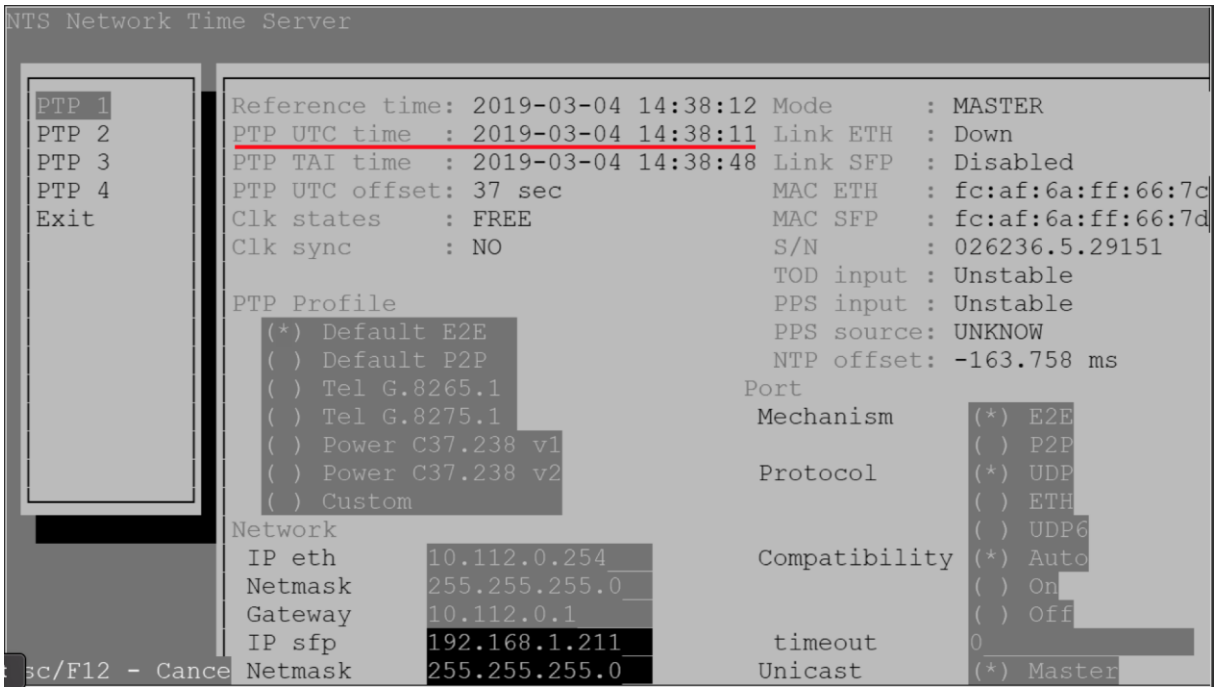


The Reference Time is a Grand Master Clock main time and the time domain reference of NTS-5000 time server. Usually, the reference time is a UTC, but can be also set to other scales including TAI too. Mostly the Reference Time is drawn from GNSS receiver (max. 2), but it can also be drawn from external atomic clocks. The reference time is also used to synchronize internal holdover oscillators (Rubidium and OCXO). Reference time is redistributed internally to all server outputs including network interfaces (PTP/NTP protocols), hardware IRIG-B output, SYSPLEX output, PPS-out, 10MHz-out etc.

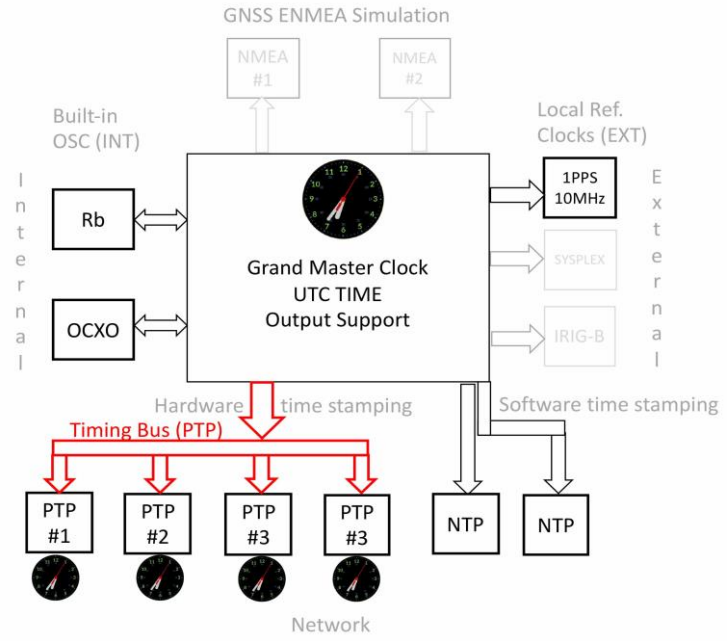


The Reference Time is a main input time used to ensure time domain operation of NTS-5000.

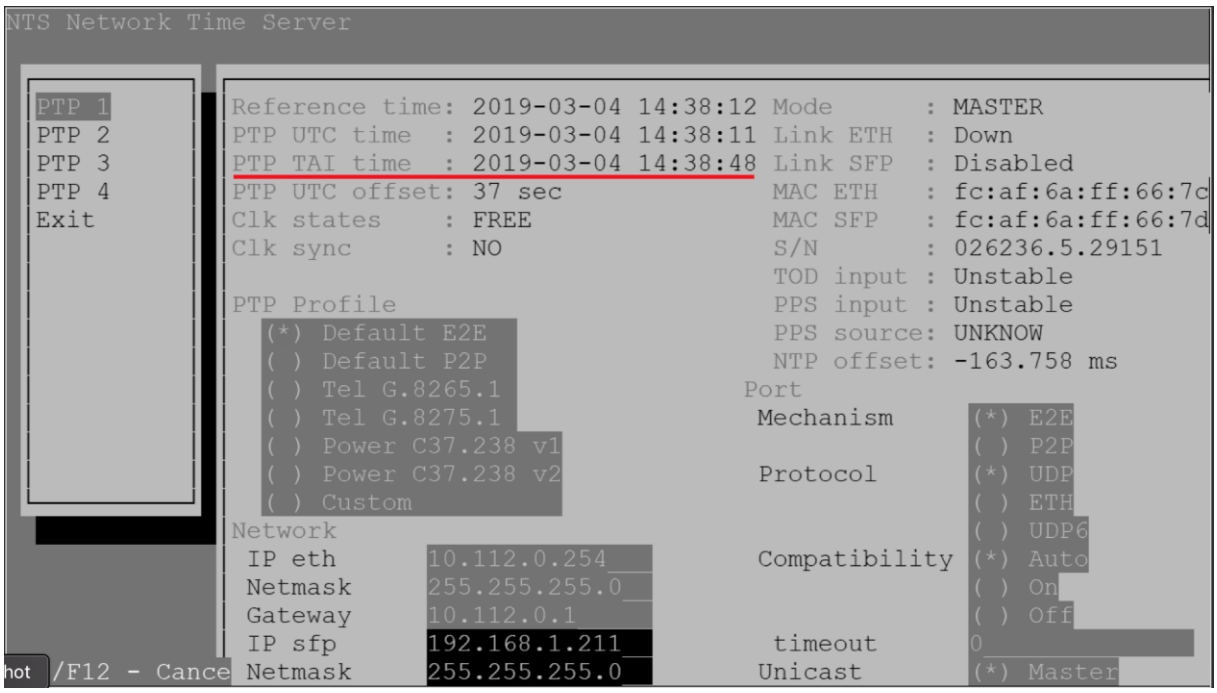
PTP UTC Time



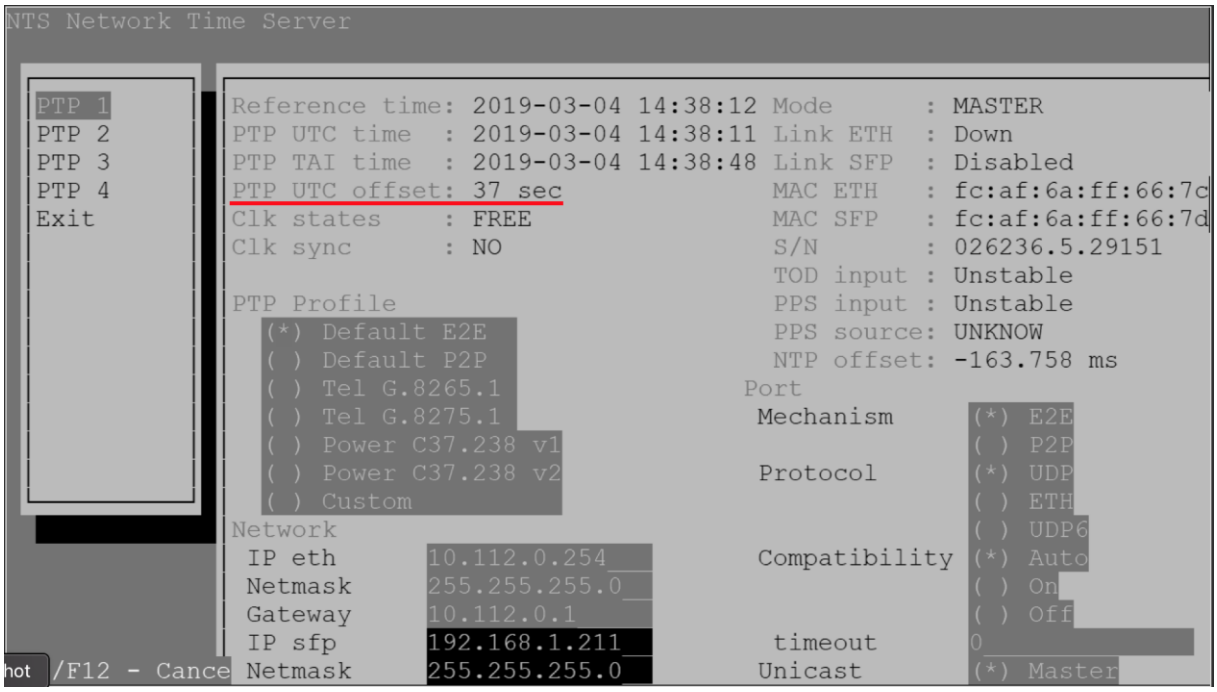
This is **PTP UTC time** is general information purpose time information. It is basis on software measurement done at input of Expander PTP BUS internal input. It is the same time as Reference Time sent, but on another side of the bus – at arrive to PTP module hardware. A little observed offset to Reference Time is related to software way of measurement and has now impact on final accuracy of synchronization. This parameter has diagnostic purpose and it used to ensure there is pending internal synchronization.



PTP TAI time

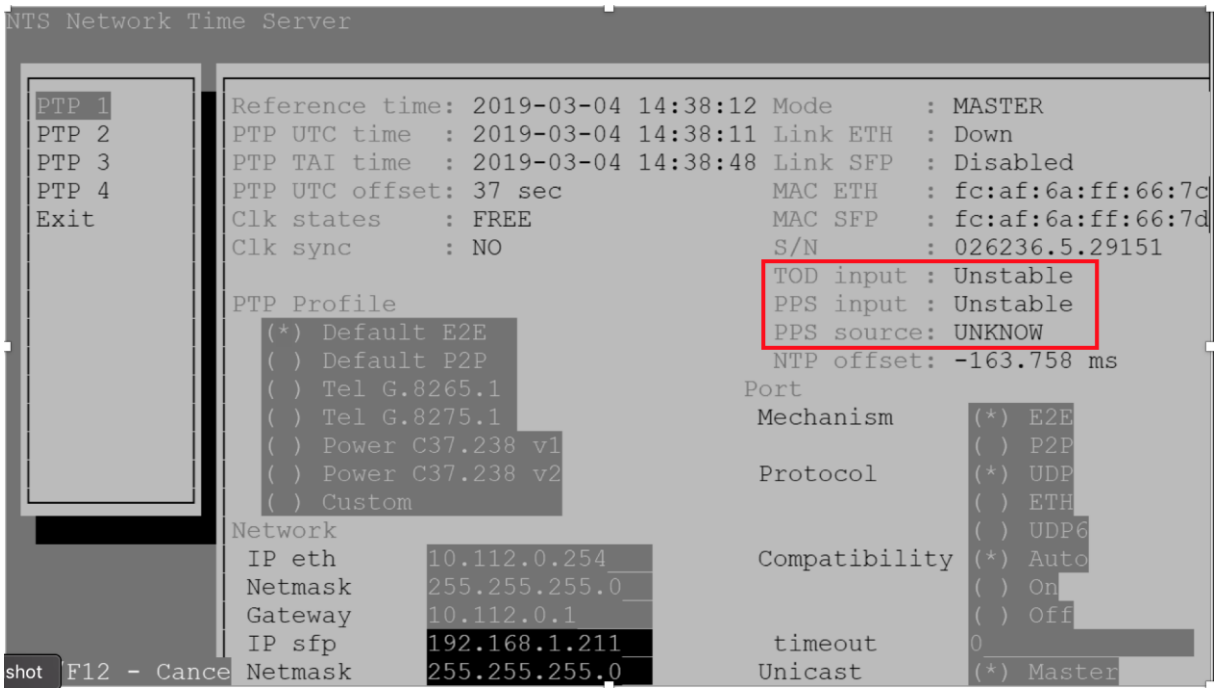


Is the same as ***PTP UTC time*** but recalculated to TAI – the Atomic Time Scale. Currently the TAI is 37 leap seconds ahead to UTC. The number of **#leap_seconds** is indicated next line.

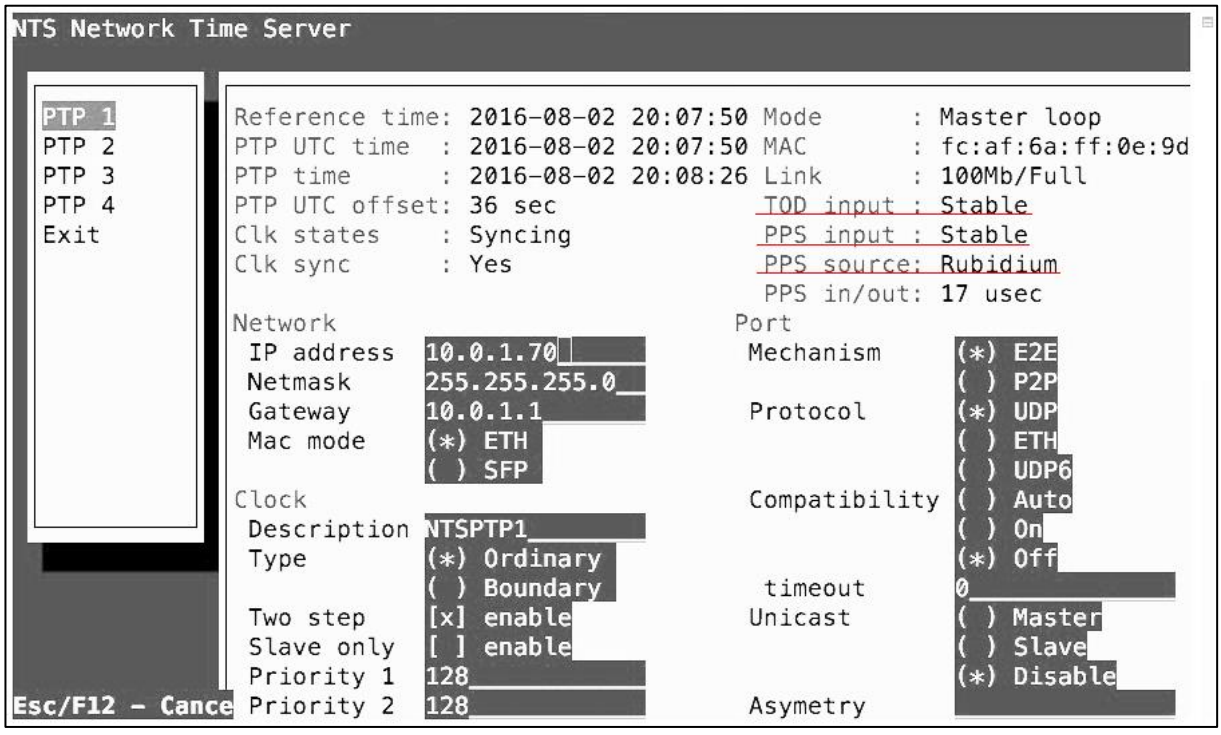


TOD input, PPS input, PPS source

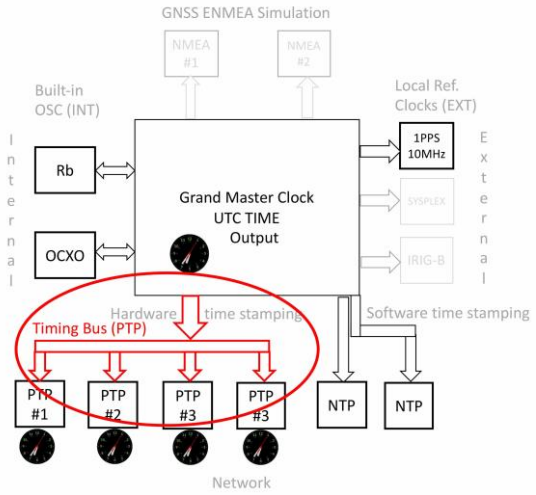
Directly afterNTS-5000 power ON the information looks following:



Once NTS-5000 server gets synchronized to *Reference time*, it starts to produce internal synchronization signals on Time Transfer Bus (TTB). These signals are input to Expander card. When Extender is internally synchronized to *Reference time* it shows information as presented below:



Notes on TTB (Time Transfer Bus) and signals as: TOD input, PPS input, PPS source



Internal Timing Bus redistributes UTC time from GMC to all 1-4 PTP autonomous op. modules

The ***Time Transfer Bus (TTB)*** supports following synchronization signals and dataflow:

- *1PPS (Pulse Per Second)* high accuracy frequency reference. Built-in 1:4 signal splitter share this single GMC reference to all 1-4 PTP modules.
- *ToD (Time of Day)* UTC phase data information. It tightly corresponds to 1PPS above data. It is sent via serial communication to all 1-4 PTP modules.
- *Extended info* package of data includes additional information from GMC incl. LEAP_SECOND and ERROR BUDGET.

Unless additional factors are taken in the account, in broad outline it can be assumed rightness that ***Reference Time*** is equal ***PTP UTC Time.*** Considered factors are:

a) Latency if I/O at GMC module output and PTP module input
b) Latency of time transfer at TB (Internal Time Transfer Bus between GMC and PTP module)
c) Time scale computing algorithms TAI-UTC
d) Others minor factors

The NTS-5000 unit arrives factory pre-calibrated. However, because of aging of electronic elements some differences can be observed in the future. This might require recalibration. Furthermore, NTS-5000 provides self-audit monitoring. It gives additional information about stability of internal synchronization signals (PPS, ToD) at the time they arrive from TTB to PTP Extender card.

Those parameters are:

ToD input: *<value>*
PPS input: *<value>*

Where value are:

- ***Stable*** *- when TTB signals are examined by PTP module to be stable*
- ***Unstable*** *- when TTB signals are examined by PTP module to be unstable*
  The PTP modules switches then to local holdover (HO) mode TCXO driven
- ***Unknown*** *- when PTP cannot examine the quality of TTB input signals to be stable/unstable*

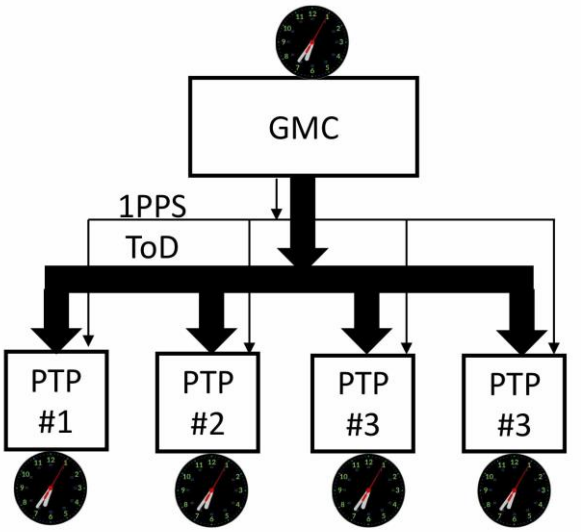
There are several possible scenarios of action when other than ***Stable*** status is reach. This manual is not providing details on such algorithms. Nevertheless, the *USER* should assume NTS-5000 unit is trying to resolve the problem automatically at grandmaster level (GMC – Grand Master Clock time management level).

The ***PPS source*** values can be:

- ***Rubidium*** *(GMC level)*
- ***OCXO*** *(GMC level)*
- ***PPSa*** *(GNSS #1)*
- ***PPSb*** *(GNSS #2)*
- ***EXT*** *(1PPS-in EXT)*
- ***SYS*** *(SYSPLEX)*
- ***IRIG*** (IRIG-B IN)

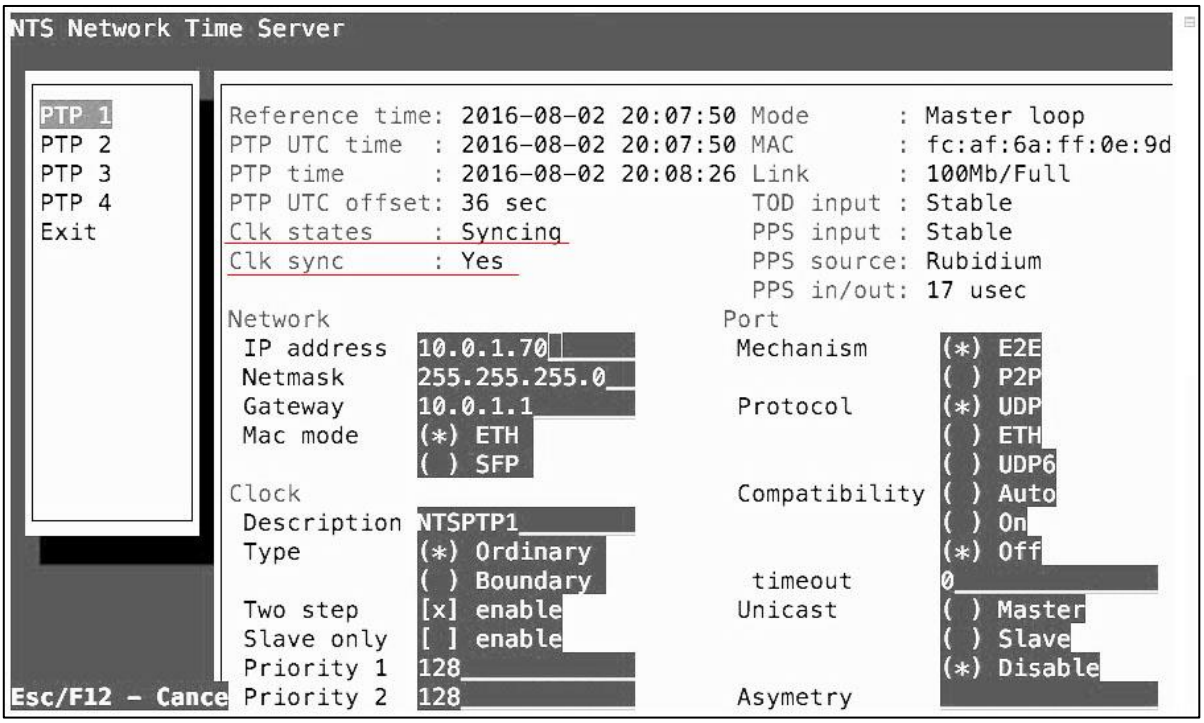
Note! After both internal oscillators (Rubidium and OCXO) are synchronized to GNSS, the NTS-5000 users mostly observe status of PPS source:

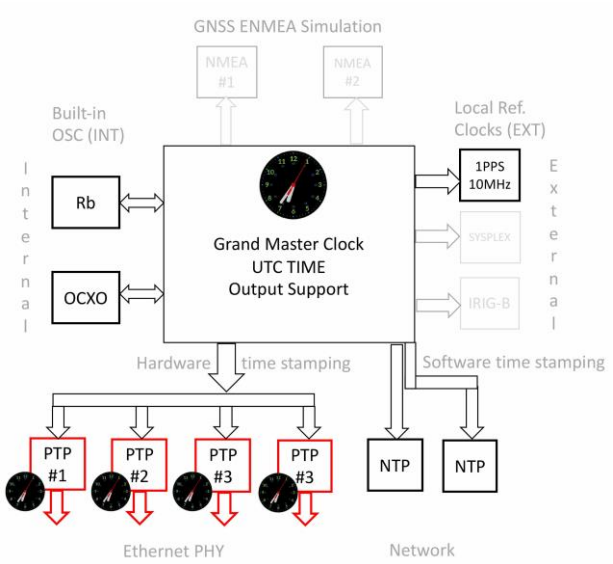
- **PPS source: Rubidium**
- **PPS source: OCXO**



Time Synchronization Bus GMC-PTP(1-4)

Before Rubidium/OCXO are synchronized, other values like PPSa (GNSS#1) or PPSb (GNSS#2) can be observed in PPS source too.





1-4 PTPv2/IEEE1588:2008 autonomous operating modules- each with own local TCXO oscillator and clock (Master Clock – MCLK)

PTPv2/IEEE1588:2008 output generation:

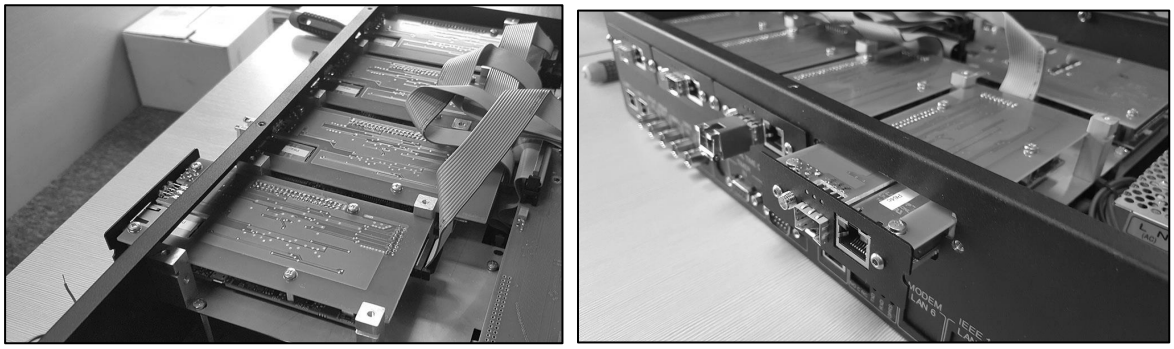
Each of 1-4 PTP modules is prepared for autonomous operation IEEE1588:2008 standard generation to Eth (SFP or RJ45).

Before modules are operationally ready they local clocks needs to be synchronized first. Each module includes at least TCXO oscillator for sub-local holdover operation (independently on Rubidium/OCXO at GMC level). Each Expander module includes autonomous operating functionality to act a Master Clock.

The synchronization process of 1-4 PTP modules can be traced via variables:

Clk sates: Syncing
Clk sync : Yes

Assuming the ***PPS/ToD input*** signals (sent via TTB) are ***stable***, the PTP modules are beginning their local Master Cock (MCLK) synchronization. Each of max. clocks are synchronized separately to let PTP modules operate autonomous and independent on each other. Each 1-4 module includes own operating system with own IP and PTP stack (IPv4/IPv6). The PTP modules separation is essential for cyber-security.



PTP1-PTP4 hardware MCLK (Master Clock PTP) modules in NTS-5000. Each with HW low-level time stamping

Clk states variable provides information of local MCLK (Master Clock) synchronization process of PTP module.

Clk states: <*status*>
status:

Syncing	– when MC is synchronizing to GMC
HOLDOVER	– when MC is operating from local TCXO
FREE	– when MC is operating FREE RUN mode TCXO (MC reminds unsynchronized, e.g. after internal RESET)
unknown	– shortly after reset of module, or if module is not responding
Syntonizing	- when MC intervals are syntonizing to ref. interval definition

In addition, the ***Clk sync*** information is provided and it can be neither **Yes** – if MC is synchronized to GMC, or **No** – if not synchronized. Together, with Clk states it provides full information on PTP module operating autonomous. The synchronized and stable operationally unit mostly displays:

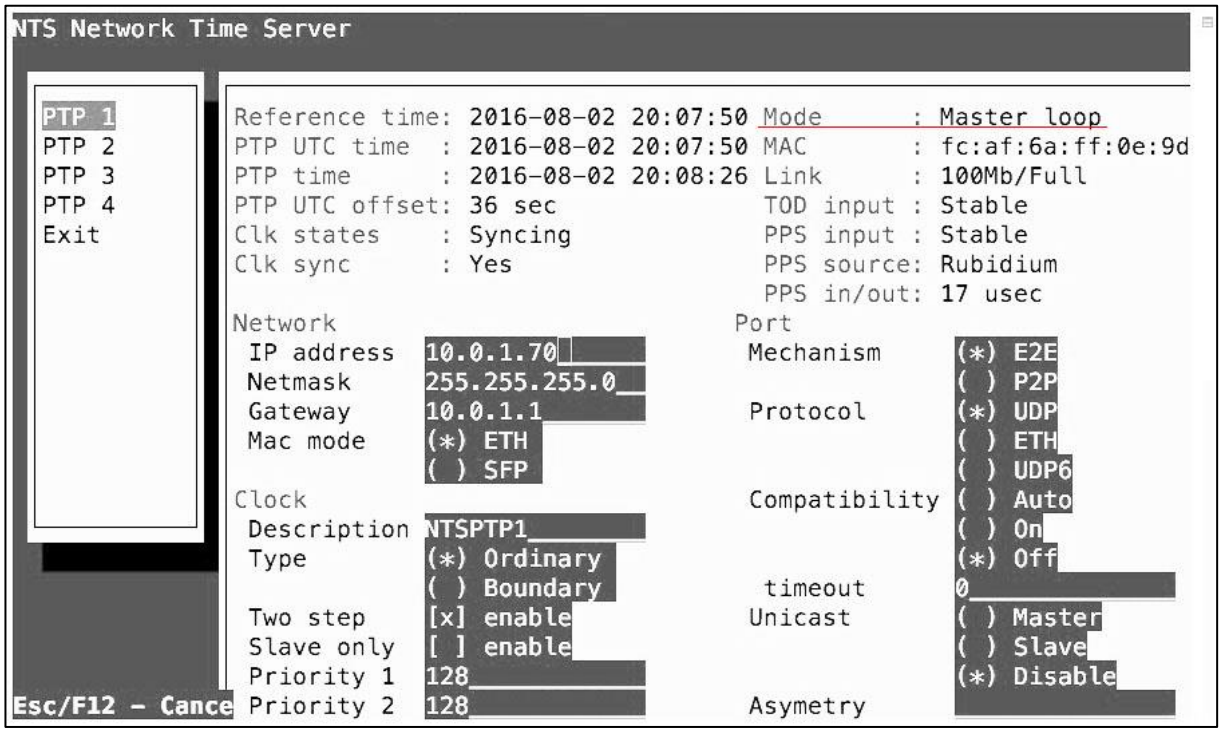
Clk states : Syncing
Clk sync : Yes

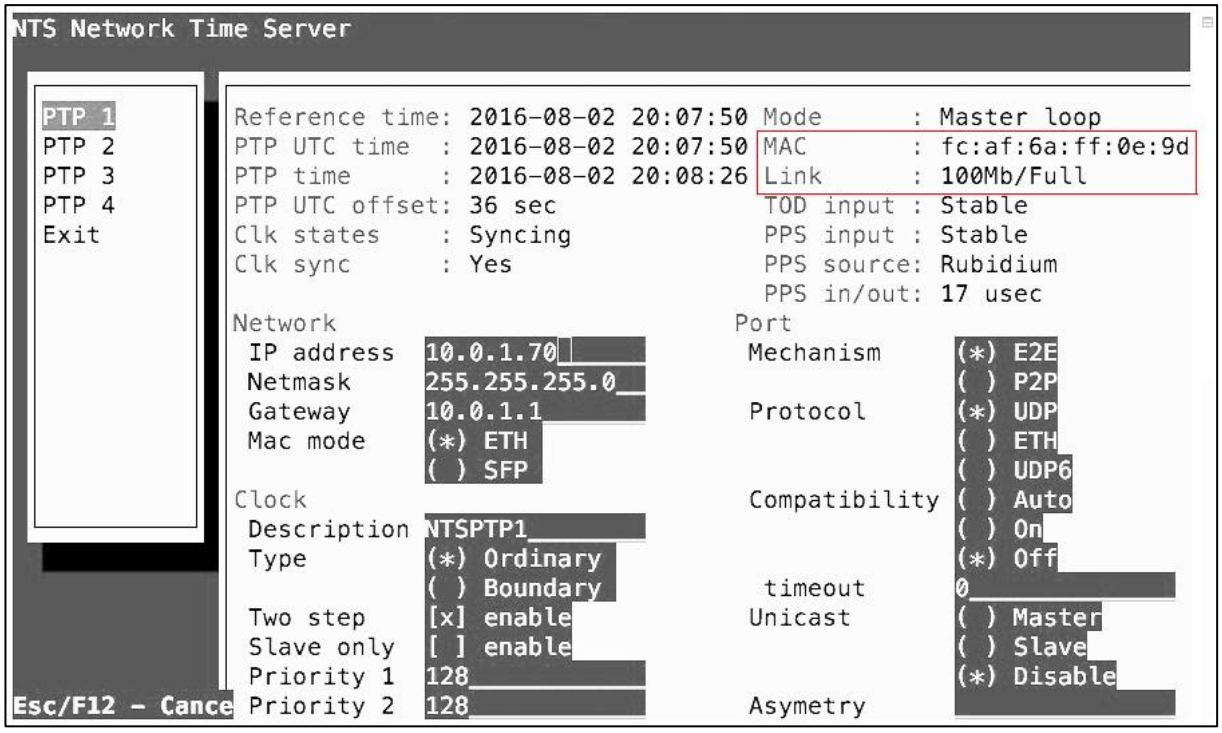
where, MC is synchronized to GMC (TTB signals are stable) but it is consciously synchronizing to keep best synchronization accuracy and MC performance. In case of getting PPS or ToD input Unstable, the ***Clk states*** transfers to ***HOLDOVER*** (assuming the ***Clk sync*** was previously ***Yes***). Similar situation after module (or unit) reset might conclude with data outputs ***Clk states*** : ***FREE*** or earlier directly after reset ***Clk states*** : ***unknown*** (assuming the ***Clk sync*** is ***No***). In addition, the ***Mode*** value parameters can be traced for screen for maintenance tracing:

mode: *<value>*

value:

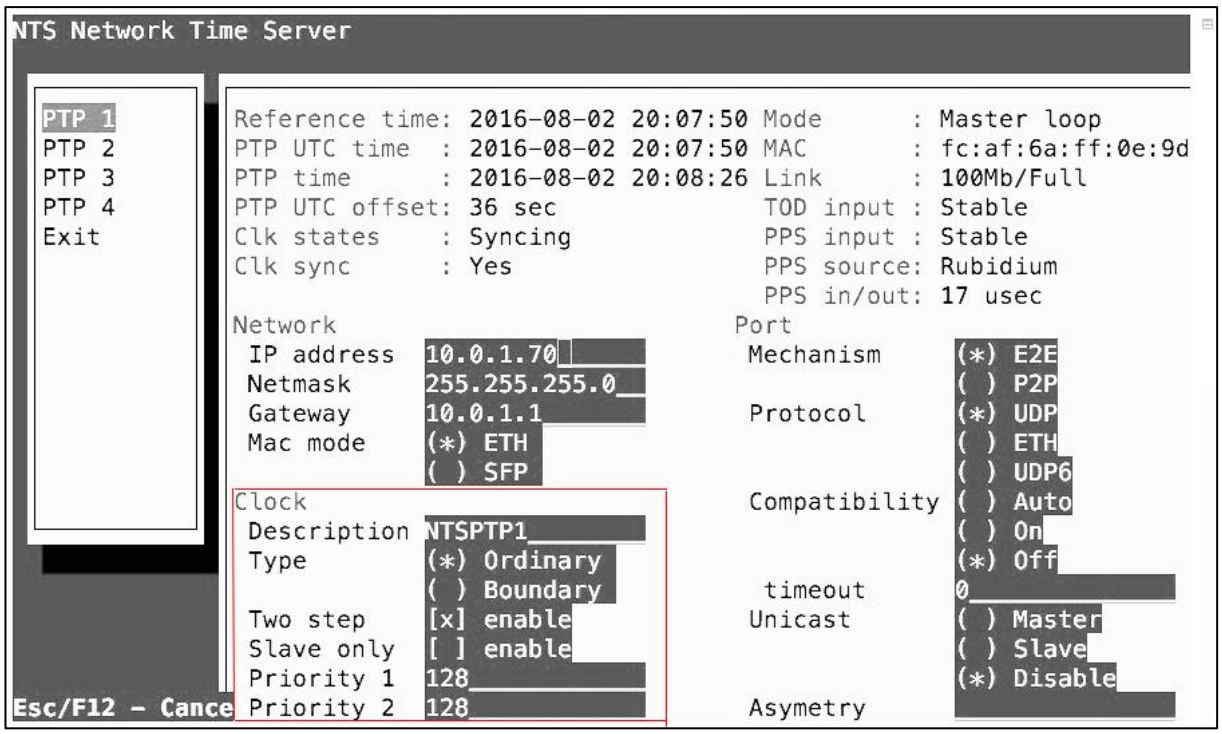
Master (loop) – MC is operating (communication is OK), PTP produces ETH output
Close – communication PTP module INPUT is close (NO communication)
Connecting – GMC is trying to lunch connection to PTP module INPUT
Read config – GMC is reading PTP module configuration (communication OK)
Configuration – PTP module configuration is pending
Init – initializing PTP Expander module
Booting – PTP Expander module is booting (restarting)
Cli wait – PTP module is waiting for command sent by GMC (Grand Master Clk)



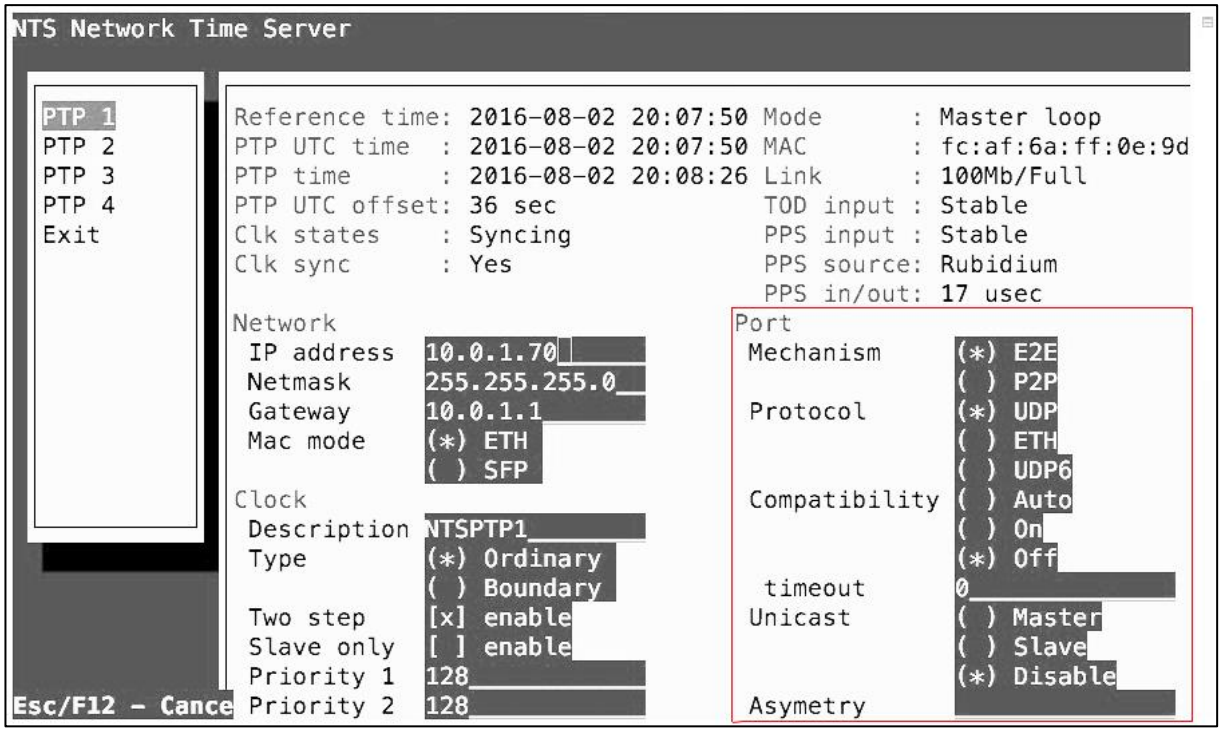


Each PTP card provides NIC parameters including MAC and type of Ethernet connection (1GE, 100/10 Mbps).

(1) PTP



Above (red colour) marked block defines PTP Clock parameters described in Precision Time Protocol standardization IEEE1588:2008 document. This specification is well done, so there are no reasons to repeat it in this manual. For the std. server operation PTP always claim to work ***Ordinary***. In some specific cases PTP card can be configured ***Boundary***. The Boundary mode can be selected when clock is synchronization via PTP/Ethernet and it provides synchronization to PTP/Ethernet. In such mode the ***Slave only*** option should be selected too. We recommend to keep default ***Two step <enable>*** and ***128 Priority*** *default set to 128 since those are most std. PTP figures to keep compatibility close.*

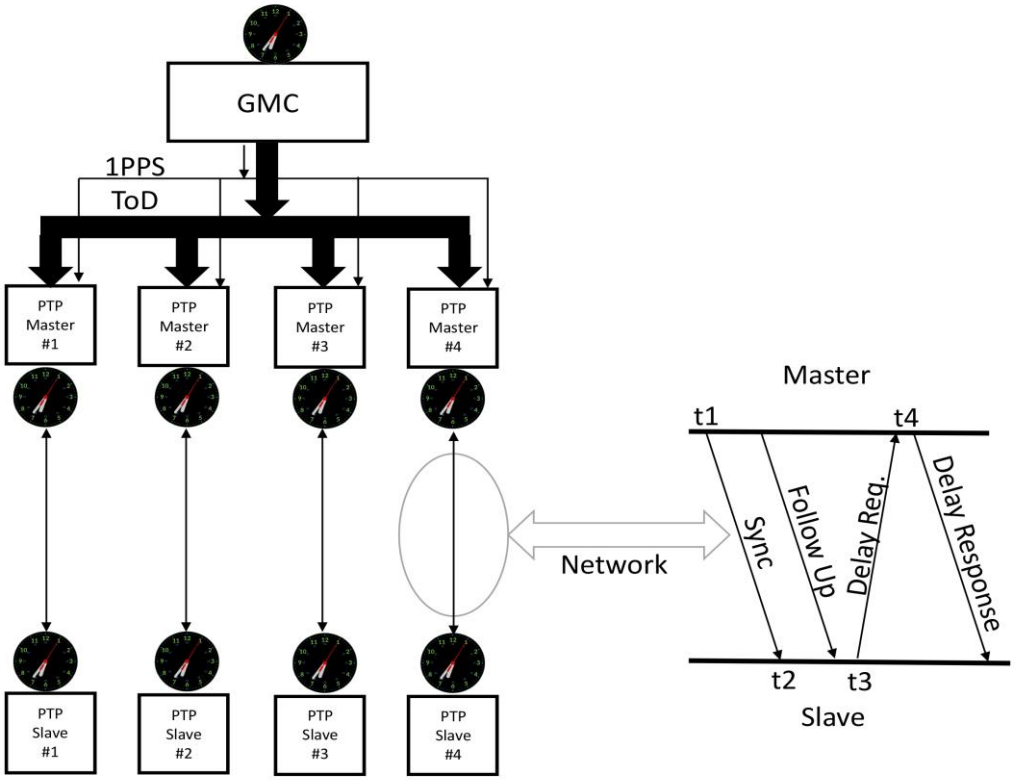


There are two PTP delay measurement ***Mechanisms***:

End-To-End (E2E - default)
Peer-To-Peer (P2P)

The ***Peer-To-Peer*** (P2P) delay measurement mechanism is best in IT engineered network, where all switches can be guaranteed to be IEEE1588:2008 capable (either transparent clocks or boundary clocks). If there are going to be any non-PTPv2/IEEE1588 aware switches, or if there is any doubt about this, then please use ***End-To-End*** (E2E) delay measurement mechanism. This is why E2E is also the default mechanism at NTS-5000.

The Precision Time Protocol (PTPv2/IEEE1588:2008) works by exchanging messages between master clocks and slave clock.



E2E mechanism

Above (right side) sequence diagram is showing the exchange of messages between a PTP master clock and a PTP save clock. For NTS-5000 this process is independent for each of max. 4 PTP masters. The departure and arrival times of the ***Sync*** and ***Delay Request*** messages are saved as the four timestamps ***t1-t4***. The ***Follow Up*** and ***Delay Response*** messages are used to transport the timestamps recorded at the MCLK to the SCLK. Such information is used to adjust slave clock time on the end of these exchanges when SCLK has all four t1-t4 timestamps. It can than calculate the offset of it's own clock with respect to the master using following delay averaging formula:

$$\text{Offset} = (t2 + t3 - t1 - t4) / 2$$

The equation assumes that the time it takes for messages to go from the MCLK to SCLK, the forward delay, is the same as the time it takes for messages to go from the slave to the master, the reverse delay. There is no problem if these delays are large, just so long as they are the same. Any difference in the forward and reverse delay results in an error in determining the difference between the master clock and the slave clock.

Why would the forward and reverse delays be different? It's mainly due to all of kind of pesky queues. There are queues in the routers, there are queues in the switches, there are even queues in the network stacks at the end devices. Usually messages spend minimal time in the queues, but sometimes they are waiting for a switch to finish up with other messages on the same port, or for an operating system to complete what it was doing so it can fetch a timestamp. In some cases, the delay can be quite long (to long), many microseconds, or even milliseconds. So obviously if this happens in the one direction, but not the other providing to a big time transfer error.

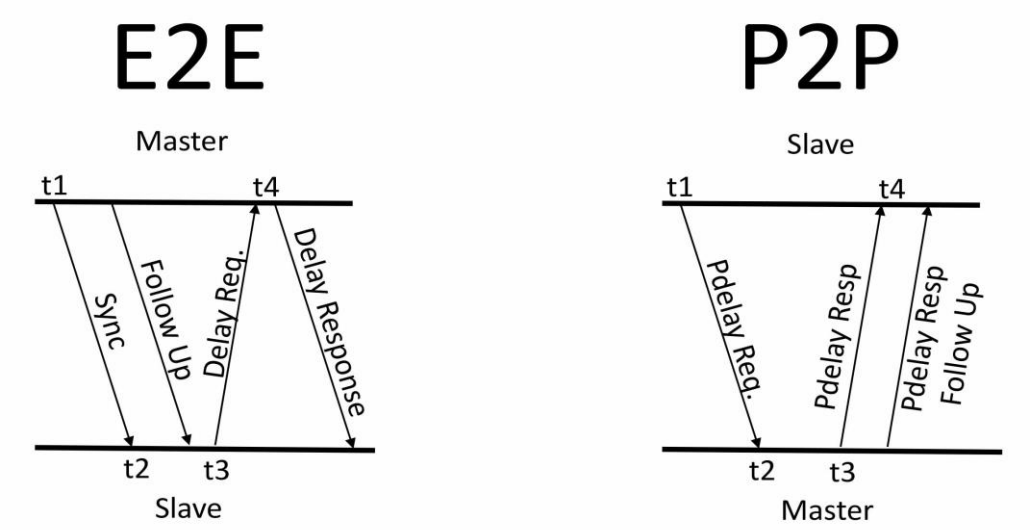
Basically this is all solved with hardware timestamping when messages depart from or arrive at a network port, special hardware generates a timestamp from the local clock, usually in the media independent interface between the data link layer (MAC) and the physical layer (PHY). That removes the unpredictably slow response of the operating system (OS) and other software (APP, DEV-driver etc). Switches and routers which are PTP aware also timestamp PTP messages. One type of such devices, is called a transparent clock works by updating PTP messages to correct for time spent in the device. Another type, called a boundary clock uses the PTP messages to set its own clock, then sends its time to PTP slaves which need it. This delay measurement mechanism is known as the **End-to-**

End delay measurement mechanism. As it turns out PTP has an alternative delay measurement mechanism known as the **Peer-to-Peer** mechanism.

In **Peer-To-Peer** networks the master still sends Sync and Follow Up messages to the slave clock just as with the end-to-end delay measurement mechanism. With peer-to-peer the slave calculates its clock offset with respect to the master as follows:

$$slave\ time = master\ time + network\ delay$$

No need to combine four timestamps like we did with **End-To-End** networks. But how did the slave know the network delay? That is the **Peer-To-Peer** delay measurement. Instead of sending delay measurement messages from the slave to the master, as with the end-to-end approach, each device on the network exchanges peer-delay measurement messages. That way each device can keep track of the delays between itself and its immediately connected neighbors. Each device periodically initiates an exchange of peer-delay messages on every connected port. Then each device removes the peer-delay from Sync messages when it enters the device, by updating the correction field in either the *Sync* or *Follow Up* message. If it is a switch, it doesn't include the peer-delay in the outgoing cable, even though it also knows that. The next device in the chain will do that correction, and we don't want to double count. The sequence of peer-delay compared to E2E looks:



If in P2P model the SCLK wants to know the delay to MCLK, it sends a ***Pdelay Req*** messages, short for peer-delay request. SCLK also saves the time it sent in t1 message. MCLK saves the time of its clock, when t2 message arrives. Then the MCLK sends a ***PDelay Resp*** message, short for peer-delay response, and a ***Pdelay Resp Follow Up***. The ***Follow Up*** message contains the departure time for the ***Pdelay Resp***, t3. SCLK also saves the arrival time of the ***Pdelay Resp***, t4, so it has all of four timestamps and can calculate the delay between the clocks. Here, as with the end-to-end mechanism, the assumption is made that the time it takes for the peer-delay messages to get from one clock to the other is the same in each direction. In the peer-to-peer case we only making that assumption over a cable, not the whole network, and there are no queues. So unless the cable is very long, that is a good assumption.

What about the queues in the switches? At the beginning of this post I said that peer-to-peer only works well when every switch is either a transparent clock or a boundary clock. That way the switch will take care of its own queuing delays. Another reason that we don't use peer-delay with ordinary switches is that the switches don't know what to do with peer-delay messages, and will not respond to them.

Although the end-to-end mechanism is more versatile, because it can handle ordinary switches and routers, the peer-to-peer mechanism has several advantages in networks where it does work:

- All links are periodically measured, so delay between the master and slave are already known when the network path changes. Note that peer-delay messages are exchanged even on ports blocked to prevent loops, such as by the Rapid Spanning Tree Protocol.

- There is no chance of Sync and Delay_Request messages taking different paths, since there are no Delay_Request messages.
- There is no need to worry about the master clocks ability to respond to Delay_Request messages when there are a lot of slaves, it only has to send the Sync and Follow_Up.

39. NTP symmetric authentication (MD5)

Network Time Protocol (NTP) supports authentication method using symmetric keys (MD5). This functionality is not available for Precision Time Protocol (PTP).

If a packet is sent while using this authentication mode, every packet is provided with a 32-bit key ID and a cryptographic 64/128 bit checksum of the packet. This checksum is built with MD5. With that algorithm the receiving NTP clients validate the checksum. Only NTP client and NTP server using the same pares of MD5 keys will successfully exchange synchronization data and therefore both parties need to have the same crypto key with the same key ID.

The key file *etc/ntp.keys*

The user must add the key number and the key value to a key file. The file can have any name and be located in any directory, but is usually named *ntp.keys* and is usually located in the same directory as the NTP software and *ntp.conf* configuration file. The *ntp.keys* file includes in each line:

KeyID EncryptionFormat KeySequence #Remarks

The first column holds the key ID (digit in range 0-65000). The second column defines the FORMAT. The third column is the MD5 (or DES) key. Supported encryption formats are:

FORMAT "**M**" - MD5 key with up to 31 ASCII characters
/Timeservers NTS-3000, 4000, 5000 only supports M format/

FORMAT "**A**" - DES key with up to eight 7-bit ASCII characters
/each character is standing for a key octet. This is used by Unix passwords, too./

FORMAT "**S**" -DES key written in hexadecimal notation,
/where the lowest bit LSB of each octet is used as the odd parity bit/

FORMAT "**N**" – DES hexadecimal string,
/NTP standard format is using the highest bit (HSB) of each octet used as the odd parity bit/

Useful remarks:

- Please be aware of the following restrictions of not using "#", TAB, Newline, and NULL as ASCII key.
- The *keyID* 0 is reserved for special purposes and should not appear too.
- The key value must be entered in upper and lower case on both sides (server/client).
- For initial testing purpose please locate *ntp.keys* file in same directory as *ntp.conf* file is.
- For final production keys file should be owned by root and should not be readable by normal users

The *ntp.keys* text ASCII file may look like this:

```
10      N       29233E0461ECD6AE   # des key in NTP format
20      M       RIrop8KPPvQvYotM   # md5 key as an ASCII random string
14      M       sundial            # md5 key as an ASCII string
15      A       sundial            # des key as an ASCII string
12345   M       BlahBlahBlah       # key can be any ASCII string and any unique KeyID
```

Following keys are identical:

```
101     A       SeCReT             # this is ASCII (DES) text
101     N       d3e54352e5548080    # this is HEX  (DES) string HSB notation
101     S       a7cb86a4cba80101    # this is HEX  (DES) string LSB notation
```

In the authentication mode a party is marked “untrusted” (not suitable for synchronization), whenever unauthorized packets (or authorized packets with a wrong key) are used. Please note that a server may recognize a lot of keys but use only a few of them. This allows a time-server to serve a time-client, who is demanding authenticated time-information, without trusting. Additional parameters are used to specify the key IDs for validating the authentic of each partner.

Configuring the client NTPD daemon for MD5 authentication

In order to use authentication, the following commands must be added to the *ntp.conf* configuration file. These changes should be made after the key has been added to the key file as described above. The symbol “#” introduces a comment (remark), which continues for the remainder of the line. The NTP daemon process must be restarted after the file has been edited.

The configuration file *ntp.conf* of a server using this authentication mode may look like this:

```
server 10.0.0.210  key 10
server 192.168.0.210 key 10
keys   <path>/etc/ntp.keys                 # UNIX family OS
keys “<path>\etc\ntp.keys”                 #  MS-WINDOWS
trustedkey 10 15
requestkey 15          # key (mode 6) for accessing server variables
controlkey 15          # key (mode 7) for accessing server variables
```

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

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

It is helpful to monitor the performance of the NTP daemon to confirm that the authentication algorithm is working as expected. The NTP daemon provides a number of monitoring tools that can be used for this purpose. For example, the peerstats command will provide information on the status of the connections to the servers that are being used to synchronize the system time. To enable this report, the following commands would be added to the NTP configuration *ntp.conf* file:

```
#
enable auth
enable monitor
enable stats
#
# turn on reporting of the peer statistics
#
statistics peerstats
#
#  the file for the report will be named peerstats with
#  the date appended. The full name of the file # will be peerstats.yyyymmdd.
#  a new file will be created every day at 0 hours UTC.
#
filegen peerstats file peerstats type day
#
# the following command specifies the full name of
# the directory where the files will be located
#
statsdir /local/bin/
```

Testing the keys

1. Any given key can be tested using the utility program *ntpdate* in debug mode (-d options). Running in debug mode will print intermediate results on screen and do not adjust the clock (-a option). The integer specifies the key number (–k option). The xxx.xxx.xxx.xxx is the IP of NTP server. The command is:

ntpdate -d -a 12345 -k /local/bin/ntp.keys xxx.xxx.xxx.xxx

The NTP server replay should include confirmation sequence:

authentication passed transmit(xxx.xxx.xxx.xxx) receive(xxx.xxx.xxx.xxx)

If the key number or key value is not correct then the message *"authentication passed"* will be replaced with *"authentication failed."* If the response shows transmit messages with no corresponding *receive* responses then either the IP address is wrong, *keyID* mismatch or a firewall or network router is blocking the connection to the timeserver. The ntpdate always require root (admin) rights.

2. Starting from NTP version 4.2.8 there is *ntpq* new command authinfo available for testing and statistic. Please type "?" at *ntpq* prompt command level to see all commands. The *ntpq* can be also executed from shell level. The command is:

ntpq –c authinfo

It returns statistic of authentication with following detailed data output:

time since reset:	21483
stored keys:	2
free keys:	15
key lookups:	2712
keys not found:	0
uncached keys:	1
expired keys:	0
encryptions:	1356
decryptions:	1356

Observing in time client "encryptions" and "decryptions" figures ensures that packages are exchanged encrypted. Both parameters should increase each pool interval, but not necessarily (depends on ntp.conf configuration and time server availability) both must point the same value.

3. It is helpful to monitor the performance of the NTP daemon to confirm that the authentication algorithm is working as expected. The NTP daemon provides a number of monitoring tools setup in ntp.conf :

#monitoring lines add to ntp.conf
enable monitor
enable stats
statistics peerstats
filegen peerstats file peerstats type day
statsdir /local/bin/

The daemon process will add an entry into the peerstats file each time the client queries a server. The entry will be in the following form:

54237 86332.222 132.163.4.107 f624 -0.011106682 0.000251015 0.000953898 0.000073756

The first two parameters give the time of the query as the MJD (Modified Julian Day number) and the UTC second of the day. The third parameter gives the IP address of the remote system. The fourth parameter describes the state of the query using the hexadecimal representation of a series of bits. The

significance of each bit is described in Appendix B of RFC1305. Using the convention that the most significant bit of the state is bit 0, the first hexadecimal digit of the state should be “f” to indicate that:

Bit 0: peer is configured
Bit 1: authentication is enabled
Bit 2: authentication is ok
Bit 3: peer is reachable

If authentication is not used, then bits 1 and 2 will be 0, and the first digit will be 9 instead of f. The “6” in the second digit signals that this server is being used to synchronize the local clock. If the client is querying more than one server, then the one that is selected to synchronize the clock will have a 6 as the second digit and the other status words will normally have a 4 in that position. The remaining parameters describe the offset, delay, dispersion, and jitter of the query.

ntp.conf/ntp.keys examples

Example configuration for testing NTP for Microsoft Windows 8.1 PRO

```
# file ntp.conf for Windows 8.1 NTP CLINET
driftfile "C:\Program Files (x86)\NTP\etc\ntp.drift"
enable auth
keys "C:\Program Files (x86)\NTP\etc\ntp.keys"
trustedkey 10101 12345 20 101
requestkey 15
controlkey 15
server 10.0.0.245 iburst minpoll 4 maxpoll 4 key 10101

### EOF ###
```

```
# file ntp.conf for Windows 8.1 NTP SERVER
driftfile "C:\Program Files (x86)\NTP\etc\ntp.drift"
enable auth
keys "C:\Program Files (x86)\NTP\etc\ntp.keys"
trustedkey 10101 12345 20 101
requestkey 15
controlkey 15
server 127.127.1.0  iburst minpoll 4 maxpoll 4
fudge  127.127.1.0  stratum 5 refid WIN8
### EOF ###
```

```
# file ntp.keys – the same file for both: SERVER & CIENT
10      M  ElpromaElectronica1
14      M  sundial
15      A  sundial
20      N  29233E0461ECD6AE        # des key in NTP format
30      M  RIrop8KPPvQvYotM        # md5 key as an ASCII random string
12345   M  BlahBlahBlah            # key can be any ASCII string and any unique KeyID
101     A  SeCReT                  # this is ASCII (DES) text
1010    N  d3e54352e5548080        # this is HEX   (DES) string HSB notation
10101   M  a7cb86a4cba80101        # this is HEX   (DES) string LSB notation
```

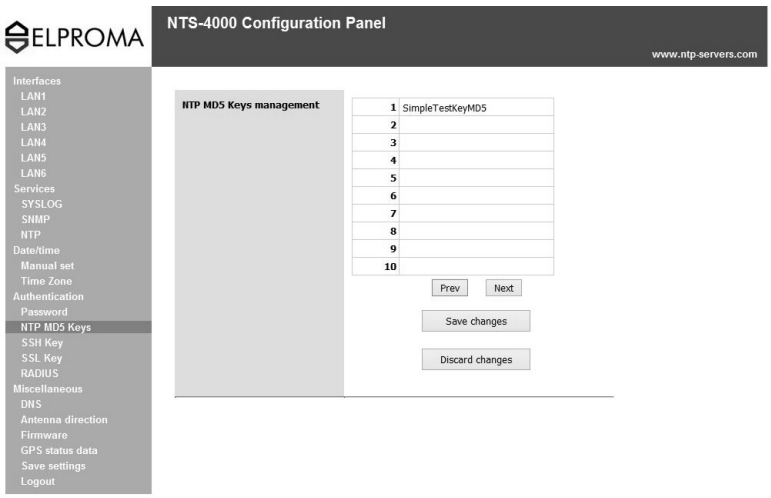
Configuring authentication at NTS-3000/4000/5000

NTS-3000/4000/5000 authentication can be lunch using std, server setup (HTTP, SSH, TELNET). Timeserver supports MD5 symmetric keys only. Please be sure to save updated configuration and

restart NTP client demon or service. It is also recommended to power down NTS-3000/4000/5000 and restart unit before using new defined MD5 symmetric keys.

MD5 Setup (WWW)

From left menu please select NTP MD5 Keys and write your MD5 ASCII keys to table. The 1-10 column represents KeyID. If you like to store large number KeyID please use Prev/Next buttons. Once your MD5 key configuration (servers ntp.keys) is ready, please save it pressing “Save changes” and wait until confirmation of storing will be displayed. Before using new defined MD5 keys please perform “Save settings” (and wait for success saving confirmation), and Logout. It is recommended to restart time server before using new keys.



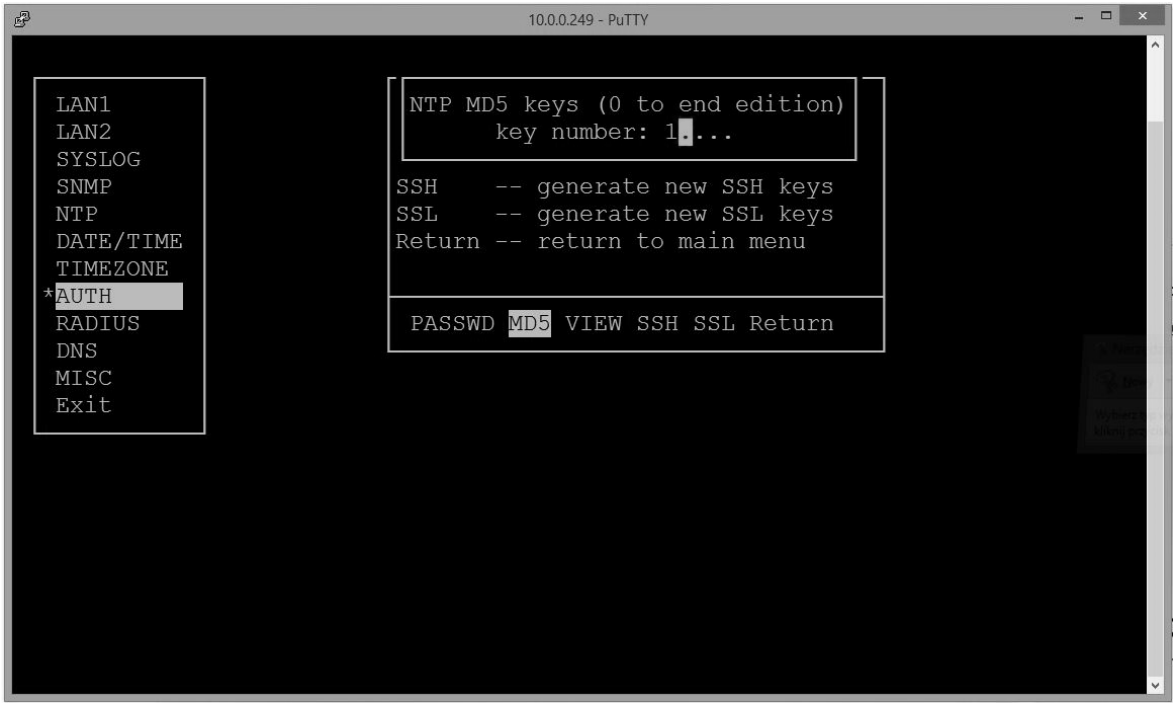
Configuring symmetric MD5 keys via HTTP (example use server IP 10.0.0.249)

Saved configuration creates automatically ntp.keys file inside NTS-3000/4000/5000. Please note keys you have defined for NTS and use them at *ntp.keys/ntp.conf* file of your client. Files may looks like:

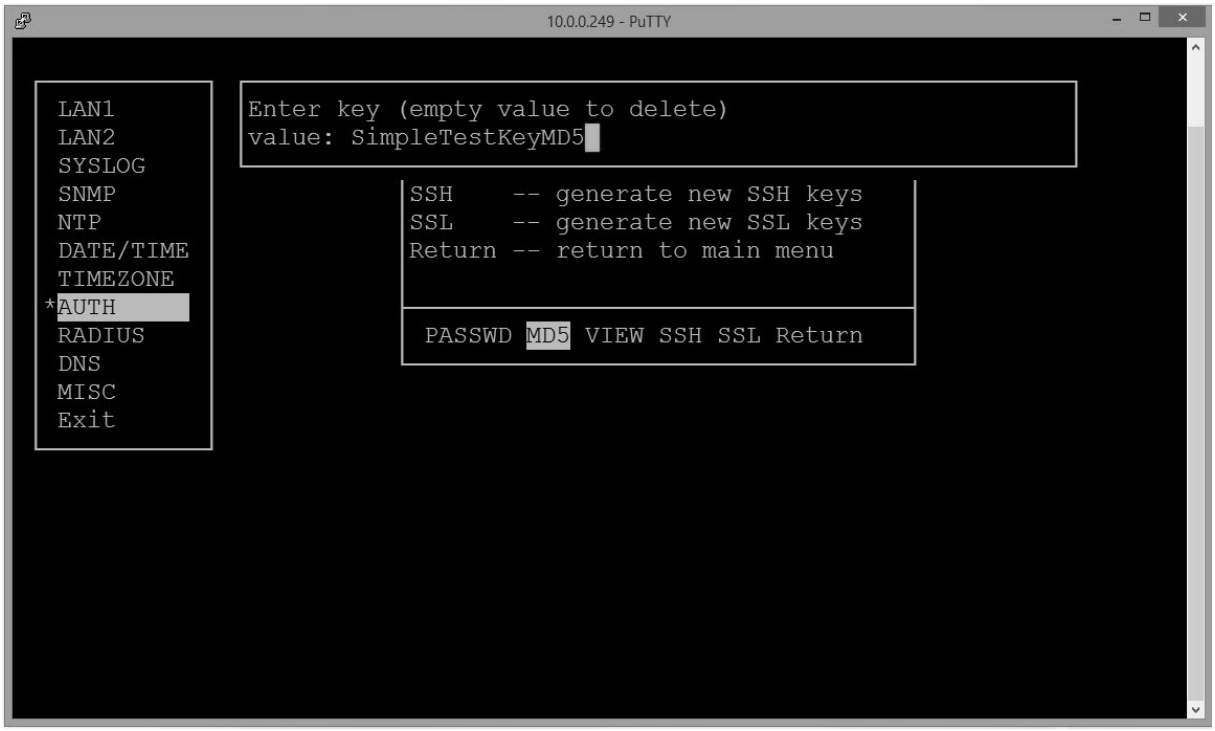
```
# ntp.conf file
enable auth
keys "C:\Program Files (x86)\NTP\etc\ntp.keys"
trustedkey 1 15 16
requestkey 16
controlkey 16
server 10.0.0.249  minpoll 4 maxpoll 4 key 1                    #KeyID=1 “SimpleTestKeyMD5”in use

# ntp.keys file
1      M  SimpleTestKeyMD5
15     M  ElpromaKey2
16     M  ClepsydraKey3
```

MD5 Setup (SSH/TELNET)

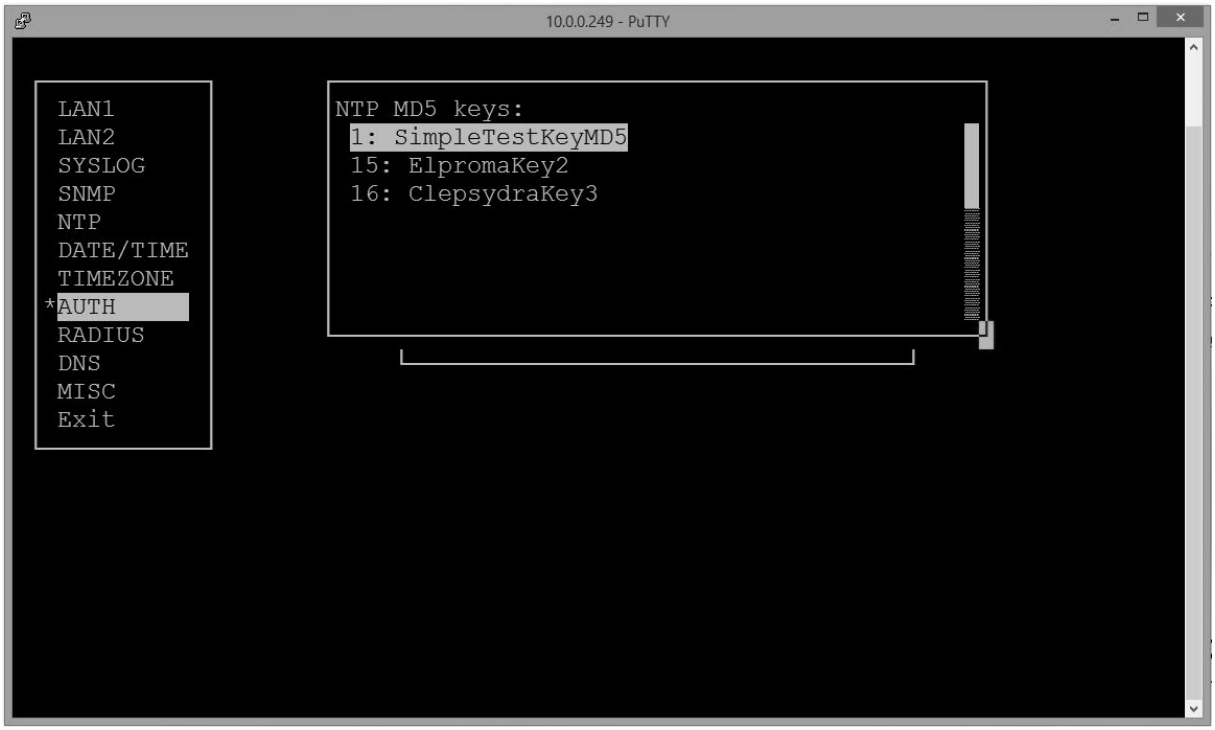
Below screenshots shows how to configure symmetric MD5 keys using text mode terminal services SSH and Telnet. For secured network environments, it is strongly recommended to use SSH service (not HTTP or Telnet).



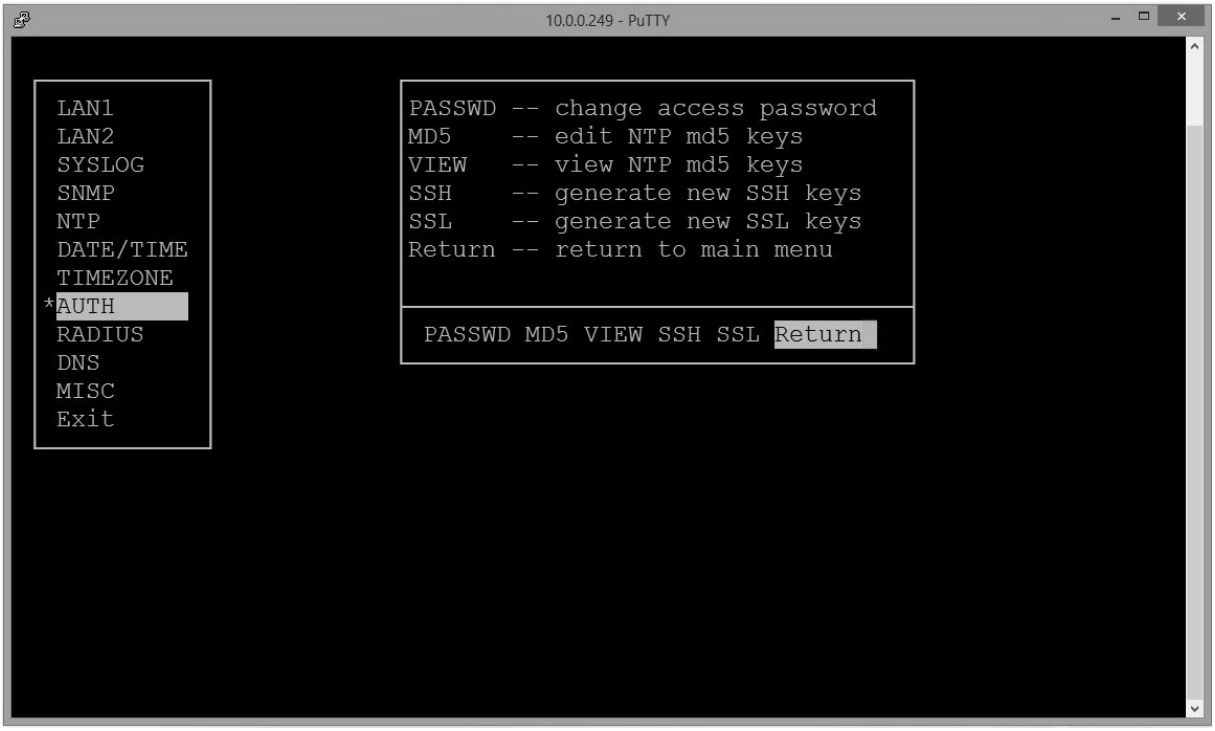
When defining new or existing MD5 key you will be requested for its KeyID (key number) first.



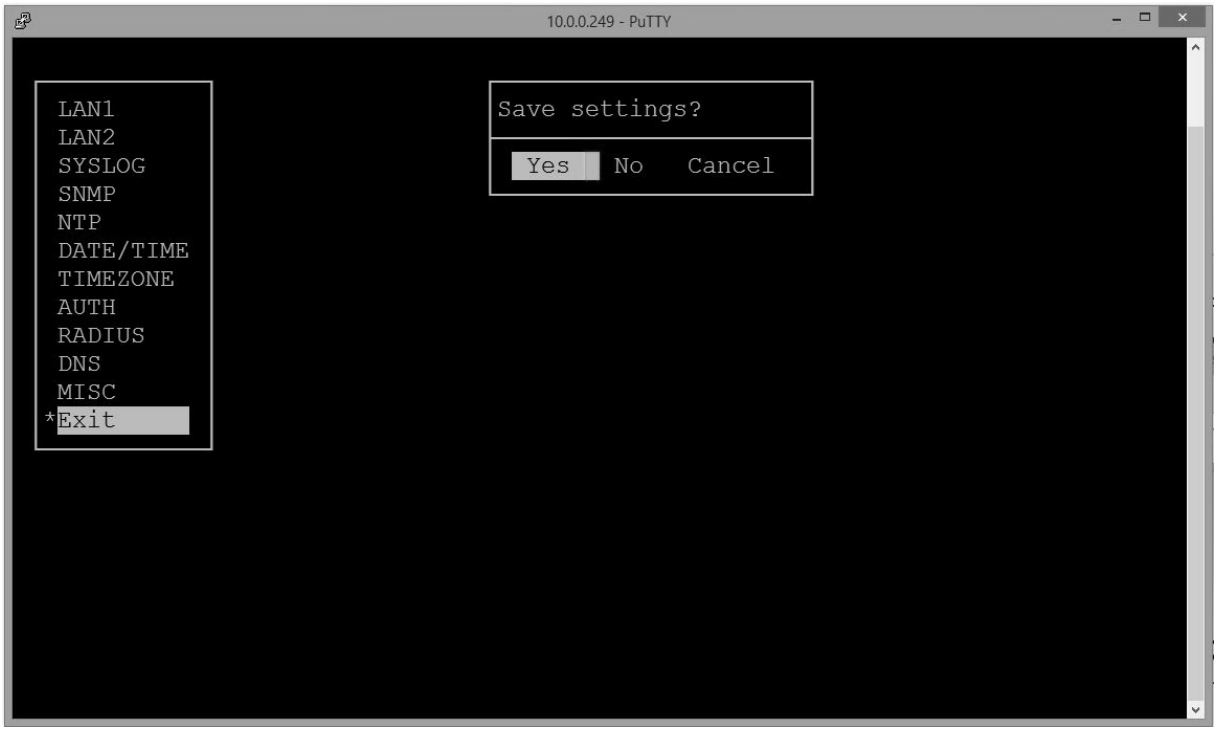
You can provide new MD5 key text sequence, modify or remove existing one.



Stored MD5 keys can be viewed. Please use VIEW from AUTH menu to view all defined MD5 keys.

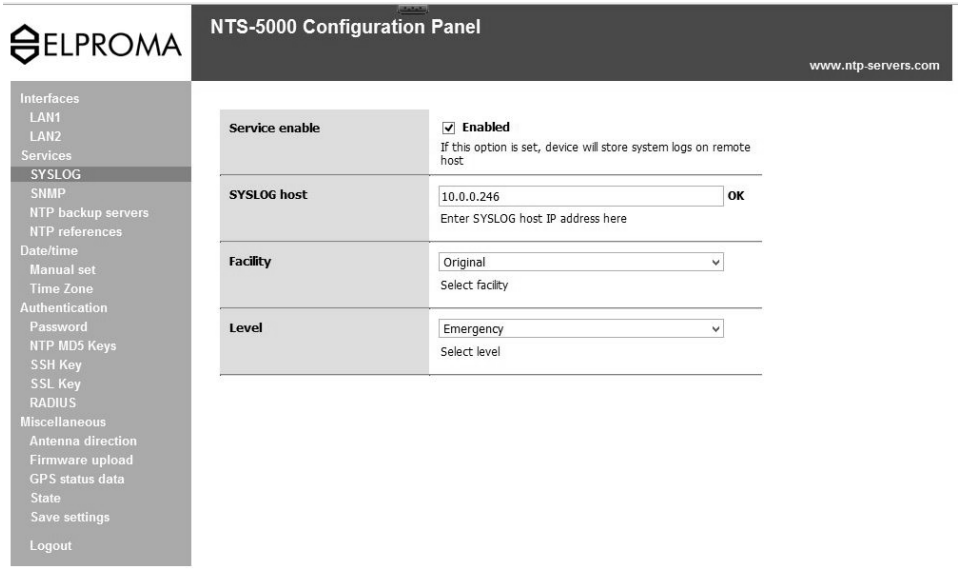


Once all MD5 keys definitions are complete please use RETURN and EXIT with saving setup. All operation will be confirmed on TTY display. We thank you for you patience and please follow those messages until final one. It is recommended to restart your timeserver before using new or modified MD5 keys. You should also perform to restart your NTP client demon (service) to take effect on changes. Please test your authenticated synchronization first before using in final production environment.

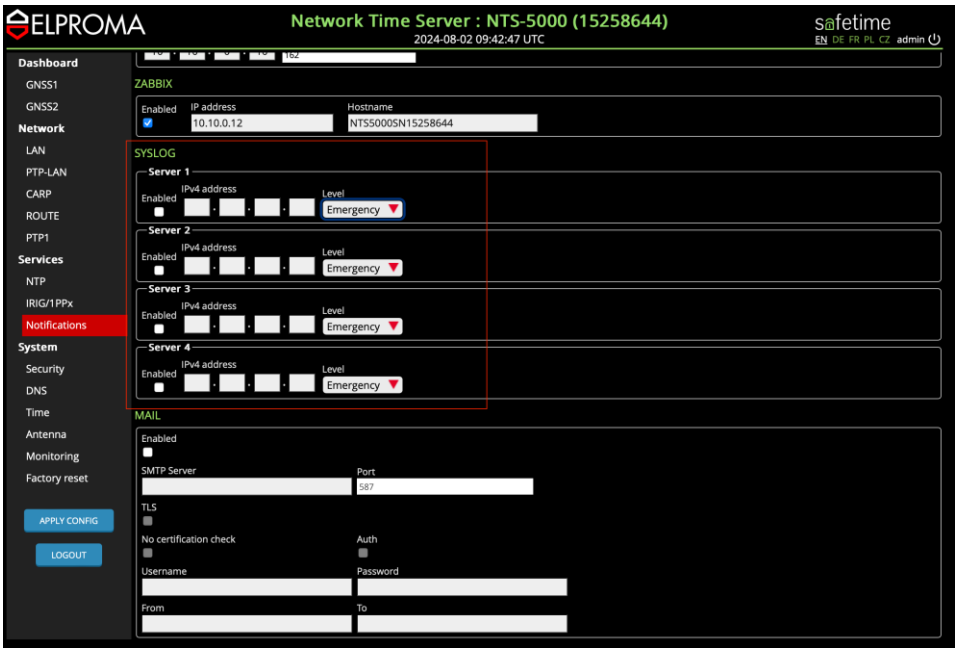

10.0.0.249 - PuTTY
LAN1
LAN2
SYSLOG
SNMP
NTP
DATE/TIME
TIMEZONE
AUTH
RADIUS
DNS
MISC
*Exit
Save settings?
Yes
No
Cancel

40. SYSLOG

Syslog is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyses them. Computer system designers can use syslog for system management and security auditing as well as general informational, analysis, and debugging messages. Syslog is a client/server protocol a logging application transmits a text message to the syslog receiver. The receiver is commonly called syslog server. Syslog messages may be sent via the UDP or TCP. The data is sent in clear text. Therefore in some cases port 514 is required to be open.



Setup version up to 2018



Setup version from 2019

NTS-3000/4000/5000 SETUP page for defining syslog server address, facility and level

NTS servers supports single syslog server reporting. Multiple syslog server support is possible intermediately using LOG redistribution between syslog servers. NTS3000/4000/5000 is providing standard reporting from most to least severe:

- *Emergency (factory default),*
- *Alert,*
- *Critical,*
- *Error,*
- *Warning,*
- *Notice,*
- *Info,*
- *Debug*

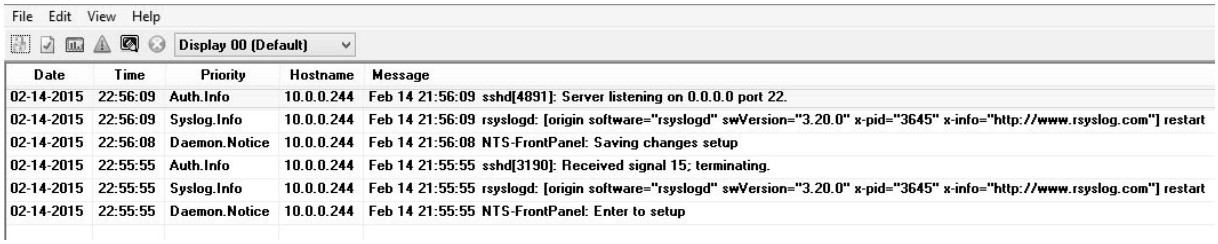
A facility level is used to specify what type of NTS-3000/4000/5000 service is logging the message. This lets the configuration file specify that messages from different facilities will be handled differently. The possible selection are: *Original (factory default – the same as FreeBSD UNIX), demon, syslog, local use from 0 to 7*.

The NTS-3000/4000/5000 sends to syslog following security messages:

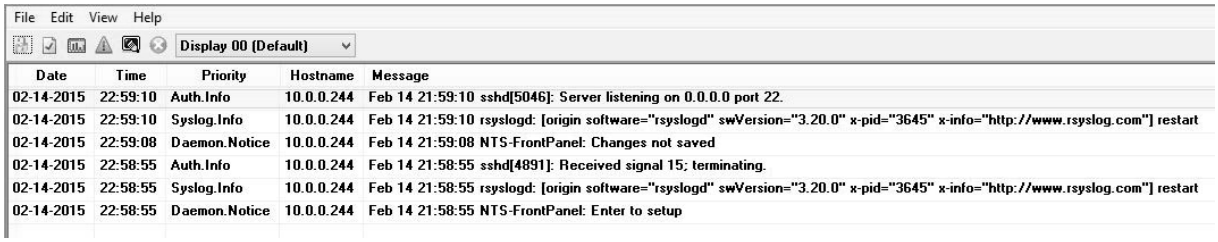
- *entering/exiting SETUP locally from front panel keyboard*
- *entering/exiting SETUP remotely using ssh, www, telnet etc*
- *the new source of UTC faze stamping is selected for synchronization (GNSS-NMEA Ant1, GNSS-NMEA Ant2, remote backup NTP servers, LOCAL clock)*

Note ! Frequency ref. as 1PPS (GNNS, EXT, IRIG-B, SYSPLEX) as well as internal build-in OSC (OCXO, Rubidium) will not trig LOG message report when synchronized to. It is because 1PPS is just a frequency std. and it is not providing any UTC time stamping information (UTC date & time). It performs high accuracy frequency tuning possible only once time server is locked (PLL/FLL) to source as Ant1, Ant2 or remote backup NTP server.

Entering/exiting SETUP locally from front panel keyboard

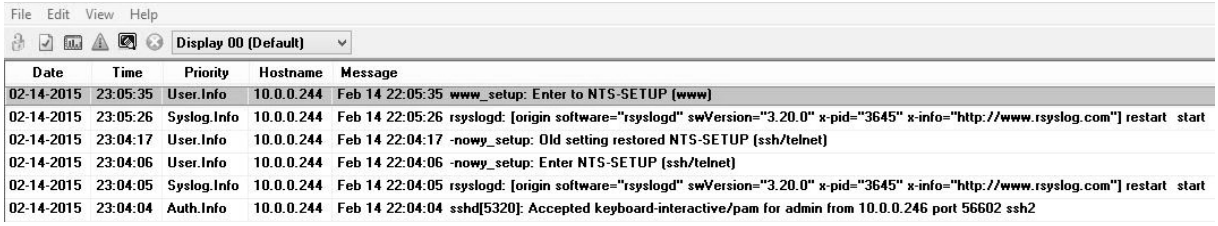


Accessing SETUP from keyboard (without saving changes)



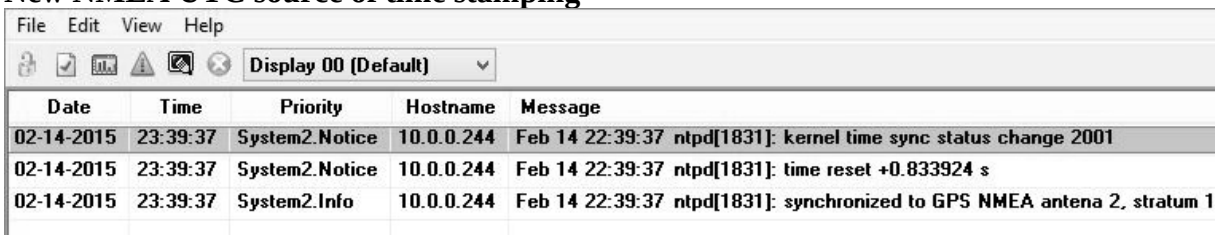
Accessing SETUP from keyboard (saving changes)

Entering/exiting SETUP remotely using ssh/www/telnet and other protocols or utility



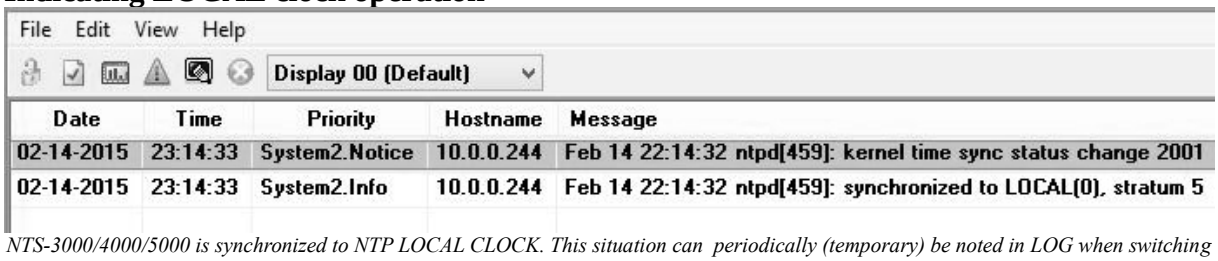
Accessing SETUP from SSH (saving changes)

New NMEA UTC source of time stamping



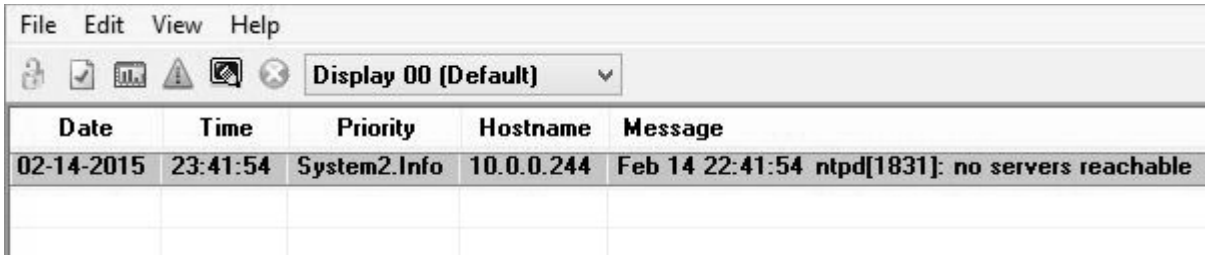
This message is sent each time NMEA UTC timestamp new source is selected. Message is not generated for frequency tuning std. as 1PSS

Indicating LOCAL clock operation



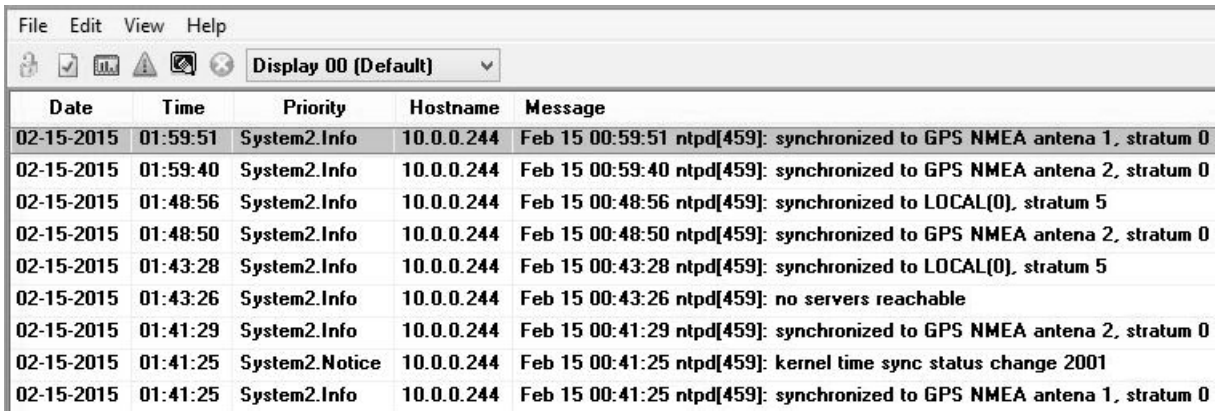
NTS-3000/4000/5000 is synchronized to NTP LOCAL CLOCK. This situation can periodically (temporary) be noted in LOG when switching between UTC sources. It is requiring than Admin inspection (eg. via NTP tool " ntpq.exe –pe") to check current status of Ant1/Ant2.

Missing UTC source for time server



NTS-3000/4000/5000 is missing source of UTC time. This situation might happen when all antennas are disconnected and server configuration has disabled OSC (OCXO, Rubidium) and LOCAL clock.

Simple LOG sequence after power up timeserver



Date	Time	Priority	Hostname	Message
02-15-2015	01:59:51	System2.Info	10.0.0.244	Feb 15 00:59:51 ntpd[459]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	01:59:40	System2.Info	10.0.0.244	Feb 15 00:59:40 ntpd[459]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	01:48:56	System2.Info	10.0.0.244	Feb 15 00:48:56 ntpd[459]: synchronized to LOCAL(0), stratum 5
02-15-2015	01:48:50	System2.Info	10.0.0.244	Feb 15 00:48:50 ntpd[459]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	01:43:28	System2.Info	10.0.0.244	Feb 15 00:43:28 ntpd[459]: synchronized to LOCAL(0), stratum 5
02-15-2015	01:43:26	System2.Info	10.0.0.244	Feb 15 00:43:26 ntpd[459]: no servers reachable
02-15-2015	01:41:29	System2.Info	10.0.0.244	Feb 15 00:41:29 ntpd[459]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	01:41:25	System2.Notice	10.0.0.244	Feb 15 00:41:25 ntpd[459]: kernel time sync status change 2001
02-15-2015	01:41:25	System2.Info	10.0.0.244	Feb 15 00:41:25 ntpd[459]: synchronized to GPS NMEA antena 1, stratum 0

Good weather conditions

Below screenshot illustrates LOG example when bed weather conditions are and there are problems in receiving SAT signals.

Date	Time	Priority	Hostname	Message
02-15-2015	11:05:53	System2.Info	10.0.0.244	Feb 15 10:05:53 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	11:05:51	System2.Info	10.0.0.244	Feb 15 10:05:51 ntpd[455]: synchronized to 10.0.1.215, stratum 1
02-15-2015	11:03:43	System2.Info	10.0.0.244	Feb 15 10:03:43 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	11:03:25	System2.Info	10.0.0.244	Feb 15 10:03:25 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	11:02:36	System2.Info	10.0.0.244	Feb 15 10:02:36 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	11:02:35	System2.Info	10.0.0.244	Feb 15 10:02:35 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	11:01:47	System2.Info	10.0.0.244	Feb 15 10:01:47 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	11:00:57	System2.Info	10.0.0.244	Feb 15 10:00:57 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	10:59:52	System2.Info	10.0.0.244	Feb 15 09:59:52 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	10:59:02	System2.Info	10.0.0.244	Feb 15 09:59:02 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:58:47	System2.Info	10.0.0.244	Feb 15 09:58:47 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	10:37:27	System2.Info	10.0.0.244	Feb 15 09:37:27 ntpd[455]: synchronized to LOCAL(0), stratum 5
02-15-2015	10:12:05	System2.Info	10.0.0.244	Feb 15 09:12:05 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:12:01	System2.Info	10.0.0.244	Feb 15 09:12:01 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:11:50	System2.Info	10.0.0.244	Feb 15 09:11:50 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:11:46	System2.Info	10.0.0.244	Feb 15 09:11:46 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:11:35	System2.Info	10.0.0.244	Feb 15 09:11:35 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:11:17	System2.Info	10.0.0.244	Feb 15 09:11:17 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:10:23	System2.Notice	10.0.0.244	Feb 15 09:10:23 ntpd[455]: time reset -1679.806025 s
02-15-2015	10:10:03	System2.Info	10.0.0.244	Feb 15 09:38:02 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:09:16	System2.Info	10.0.0.244	Feb 15 09:37:15 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:09:15	System2.Info	10.0.0.244	Feb 15 09:37:14 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:09:01	System2.Info	10.0.0.244	Feb 15 09:37:00 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:08:59	System2.Info	10.0.0.244	Feb 15 09:36:58 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:08:45	System2.Info	10.0.0.244	Feb 15 09:36:44 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:08:44	System2.Info	10.0.0.244	Feb 15 09:36:43 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:08:14	System2.Info	10.0.0.244	Feb 15 09:36:13 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:07:41	System2.Info	10.0.0.244	Feb 15 09:35:40 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:07:11	System2.Info	10.0.0.244	Feb 15 09:35:11 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:06:18	System2.Info	10.0.0.244	Feb 15 09:34:17 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:06:07	System2.Info	10.0.0.244	Feb 15 09:34:07 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:05:24	System2.Info	10.0.0.244	Feb 15 09:33:23 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:03:57	System2.Info	10.0.0.244	Feb 15 09:31:57 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:03:25	System2.Info	10.0.0.244	Feb 15 09:31:24 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:02:34	System2.Info	10.0.0.244	Feb 15 09:30:33 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:02:20	System2.Info	10.0.0.244	Feb 15 09:30:19 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:01:49	System2.Info	10.0.0.244	Feb 15 09:29:49 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0
02-15-2015	10:01:46	System2.Info	10.0.0.244	Feb 15 09:29:45 ntpd[455]: synchronized to GPS NMEA antena 2, stratum 0
02-15-2015	10:01:45	System2.Info	10.0.0.244	Feb 15 09:29:44 ntpd[455]: synchronized to GPS NMEA antena 1, stratum 0

Bad weather conditions (missing SAT signals or GNSS signal is unstable)

Important note ! Each time LOCAL clock message is the last status written to LOG the inspection via std. NTP tool “ntpq –pe” is recommended to check antennas and internal oscillators. This situation does not necessary mean emergency call since there is a high probability server reminds FLL (frequency locked) to 1PPS of NMEA GNSS (Ant1 or Ant2). If next LOG message confirms new synchronization source to NMEA (see above example on the top) there are no needs to verify LOCAL clock action.

41. Application notes HFT (MiFID II)

Below scheme presents recommendation of UTC time distribution via PTP based on NTS5000 HFT equipped with 4x PTPv2/IEEE1588 hardware cards. Solution warranties following properties:

1) All traders work in same UTC time domain (robust synchronization)

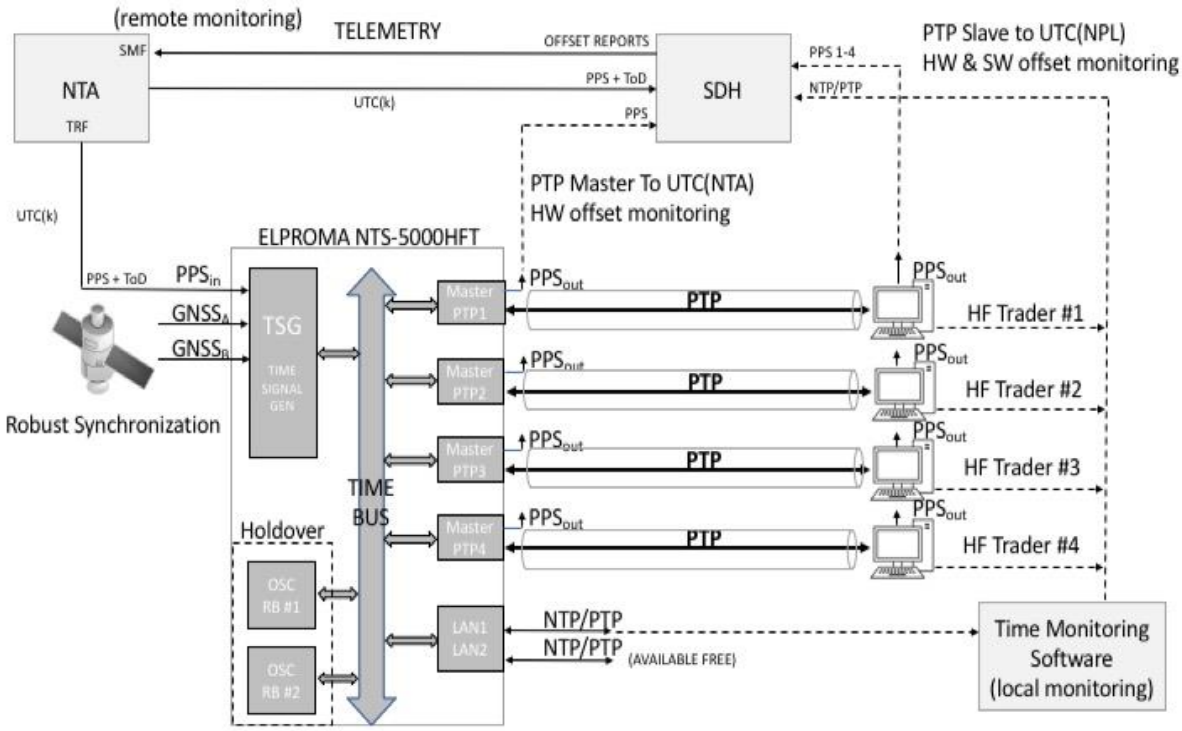
2) Mulit source time ref. provides robust UTC synchronization. Time is driven simultaneously from GNSS and NTA (NMI).

3) Each trader has own independent PTPv2/IEEE1588 synchronization line, so traders cannot interfere each other synchronization (traffic problem and its impact to PTP). Each trader PTP synchronization creates kind of “synchronization umwelt”. Each PTP Master has own IP stack, own OS driven. There is no communication between PTP masters inside NTS-5000. The Grand Master NTS-5000 supports synchronization to all trader “synchronization umwelts” – and they all work in same UTC time domain powered by robust synchronization.

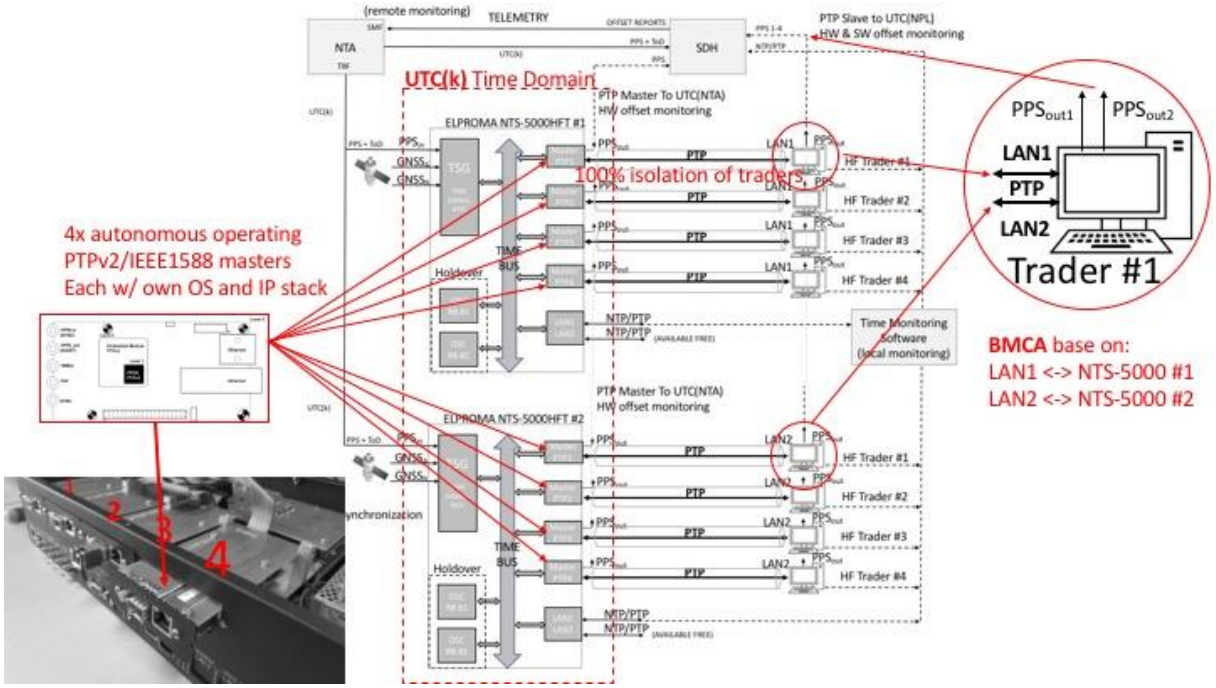
4) Each trader PTP slave should consider to support:

   a) NIC 1PPS-out for hardware monitoring (SDH). 1PPS-output should be considered to be compared to ref. 1PPS(k). All monitored data, incl. transaction LOG should be cryptographically timestamped RFC3161

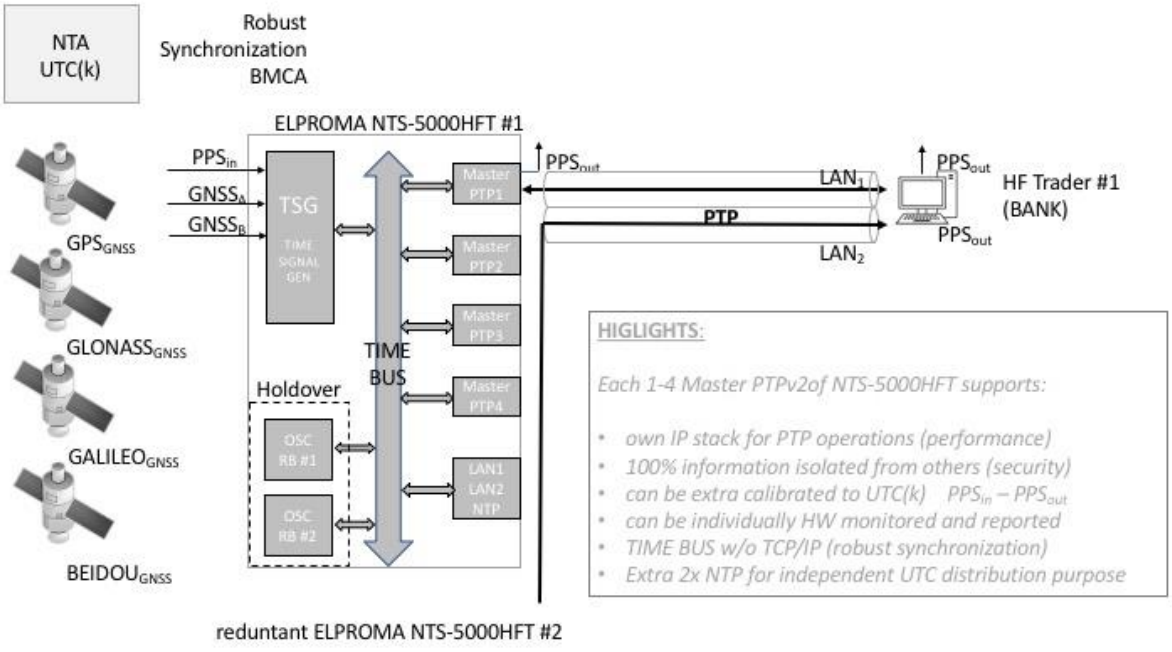
   b) Solution can be considered to use software level NTP/PTP monitoring (e.g. FSMlab Time Keeper). This is independent on NTA 1PPS hardware validation. All output audit data should be stored in LOG files, cryptographically RFC3161 timestamped, and archved for future AUDIT.



Example of Stock Exchange HFT synchronization system supporting 4 high speed traders

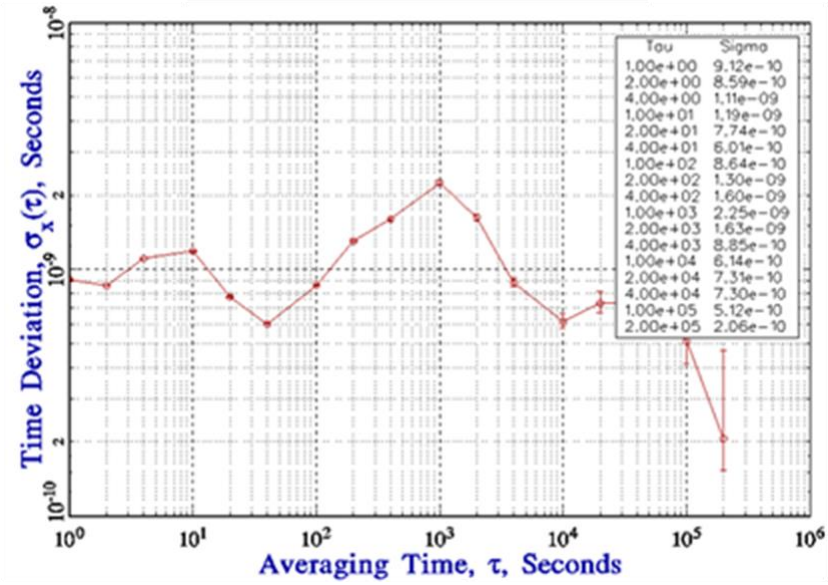


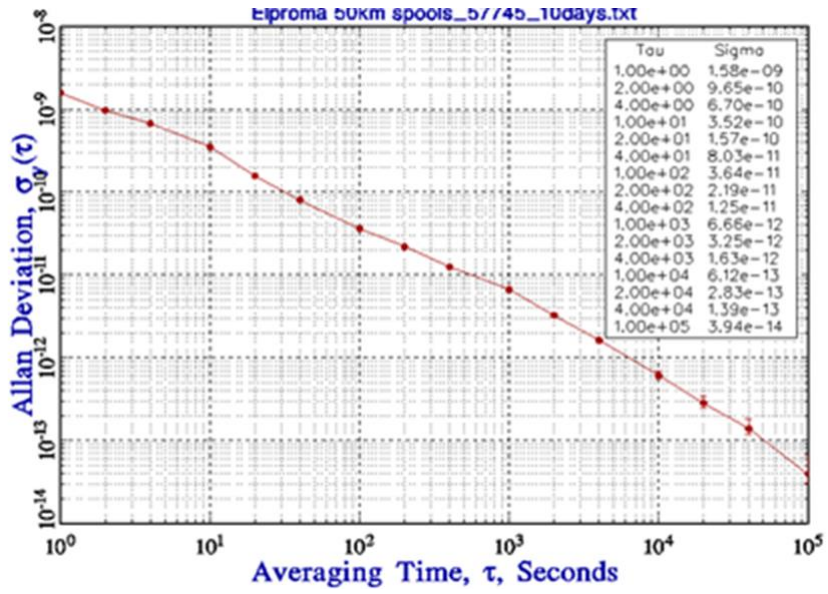
Example of Stock Exchange HFT synchronization system supporting two redundant NTS-5000HFT servers



Example of connecting PTP slave to NTS-5000HFT

Above configuration was tested w/ std. M1000 PTP Slave on distance 50km achieving synchronization accuracy of 60ns with jitter +/- 10ns. Below data presents Time Deviation (TDEV) and Allan Deviation (ADEV) plots from December/January 2017 testing at London NPL.





Tutorial

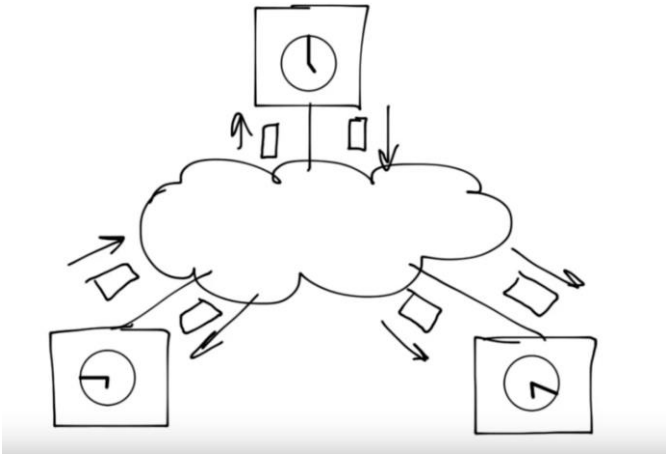
42. PTP (Precision Time Protocol) IEEE1588

The Precision Time Protocol (PTP) IEEE 1588 is designed to synchronize real-time clocks in LANs used for telecommunications, power grids, financial market, and industrial automation. Especially protocol is currently employed to synchronize financial HFT transactions, mobile phone tower transmissions Lte/5G BTS, sub-sea acoustic arrays, and any networks that require precise timing but lack access to GNSS time reference.

Typical accuracies achieved on a high-speed, multiple-segment LAN are within 100 ns and in some cases much better. Version 1 of the PTP was published in 2002. Version 2 was published in 2008 and it is not backward compatible. Shortly it is expected a new PTP IEEE1588 version 2.1

The PTP messages use the User Datagram Protocol over Internet Protocol (UDP/IP) for transport. Version 1 IEEE1588-2002 uses only IPv4 transports, but this has been extended to include IPv6 in IEEE1588-2008specification. In PTPv1 IEEE1588-2002, all PTP messages are sent using multicast messaging, while PTPv2 IEEE1588-2008 introduced an option for devices to negotiate unicast transmission on a port-by-port basis. Multicast transmissions use IP multicast addressing, for which multicast group addresses are defined for IPv4 and IPv6.

Event messages are sent to port number 319.
General messages use port number 320.



Terminal and Network Devices

The IEEE 1588 standards describe a hierarchical master-slave architecture for clock distribution

A 1588 clock is an oscillator, usually a temperature-compensated crystal oscillator (TCXO), and a counter that represents time in seconds and nanoseconds since 0 h 1 January 1970. The intended timescale is International Atomic Time (TAI) with provisions for the UTC offset and advance notice of leap seconds. The time representation is similar to POSIX, except the PTP seconds field has 48 bits, making the timestamp 10 octets long.

. How many Slaves supports PTP Master?

The short answer: It depends….

A slightly longer answer: The NTS-5000 PTP IEEE1588 expander cards (LAN3 and above) are designs can handle approx. 350 outgoing PTP messages per second. In Multicast this means that:

$$s + d * n < 350 \text{ or } n < (350 - s) / d$$

Where s is the number of sync messages (one-step) per second, d is the number of delay request messages per second and n is the number of slaves. We also have the announce messages, but these are usually kept at a very low rate, so it does not really matter. Assuming the rates are the same for sync and delay request this means:

- 1/sec: 349, but we say 250 to be safe. It depends a lot on how well the slaves distribute their delay requests over time.
- 2/sec: 174
- 32/sec: 9 (tested in our lab)
- 64/sec: 4 (tested in our lab)

In Unicast the formula is:

$$(s + d + a) * n < 350 \text{ or } n < 350 / (s + d + a)$$

Where s is the number of sync messages (one-step) per second, d is the number of delay request messages per second, a is number of announce messages per second and n is the number of slaves. Assuming the rates are the same for sync and delay request and the default announce rate of 1 every two seconds):

- 1/sec: 140
- 2/sec: 77
- 16/sec: 10 (tested in our lab)
- 32/sec: 5 (tested in our lab)
- 64/sec: 2 (tested in our lab)

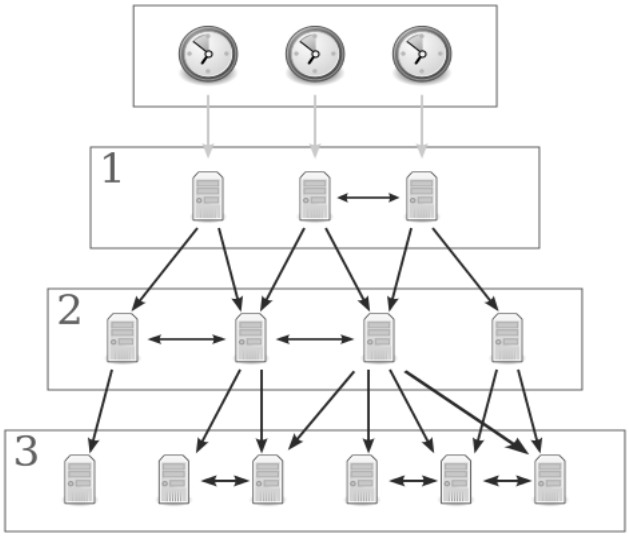
Now, this is theoretical calculations (although practically verified to some extent) so keep that in mind and use a sound margin to any numbers.

Another thing of great importance, is that our concept of Edge Grandmasters and Gateway clocks significantly reduces the need of high message rates, due to the fact that these devices will be much closer to the clients, with less complex networks in between. 16 msg/s or less should be sufficient in most cases.

43. NTP (Network Time Protocol)

When NTP on LAN1-LAN2 are operational they automatically also support older Unix DAYTIME RFC687 and RFC688. No additional configuration is required for DAYTIME.

STRATUM-0 UTC ref. time - The Clocks



NTP structure is organized in 0-15 level STRATA tree. Beginning from Stratum 2 each computer acts client to STRATUM-1 server and server for STRATUM-3. Servers can PEER providing redundancy and improving robustness of synchronization. Other protocols as SNTP and PTP do not support STRATUM hierarchy. The operate CLIENT-SERVER (Master-Slave) structure only.

. NTP – Network Time Protocol

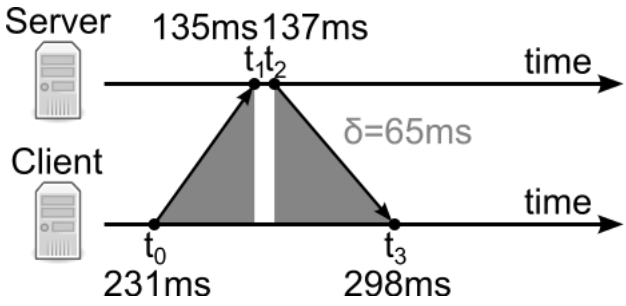
Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest and stable Internet protocols in current use. NTP was designed by David L. Mills of the University of Delaware.

NTP is intended to synchronize all participating computers operating over public Internet to within a few milliseconds of Coordinated Universal Time (UTC). Using NTS-x000 family product this accuracy can be improved inside local networks up to level of teens of microseconds.

NTP uses the intersection algorithm, a modified version of Marzullo algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency. This algorithm is also used to detect time manipulations if several time servers are available as primary reference of time.

NTP uses a hierarchical 0-15, semi-layered system of time sources. Each level of this hierarchy is termed a *stratum* and is assigned a number starting with zero for the reference clock at the top. A server synchronized to a stratum *n* server runs at stratum *n* + 1. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

Important Note! *Stratum is not always an indication of quality or reliability*



A typical NTP client will regularly poll three or more servers on diverse networks. To synchronize its clock, the client must compute its time offset and round-trip delay. Time offset θ is defined by

and the round-trip delay δ by

Where:

t0 is the client's timestamp of the request packet transmission,
t1 is the server's timestamp of the request packet reception,
t2 is the server's timestamp of the response packet transmission and
t3 is the client's timestamp of the response packet reception

The values for θ and δ are passed through filters and subjected to statistical analysis. Outliers are discarded and an estimate of time offset is derived from the best three remaining candidates. The clock frequency is then adjusted to reduce the offset gradually, creating a feedback loop.

The synchronization is correct when both the incoming and outgoing routes between the client and the server have symmetrical nominal delay. If the routes do not have a common nominal delay, there will be a systematic bias of half the difference between the forward and backward travel times.

. SNTP - Simple Network Time Protocol

SNTP (Simple Network Time Protocol) and NTP (Network Time Protocol) are describing exactly the same network package format, the differences can be found in the way how a system deals with the content of these packages in order to synchronize its time. They are basically two different ways of how to deal with time synchronization. It is especially important for client side - responsible for accuracy, security and stability of synchronization.

Compering to NTP, the SNTP does not support multisource and cryptographic authentication.

While a full featured NTP client reaches a very high level of accuracy and avoids abrupt timesteps as much as possible by using different mathematical and statistical methods and smooth clock speed adjustments, SNTP client can only be recommended for simple applications, where the requirements for accuracy and reliability are not too demanding.

By disregarding drift values and using simplified ways of system clock adjustment methods (often simple time stepping), SNTP client achieves only a low-quality time synchronization when compared with a full NTP implementation.

SNTP version 4 is defined in RFC2030, where it reads: *"It is strongly recommended that SNTP be used only at the extremities of the synchronization subnet. SNTP clients should operate only at the leaves (highest stratum) of the subnet and in configurations where no NTP or SNTP client is dependent on another SNTP client for synchronization. SNTP servers should operate only at the root (stratum 1) of the subnet and then only in configurations where no other source of synchronization other than a reliable radio or modem time service is available. The full degree of reliability ordinarily expected of primary servers is possible only using the redundant sources, diverse subnet paths and crafted algorithms of a full NTP implementation "*

Therefore, SNTP servers can supports both NTP and SNTP clients if server provides reliable high security and trustable source of time. In all other term "NTP time server" or "NTP compatible client" can - by definition - describe a system with a fully implemented NTP as well as any other product which uses and understands the NTP protocol but achieves far worse levels of reliability, accuracy and security

. PTP – Precision Time Protocol (IEEE1588)

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. IEEE 1588 is designed for local systems requiring accuracies beyond those attainable using NTP.

The IEEE 1588 standards describe a hierarchical master-slave architecture for clock distribution. Under this architecture, a time distribution system consists of one or more communication media (network segments), and one or more clocks. An ordinary clock is a device with a single network connection and is either the source of (PTP-master) or destination for (PTP-slave) a synchronization reference. A boundary clock has multiple network connections and can accurately synchronize one network segment to another. A synchronization PTP-master is selected for each of the network segments in the system. The root timing reference is called the grandmaster. The grandmaster transmits synchronization information to the clocks residing on its network segment. The boundary clocks with a presence on that segment then relay accurate time to the other segments to which they are also connected.

A simplified PTP system frequently consists of ordinary clocks connected to a single network, and no boundary clocks are used. A grandmaster is selected, and all other clocks synchronize directly to it.

IEEE 1588: 2008 standard introduces a clock associated with network equipment used to convey PTP messages. The transparent clock modifies PTP messages as they pass through the device. Timestamps in the messages are corrected for time spent traversing the network equipment. This scheme improves distribution accuracy by compensating for delivery variability across the network.

PTP typically uses the same epoch as Unix time (start of 1 January 1970). While the Unix time is based on Coordinated Universal Time (UTC) and is subject to leap seconds, PTP is based on International Atomic Time (TAI). The PTP grandmaster communicates the current offset between UTC and TAI, so that UTC can be computed from the received PTP time.

Hardening guide

1. Disable HTTP and Telnet Protocols:

- HTTP and Telnet are plaintext protocols, meaning that data transmitted using these protocols is not encrypted. Disabling these protocols enhances security by reducing the risk of unauthorized access and interception of sensitive information. Instead, consider using more secure alternatives like HTTPS for web communication and SSH for remote access.

2. Use Strong Passwords:

- Weak passwords are susceptible to brute force attacks, where attackers systematically try different combinations to gain unauthorized access. Utilizing strong, complex passwords significantly strengthens the system's security posture, making it more challenging for malicious actors to compromise user accounts.

3. Enable Only Necessary Services on Interfaces:

- Every service enabled on an interface increases the potential attack surface. By disabling unnecessary services, you reduce the number of entry points that could be exploited by attackers. This minimizes vulnerabilities and helps in maintaining a lean and more secure system.

4. Segregate Interfaces for Production and Management Purposes:

- Segregating interfaces is a fundamental security principle that helps prevent unauthorized access and potential disruptions. By dedicating specific interfaces for production tasks and separate ones for management purposes, you create an additional layer of defense. This isolation ensures that critical functions, like time synchronization for production, are not jeopardized by potential security incidents on management interfaces. It also helps in implementing and enforcing different security policies based on the role of each interface.

APPENDIX

. SNMP/MIB-2 file traps for managing NTS-5000

The SNMP MIB-2 file can be downloaded here:
https://cloud.elpromaelectronics.com/index.php/s/NTS-MIB

. GNSS Anti-Jamming/Spoofing

The NTS-x000 family is carrier grade Grandmaster clock with additional capabilities of security that provide a flexible technology suite to match the synchronization needs of evolving networks. It enables communications service providers to build a stable, robust and reliable network infrastructure using simultaneously synchronisation protocols: PTP IEEE1588, SyncE, NTP, SNTP, Chrony, IRIG, 1PPS/ToD (TC), 10MHz… etc.

The hardware redundancy is built-in from scratch to each level of architecture of NTS-5000 time server. Dual GNSS receivers (ANT1, ANT2), dual holdover oscillators (Rubidium, OCXO), multiport network interface expansion module cards NIC (each with private PTP/NTP/SyncE software stacks built into the hardware chip FPGA) ensures that there is no impact on client synchronisation performance when failover occurs. Separating clients from each other provide protection far superior to network redundancy models where random traffic push to reacquire synchronization from a different grandmaster somewhere else in the network. When locked to a GNSS input, the NTS-5000 meets the applicable performance requirements of the ITU-T G.8272 (Rubidium version only) standard for a primary reference time clock (PRTC). This is important considering **protection of the input clock sources that has become increasingly important these days.**

NTS-x000 has 3 independent LEVELS of protection

The LEVEL-1 protection is built-in to standard NTS-x000 network appliance, however to enable it needs, a pied license. This functionality is supported for each GNSS receiver (ANT1, ANT2). Both connected Smart Antennas can do auto antenna ON/OFF switching when RF jamming or GNSS spoofing is recognised. It lets NTS-x000 switch early enough to built-in oscillator (Rubidium, OCXO) holdover mode refusing false signals from antenna.

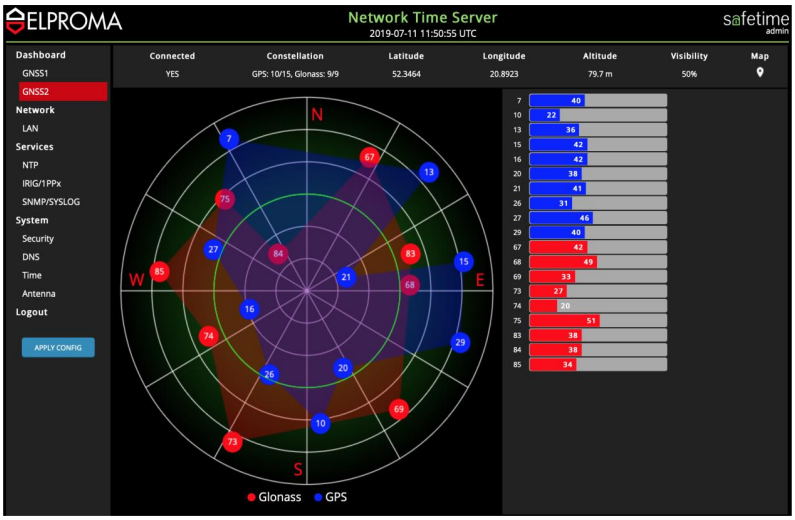
The NTS-5000 will then still ensure the accuracy of 200ns (nanoseconds) for another 15 hours of GNSS less operation (the ANT1/ANT2 antenna is OFF or STAND-BY mode) when equipped with Rubidium & OCXO oscillators, and 4 hours only when NTS-5000 (NTS-4000) is equipped with OCXO oscillator only (no Rubidium). Longer holdovers increase the oscillator drift ensuring less accuracy of synchronisation on next days. The NTS-3000 does not include internal oscillator, therefore it drifts near immediately, once the GNSS is missing.

Once the RF jamming/spoofing attack ends the NTS-x000 switches back to normal operation synchronizing from GNSS. The LEVEL-1 protection can be extra amplified by using simultaneously 2x GNSS receivers located min. 50m (optimally if more than 200m) from each other. This is so-called the “Geographical” anti-jamming/spoofing approach, perhaps the most effective one to prevent against mobile jammers and Hack-RF GPS spoofers.

The vulnerability of GNSS, especially of the GPS system, to various signal incidents is well documented. The rapid proliferation of GNSS systems has embedded these vulnerabilities into critical national infrastructures as well as corporate infrastructures that rely on GNSS delivered for daily operations. This widespread deployment of GNSS receivers makes it impractical to replace all fielded GNSS systems in a timely or cost-effective manner. The NTS-x000 family protects for all vulnerabilities.

GNSS satellite traceability is important.

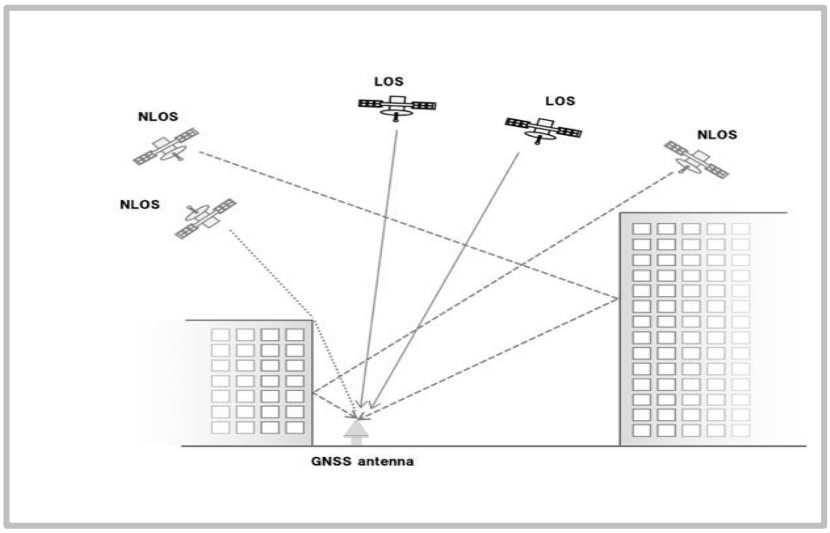
NTS-x000 has built-in professional GNSS satellite traceability monitoring linked to SNMP / MIB-2 NMS system. It is compatible to any OSS software. The Elproma MIB-2 file is defining one of the world largest database of alarm traps, including RF jamming and spoofing recognition alarms.



Adaptive GNSS antennas - multi-path mitigation and 3rd part suppliers

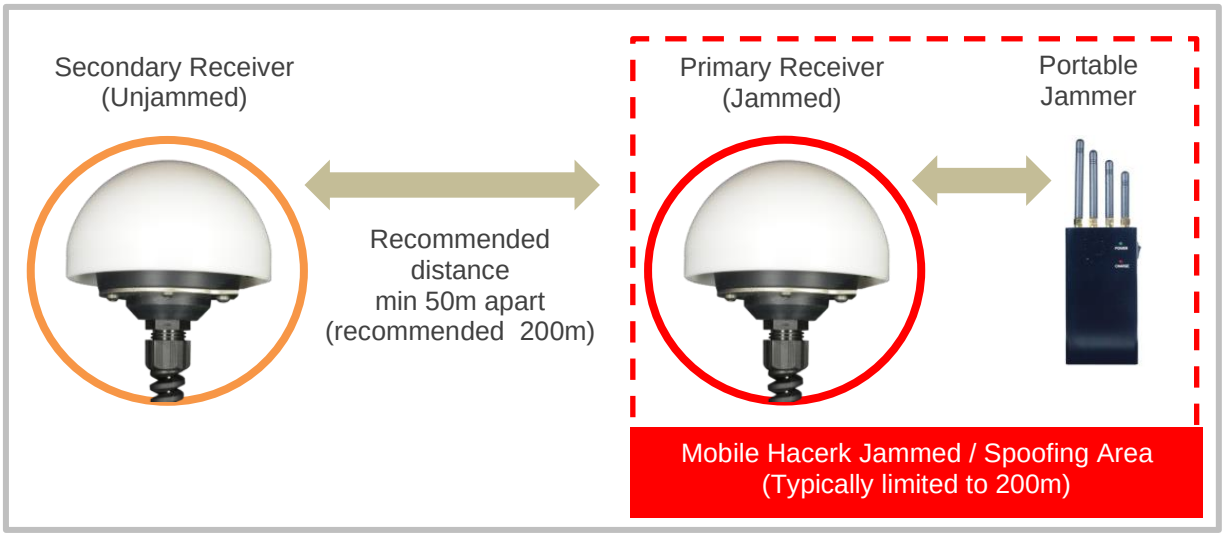
The NTS-x000 is delivered with Smart Antenna in which the replaceable GNSS receiver adaptive board is built into the antenna dome, instead of the usual approach of placing the receiver inside the server enclosure. The replaceable GNSS receiver boards are OCP (Open Computing Project) standard and security checked inside Facebook, Microsoft, Google, Amazon labs. The NTS-x000 can be also equipped with the 3rd part adaptive antenna suppliers.

One of cyber-security acknowledged for NTS-x000 receivers is Furuno manufacturer, who has developed a new special technology to enhance the reception of GNSS signal. This unique functionality enables correct timing signal to be computed even when antennas are mounted in a lower canyon ground and accept reflected/diffracted GNSS signals.



“Geographical” 200m distance jamming/spoofing risk diversification

The NTS-x000 comes with dual GNSS antenna physical ports ANT1 ANT2. At LEVEL-1 antenna protection, when 2 x Smart Antenna are at least 50m apart, the physical distance deters the risk of mobile jammers as the signal interference is typically limited to max. 200m. Therefore, if the primary antenna is jammed, the secondary antenna (outside the jammed area) can take over to provide GNSS signal to NTS-x000. Independently NTS-x000 senses RF-interferences switching-OFF jammed antenna and continuing with 2nd antenna or switching to GNSS-less holdover mode.



Elproma has developed a Smart Antenna in which the replaceable GNSS receiver board is built into the Smart Antenna dome, instead of the usual approach of placing the receiver inside the server enclosure. One pcs of Smart Antenna is included to NTS-5000 and the 2nd needs to be purchased separately.

Critical Infrastructures and US President Directive EO13905

Easy GNSS receiver replacement enables custom cybersecurity ensuring correct industry profile setting suitable for current “Geopolitical” situation in region. Protection of the input time from GNSS source has become increasingly important today and therefore it is requiring flexibility of changing to GNSS trusted receivers - the one security approved by Open Computing Project society (OCP-TAP).

The US Presidential Directive EO13905 recommends using only GPS for US critical infrastructure and further recommends synchronization backups from NIST servers or from alternative PNT systems (e.g. Xona Space Systems). Similar recommendations are underway in the EU which recommend a GALILEO + GPS configuration. Russia's economy is focused on GLONASS, India prefers IRNSS, and China recommends BEIDOU to support local critical infrastructure. Other countries set its own policy.

Elproma has uniquely decoupled the GNSS receiver to their smart NTS-antenna to enable flexibility and cybersecurity:

- Flexible to switch between GNSS receiver manufacturers Furuno, u-blox, Trimble…
- Help to diverge risks of security & firmware gaps in using different GNSS receivers
- Ease of migration to a new future GNSS constellations IRNSS, IRIDIUM, XONA…
- Ease of migration from single (L1) to dual (L1+L5 / L1+L2) or triple band L1+L2+L5
- Using dual GNSS Smart Antennas improves high availability (HA) of GNSS
- Improves robustness of UTC leap-second support and preventing unexpected peaks

Custom periodical GNSS synchronisation with “DELTA-T“ condition

The highest level of cybersecurity is offered by those systems that use proprietary, irregularly changed (dynamic) security strategy. The NTS-x000 is able to use custom defined security algorithm using pseudo randomness (RNG). The operating concept assumes that, once synchronized initially to GNSS, the NTS-5000 stays in constant holdover mode and only periodically synchronizes its Rubidium + OCXO oscillators to GNSS. This requires the special operation of the Smart Antennas in the STAND-BY reading mode. The NTS-x000 server checks the condition of UTC offset between OSC and GNSS, and unless it detects UTC offset greater than the predefined DELTA-T, it will periodically turn on the synchronization stabilizing the operation of both for both Rubidium & OCXO oscillators. This method is effective for fast spoofing only. For slow gradual long-term spoofing it is recommended to use cloud time backup.

Tips and basic recommendations (what do they not tech you at school)

- Use 2x GNSS Smart Antenna (GNSS receiver built-in to antenna dome) for redundancy
- Use above redundancy on smart way – ask you supplier to provide both Smart Antennas with a different vendor GNSS receivers.
    - ✓ In other words - do not use the same type of GNSS receivers for both Smart Antennas.
    - ✓ If you use the GNSS receiver, the GNSS spoofing attack will easily avoid both receivers
    - ✓ The GNSS spoofing needs strategy. If more niche your configuration is then more protected you are…

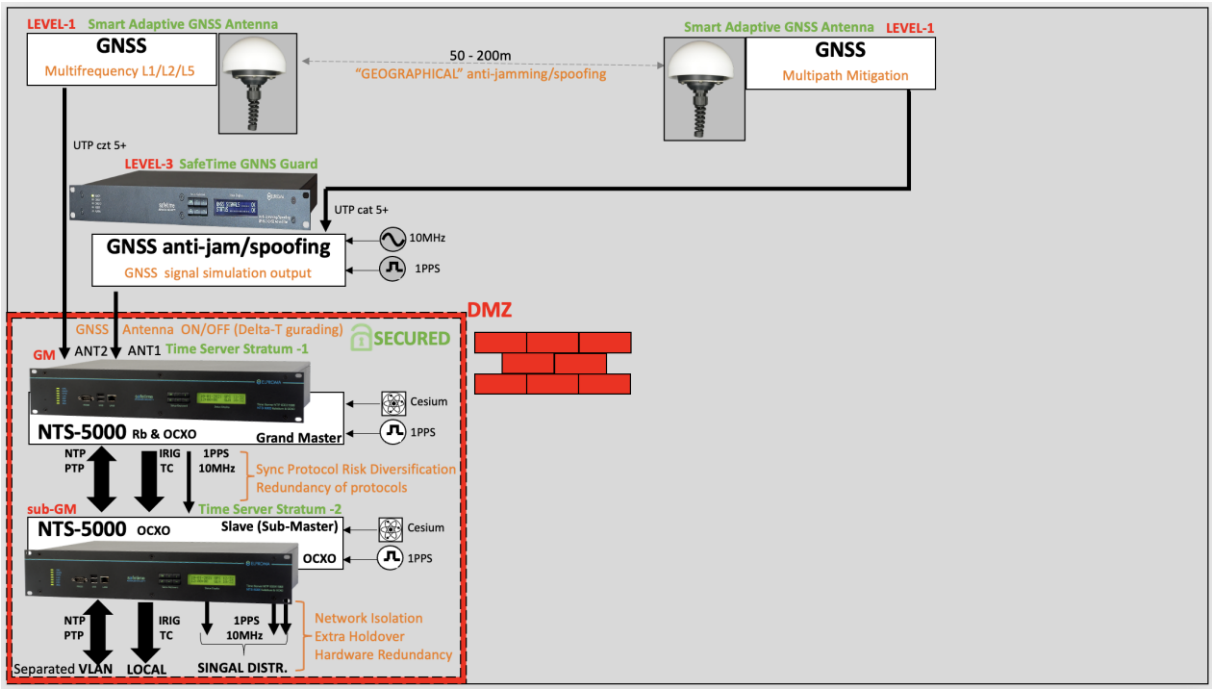
- Use natural “GEOGRAPHICAL” anti-jamming/spoofing by locating both Smart Antennas on a min. 200m from each other. More of mobile GNSS jammers and RF-hacker spoofers have limited range of effective disruption distance do max. 200m.
- Locating 2x Smart Antennas in a distance of min 50-200m reduces probability both will be affected by mobile jamming/spoofing.

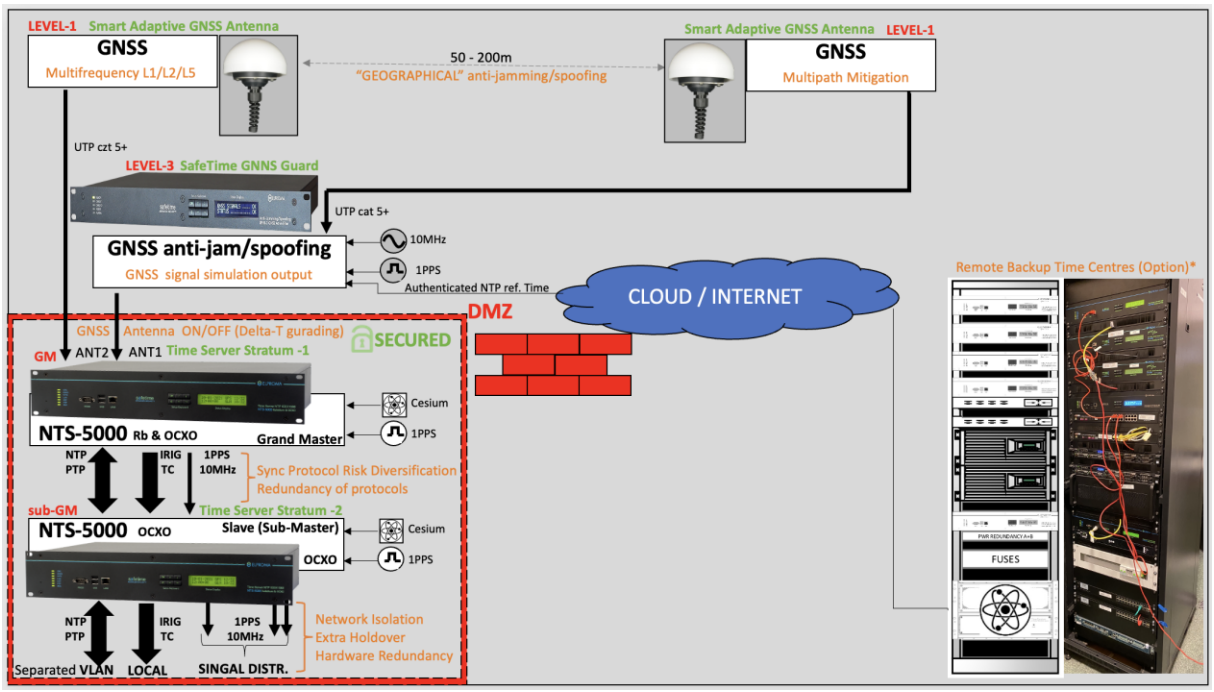
Inside USA/EU:

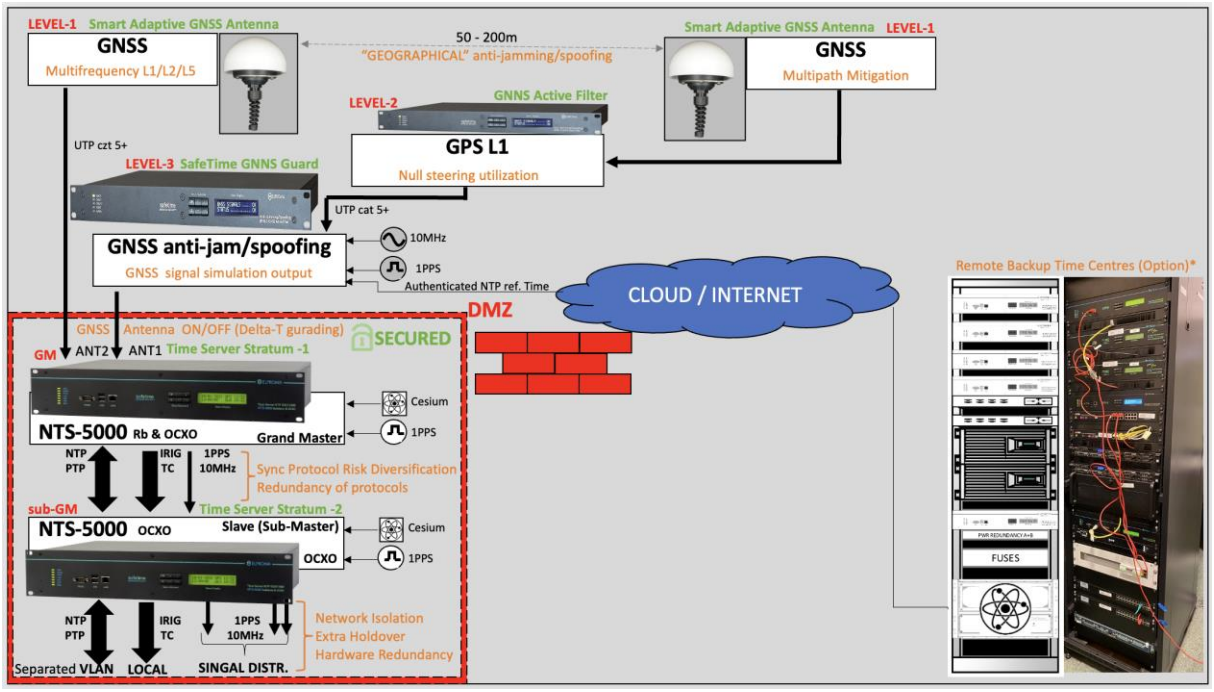
- The GNSS receivers should be configured exclusively for GPS-alone, GALILEO-alone, GPS+GALILEO pair only…
- GNSS constellations like the Russian GLONASS or Chinas BEIDOU can be considered for time monitoring only …
- Follow the US President Directive EU13905 to stay synchronize to emanative remote time backup centres (NIST, EURAMET etc.)

Outside USA/EU (all other countries):

- Always try to make your GNSS configuration suitable for current geopolitical situation in the region…
- Try to consider the GNSS receivers that supports multipath-mitigation, null steering anti-jamming techniques…
- Separate your NTS-5000 time server form physical GNSS signals using SafeTime GNSS Guard. It is the equivalent of network Firewall appliance, but dedicated for separation from physical GNSS signals.
- The SafeTime GNSS Guard is a satellite GPS L1 C/A code simulator operating on electric signal level.
- The SafeTime GNSS guard protection enables functionality to get ref. time from remote Time Backup Center or NMI.
- This is the only protection for strong (>150dB) military RF-jamming attack.
- Order special protection functions for NTS-x000 that switches OFF the antenna when RF- interference is recognised.
- The customised NTS-5000 is able to work all the time in holdover mode of oscillator switching from time to time ON to get synchronised




LEVEL-1 Smart Adaptive GNSS Antenna
GNSS
Multifrequency L1/L2/L5
50 - 200m
"GEOGRAPHICAL" anti-jamming/spoofing
Smart Adaptive GNSS Antenna LEVEL-1
GNSS
Multipath Mitigation
UTP czt 5+
LEVEL-3 SafeTime GNNS Guard
UTP cat 5+
GNSS anti-jam/spoofing
GNSS signal simulation output
10MHz
1PPS
Authenticated NTP ref. Time
CLOUD / INTERNET
Remote Backup Time Centres (Option)*
DMZ
GNSS Antenna ON/OFF (Delta-T gurading)
SECURED
GM
ANT2
ANT1
Time Server Stratum -1
NTS-5000 Rb & OCXO
Grand Master
Cesium
1PPS
NTP
PTP
IRIG
TC
1PPS
10MHz
Sync Protocol Risk Diversification
Redundancy of protocols
sub-GM
Time Server Stratum -2
NTS-5000 OCXO
Slave (Sub-Master)
OCXO
Network Isolation
Extra Holdover
Hardware Redundancy
Separated VLAN
LOCAL
SINGAL DISTR.
FUSES



For detailed product technical specification please visit:
www.elpromaelectronics.com

tel. +48 227517680