THUNDERBOLT GM200/TS200

IEEE-1588 (PTP) GRANDMASTER CLOCK (GM200)
NTP TIME SERVER (TS200)

USER GUIDE

For use with: Thunderbolt GM200/TS200 time server (P/N 111224-xx)

Version 3.00.00
Revision A
April 2021

P/N: 106131-00

Corporate Office

Trimble Inc.

935 Stewart Drive

Sunnyvale, California 94085

USA

Time & Frequency Division

Trimble Inc.

935 Stewart Drive

Sunnyvale, California 94085

USA

www.trimble.com

Email: tsgsupport@trimble.com

Legal Notices

Trimble, the Globe & Triangle logo, and Thunderbolt are trademarks of Trimble Inc., registered in the United States and in other countries. Bullet is a trademark of Trimble Inc.

Microsoft, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are the property of their respective owners.

Release Notice

This is the April 2021 release (Revision A) of the Thunderbolt GM200/TS200 documentation.

The Australian Consumer Law

Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Trimble's warranty (set out below) is in addition to any mandatory rights and remedies that you may have under the Australian Consumer Law.

LIMITED WARRANTY TERMS AND CONDITIONS

Product Limited Warranty

Subject to the following terms and conditions, Trimble Inc. ("Trimble") warrants that for a period of one (1) year from date of purchase this Trimble product (the "Product") will substantially conform to Trimble's publicly available specifications for the Product and that the hardware and any storage media components of the Product will be substantially free from defects in materials and workmanship.

Product Software

Product software, whether built into hardware circuitry as firmware, provided as a standalone computer software product, embedded in flash memory, or stored on magnetic or other media, is licensed solely for use with or as an integral part of the Product and is not sold. If accompanied by a separate end user license agreement ("EULA"), use of any such software will be subject to the terms of such end user license agreement (including any differing limited warranty terms, exclusions, and limitations), which shall control over the terms and conditions set forth herein.

Except for the limited license rights expressly provided herein, Trimble and its suppliers have and will retain all rights, title and interest (including, without limitation, all patent, copyright, trademark, trade secret and other intellectual property rights) in and to the Product Software and all copies, modifications and derivative works thereof (including any changes which incorporate any of your ideas, feedback or suggestions).

You shall not (and shall not allow any third party to): (a) decompile, disassemble, or otherwise reverse engineer the Product Software or attempt to reconstruct or discover any source code, underlying ideas, algorithms, file formats or programming interfaces of the Product Software by any means whatsoever (except and only to the extent that applicable law prohibits or restricts reverse engineering restrictions); (b) distribute, sell, sublicense, rent, lease, or use the Product Software (or any portion thereof) for time sharing, hosting, service provider, or like purposes; (c) remove any product identification, proprietary, copyright, or other notices contained in the Product Software; (d) modify any part of the Product Software, create a derivative work of any part of the Product Software, or incorporate the Product Software into or with other software, except to the extent expressly authorized in writing by Trimble; (e) attempt to circumvent or disable the security key mechanism that protects the Product Software against unauthorized use (except and only to the extent that applicable law prohibits or restricts such restrictions); or (f) publicly disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the Product Software. If the Product Software has been provided to you as embedded in any hardware device, you are not licensed to separate the Product Software from the hardware device. If the Product Software has been provided to you separately from a hardware device but is intended to be loaded onto a hardware device specified by Trimble (such as a firmware update), your license is limited to loading the Product Software on the device specified by Trimble, and for no other use.

Software Fixes

During the limited warranty period you will be entitled to receive such Fixes to the Product software that Trimble releases and makes commercially available and for which it does not charge separately, subject to the procedures for delivery to purchasers of Trimble products generally. If you have purchased the Product from a Trimble authorized dealer rather than from Trimble directly, Trimble may, at its option, forward the software Fix to the Trimble authorized dealer for final distribution to you. Minor Updates, Major Upgrades, new products, or substantially new software releases, as identified by Trimble, are expressly excluded from this update process and limited warranty. Receipt of software Fixes or other enhancements shall not serve to extend the limited warranty period. For purposes of this warranty the following definitions shall apply: (1) "Fix(es)" means an error correction or other update created to fix a previous software version that does not substantially conform to its Trimble specifications; (2) "Minor Update" occurs when enhancements are made to current features in a software program; and (3) "Major Upgrade" occurs when significant new features are added to software, or when a new product containing new features replaces the further development of a current product line. Trimble reserves the right to determine, in its sole discretion, what constitutes a Fix, Minor Update, or Major Upgrade.

Warranty Remedies

If the Trimble Product fails during the warranty period for reasons covered by this limited warranty and you notify Trimble of such failure during the warranty period, Trimble will repair OR replace the nonconforming Product with new, equivalent to new, or reconditioned parts or Product, OR refund the Product purchase price paid by you, at Trimble's option, upon your return of the Product in accordance with Trimble's product return procedures then in effect.

How to Obtain Warranty Service

To obtain warranty service for the Product, please contact your local Trimble authorized dealer. Alternatively, you may contact Trimble to request warranty service by sending an email to tsgsupport@trimble.com. Please prepare to provide:

– your name, address, and telephone numbers

– proof of purchase

– a copy of this Trimble warranty

– a description of the nonconforming Product including the model number

– an explanation of the problem

The customer service representative may need additional information from you depending on the nature of the problem. Any expenses incurred in the making of a claim under this warranty will be borne by you.

Warranty Exclusions and Disclaimer

This Product limited warranty shall only apply in the event and to the extent that: (a) the Product is properly and correctly installed, configured, interfaced, maintained, stored, and operated in accordance with Trimble's applicable operator's manual and specifications, and; (b) the Product is not modified or misused.

This Product limited warranty shall not apply to, and Trimble shall not be responsible for, defects or performance problems resulting from: (i) the combination or utilization of the Product with hardware or software products, information, data, systems, interfaces, or devices not made, supplied, or specified by Trimble;

(ii) the operation of the Product under any specification other than, or in addition to, Trimble's standard specifications for its products; (iii) the unauthorized installation, modification, or use of the Product; (iv) damage caused by: accident, lightning or other electrical discharge, fresh or salt water immersion or spray (outside of Product specifications), or exposure to environmental conditions for which the Product is not intended; (v) normal wear and tear on consumable parts (e.g., batteries); or (vi) cosmetic damage. Trimble does not warrant or guarantee the results obtained through the use of the Product, or that software components will operate error free.

NOTICE REGARDING PRODUCTS EQUIPPED WITH TECHNOLOGY CAPABLE OF TRACKING SATELLITE SIGNALS FROM SATELLITE BASED AUGMENTATION SYSTEMS (SBAS) (WAAS/EGNOS, AND MSAS), OMNISTAR, GPS, MODERNIZED GPS OR GLONASS SATELLITES, OR FROM IALA BEACON SOURCES: TRIMBLE IS NOT RESPONSIBLE FOR THE OPERATION OR FAILURE OF OPERATION OF ANY SATELLITE BASED POSITIONING SYSTEM OR THE AVAILABILITY OF ANY SATELLITE BASED POSITIONING SIGNALS.

THE FOREGOING LIMITED WARRANTY TERMS STATE TRIMBLE'S ENTIRE LIABILITY, AND YOUR EXCLUSIVE REMEDIES, RELATING TO THE TRIMBLE PRODUCT UNDER THIS LIMITED WARRANTY. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED HEREIN, THE PRODUCT, AND ACCOMPANYING DOCUMENTATION AND MATERIALS ARE PROVIDED "AS-IS" AND WITHOUT EXPRESS OR IMPLIED WARRANTY OF ANY KIND, BY EITHER TRIMBLE OR ANYONE WHO HAS BEEN INVOLVED IN ITS CREATION,

PRODUCTION, INSTALLATION, OR DISTRIBUTION, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR GUARANTEES OF MERCHANTABILITY, ACCEPTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT. THE STATED EXPRESS WARRANTIES ARE IN LIEU OF ALL OBLIGATIONS OR LIABILITIES ON THE PART OF TRIMBLE ARISING OUT OF, OR IN CONNECTION WITH, ANY PRODUCT. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS

ON DURATION OR THE EXCLUSION OF AN IMPLIED WARRANTY, THE ABOVE LIMITATION MAY NOT APPLY OR FULLY APPLY TO YOU.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, TRIMBLE'S ENTIRE LIABILITY UNDER ANY PROVISION HEREIN SHALL BE LIMITED TO THE AMOUNT PAID BY YOU FOR THE PRODUCT AND IN NO EVENT SHALL TRIMBLE OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGE WHATSOEVER UNDER ANY CIRCUMSTANCE OR LEGAL THEORY RELATING IN ANYWAY TO THE PRODUCTS, SOFTWARE AND ACCOMPANYING DOCUMENTATION AND MATERIALS, (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER PECUNIARY LOSS), REGARDLESS OF WHETHER TRIMBLE HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH LOSS AND REGARDLESS OF THE COURSE OF DEALING WHICH DEVELOPS OR HAS DEVELOPED BETWEEN YOU AND TRIMBLE. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY OR FULLY APPLY TO YOU.

PLEASE NOTE: THE ABOVE TRIMBLE LIMITED WARRANTY PROVISIONS WILL NOT APPLY TO PRODUCTS PURCHASED IN THOSE JURISDICTIONS (E.G., MEMBER STATES OF THE EUROPEAN ECONOMIC AREA) IN WHICH PRODUCT WARRANTIES ARE THE RESPONSIBILITY OF THE LOCAL TRIMBLE AUTHORIZED DEALER FROM WHOM THE PRODUCTS ARE ACQUIRED. IN SUCH A CASE, PLEASE CONTACT YOUR LOCAL TRIMBLE AUTHORIZED DEALER FOR APPLICABLE WARRANTY INFORMATION.

Official Language

THE OFFICIAL LANGUAGE OF THESE TERMS AND CONDITIONS IS ENGLISH. IN THE EVENT OF A CONFLICT BETWEEN ENGLISH AND OTHER LANGUAGE VERSIONS, THE ENGLISH LANGUAGE SHALL CONTROL.

Registration

To receive information regarding updates and new products, please contact your local Trimble authorized dealer or visit the Trimble website at www.trimble.com/register. Upon registration you may select the newsletter, upgrade, or new product information you desire.

Notices

Class B Statement – Notice to Users. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

– Reorient or relocate the receiving antenna.

– Increase the separation between the equipment and the receiver.

– Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

– Consult the dealer or an experienced radio/TV technician for help.

Changes and modifications not expressly approved by the manufacturer or registrant of this equipment can void your authority to operate this equipment under Federal Communications Commission rules.

Canada

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of the Canadian Department of Communications, ICES-003.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Classe B prescrites dans le règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada, ICES-003.

Europe

This product has been tested and found to comply with the requirements for a Class B device pursuant to European Council Directive 89/336/EEC on EMC, thereby satisfying the requirements for CE Marking and sale within the European Economic Area (EEA). These requirements are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential or commercial environment.

Notice to Our European Union Customers

For product recycling instructions and more information, please go to http://www.trimble.com/Corporate/Environmental_Compliance.aspx.

Recycling in Europe: To recycle Trimble WEEE (Waste Electrical and Electronic Equipment, products that run on electrical power.), Call +31 497 53 24 30, and ask for the "WEEE Associate". Or, mail a request for recycling instructions to:

Trimble Europe BV

c/o Menlo Worldwide Logistics Meerheide 45

5521 DZ Eersel, NL

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Declaration of Conformity

We, Trimble Inc.,

935 Stewart Drive
Sunnyvale
California 94085-3913
United States of America

+1-408-481-8000

declare under sole responsibility that the product: Thunderbolt® GM200/TS200 time server complies with Part 15B of FCC Rules.

Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

List of Abbreviations

A-GPS	Assisted GPS
APTS	Assisted Partial Timing Support
BC or T-BC	Boundary Clock or Telecom Boundary Clock
C/No	Carrier-to-Noise power ratio
DC	Direct Current
DOP	Dilution of Precision
EGNOS	European Geostationary Navigation Overlay Service
ESD	Electrostatic Discharge
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema
GND	Ground
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
LNA	Low Noise Amplifier
NMEA	National Marine Electronics Association
NTP	Network Time Protocol. Common time distribution over networks
OCXO	Oven Controlled Crystal Oscillator
OD mode	Over-determined clock mode
PoE	Power over Ethernet
PCB	Printed Circuit Board
PDOP	Position Dilution of Precision
PPS	Pulse per Second
PTP	Precision Time Protocol (IEEE-1588)
QZSS	Quasi-Zenith Satellite System
RF	Radio Frequency
Sync E	Synchronous Ethernet
SFP	Small Form-factor Pluggable
ToD	Time of Day
T-R AIM	Timing Receiver Autonomous Integrity Monitoring
VCC	Voltage at the Common Collector; positive supply voltage
VSWR	Voltage Standing Wave Ratio

Safety Information

Warnings and Cautions

Always follow the instructions that accompany a Warning or Caution. The information it provides is intended to minimize the risk of personal injury and/or damage to property. In particular, observe safety instructions that are presented in the following format:

WARNING – This alert warns of a potential hazard which, if not avoided, could result in severe injury or even death.

CAUTION – This alert warns of a potential hazard or unsafe practice which, if not avoided, could result in injury or property damage or irretrievable data loss.

CAUTION – Electrical hazard – risk of damage to equipment. Make sure all electrostatic energy is dissipated before installing or removing components from the device. An electrostatic discharge (ESD) can cause serious damage to the component once it is outside the chassis.

This system can become extremely hot and cause burns. To reduce the risk of injury from a hot system, allow the surface to cool before touching it.

Operation and storage

WARNING – Operating or storing the Thunderbolt GM200/TS200 time server outside the specified temperature range can damage it. For more information, see the product specifications on the data sheet.

WARNING – The Thunderbolt GM200/TS200time server is only to be used in a restricted access location.

WARNING – Short-circuit (overcurrent) protection device required. The Thunderbolt GM200/TS200time server relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is listed rated not greater than 10 A.

Routing any cable

CAUTION – Be careful not to damage the cable. Take care to avoid sharp bends or kinks in the cable, hot surfaces (for example, exhaust manifolds or stacks), rotating or reciprocating equipment, sharp or abrasive surfaces, door and window jambs, and corrosive fluids or gases.

Contents

1. Introduction

The Precision Time Protocol (PTP) is one of the most important packet timing protocols for next generation network synchronization. Other packet-based protocols include the Network Time Protocol (NTP). However, PTP offers much better accuracy and often at an accuracy of <100 nanoseconds.

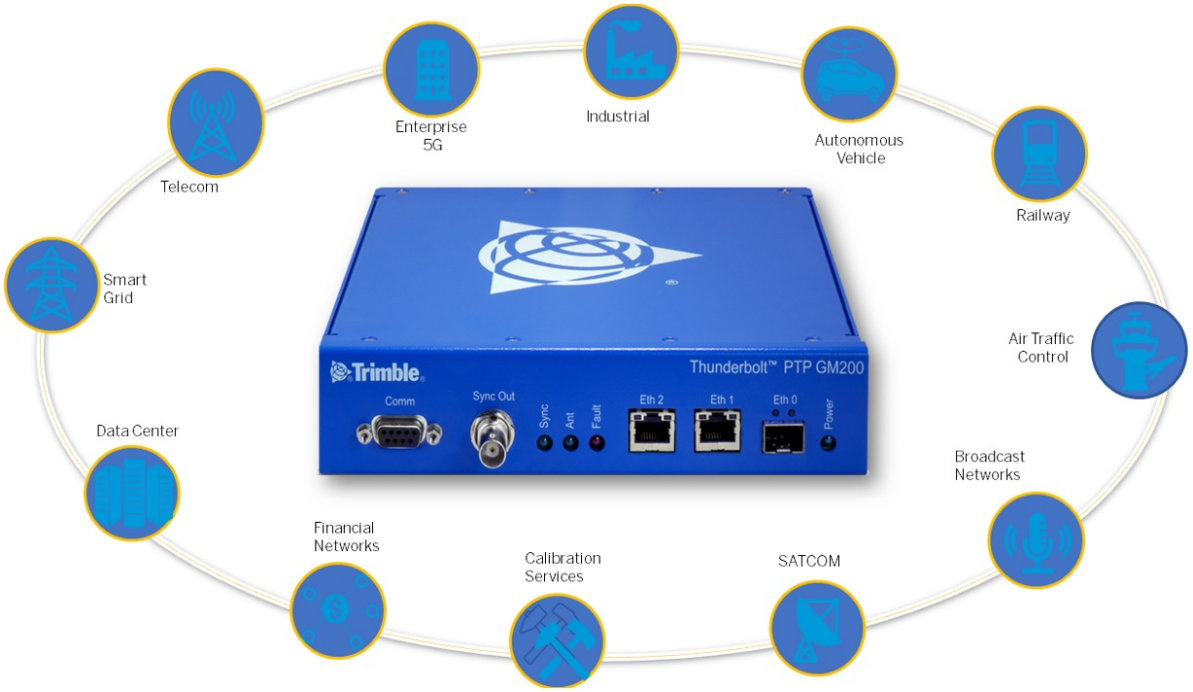
PTP is a packet-based two-way communications protocol specifically designed to precisely synchronize distributed clocks to sub-microsecond resolution, typically on an Ethernet or IP-based network. Defined by *IEEE 1588* standards, PTP provides real-time applications with precise time-of-day (ToD) information and time-stamped inputs, as well as scheduled and/or synchronized outputs for a variety of systems in different industry-specific networks, ranging from LTE/5G-based mobile networks, industrial automation, audio-visual networks, smart grid to transportation, automotive and Industrial Internet of Things (IoT) networking. The Trimble Thunderbolt® GM200 time server offers PTP and NTP enabling backward compatibility with existing network sync infrastructure for the deployments in different vertical industries. It is the industry's most cost-effective grandmaster solution available today. The Thunderbolt GM200 time server is widely deployed in the following industries:

- Smart Grids & Power Utilities: Synchronization is critical to the control and management of power utilities specifically the smart grid infrastructure. The GM200 time server is used in many power utility infrastructures around the globe to provide a highly accurate sync plane for power substations.
- Telecom: The telecommunication infrastructure is undergoing significant changes due to increase packetization and penetration of 5G-led virtualized RAN and software defined network virtualization. The GM200 time server has been a product of choice for

many service providers to augment their existing LTE-A sync planes and provide a highly precise sync plane for 5G-based edge infrastructure.

- Enterprise 5G: With many countries auctioning unlicensed and licensed 5G spectrums for commercial use, a number of new generation service providers have taken the opportunity to offer highly reliable 5G wireless infrastructure for enterprises, which solves many pressing issues such as reliable communications in the healthcare industry and logistics and broadband services for all enterprises. In the USA, the Citizen Band Radio Service (CBRS) is becoming a common choice for enterprise 5G solutions. The GM200 time server is widely deployed in CBRS and similar enterprise 5G use cases in many countries.
- Industrial Networks & Industrial Automation: Much of the industrial network is deterministic meaning high accuracy and reliability of transport are standard. Industrial networks serves as the fundamental conduit to build connectivity infrastructure for industrial and factory automation. A highly precise sync plane is an integral part of deterministic industrial network, and now, the overall transport solution for industrial and factory automation. The GM200 time server has been a product of choice to build highly accurate industrial networks in many countries.
- Autonomous Vehicles: Many elements within autonomous vehicle interconnects require a highly precise sync plane including sensors and LiDAR cameras. The GM200 time server is a product of choice for autonomous vehicle sync plane deployments globally.
- Railways: The signaling and control of high-speed railways requires a new type of network known as Communication-based Train Control (CBTC). Time Sensitive Networking (TSN) is a choice of a sync plane solution for CBTC and for this reason, the GM200 time server has been deployed in many countries to enable a TSN solution for high-speed railways.
- Air Traffic Control: Airports and Air Traffic Control systems need accurate timing to manage airport operations from ticketing systems to clearing airspace and assisting flight landings and departures. Less accurate clocks may provide disastrous consequences for air traffic management and perhaps the overall operations of the airport. When it comes to a cost effective reliable clocking solution, airports and air traffic control systems rely on the GM200 time server. The product has been widely deployed around the world.
- Broadcast Networks: Synchronization is critical to broadcast systems whether it is a mobile or stationary network system. The GM200 time server is deployed in many sports broadcast networks as well a sole source for a clock in head-end systems.

- SATCOM: A highly precise sync plane is essential for control and command centers for satellites communications. The GM200 time server provides unparalleled performance for SATCOM sync plane and is trusted by many customers.
- Calibration Services: Providing a single source for a reliable clock that is both cost effective and essential in calibration and testing services. When it comes to reliability and performance, the GM200 time serverprovides best cost performance choice for a reliable clock in testing services and hence, widely deployed in many calibration services use cases for this purpose.
- Financial Networks: A highly accurate clock is standard in high-performance trading, computing, and many other financial services systems. The GM200 time server provides meets stringent MiFID standards as a highly accurate clock source for financial networks.
- Data Center: Many applications including distributed database systems need highly accurate clocks that are difficult to obtain through NTP-based time distribution. Thus, many data centers choose application-centric sync clusters to provide a highly accurate clock where it is needed. The GM200 time server is both a cost effective and highly reliable clock source for application-centric point of delivery (POD). Additionally, the GM200 time server is a profile-rich device that provides appropriate PTP profiles for different use cases of distributed data centers in various industry verticals.



Today's mission critical infrastructure relies on a highly accurate clock for various clusters within the network infrastructure. The GM200 time server meets and exceeds performance requirements of many industry verticals as edge grand master.

Its price performance is ideal for highly distributed sync plane design. Additionally, the GM200 time server offers 12 hours holdover capabilities and thus guaranteeing a highly precise reliable clock source during network anomalies.

1.1 Product overview

The Trimble® Thunderbolt® GM200/TS200 time server is a Stratum 1 IEEE-1588 PTP grandmaster clock with an integrated Trimble GNSS receiver (*referred to in this document as the time server*). The time server is designed and optimized for the deployment in wireless service provider networks to meet the stringent time and phase requirements of 4G/5G and small cell networks.

It provides NTP, PTP, and Synchronous Ethernet timing protocols. The time server uses GNSS (Global Navigation Satellite Systems) signals from GPS, GLONASS, Galileo, Beidou, and QZSS as the primary time source for synchronization.

The time server can use its built-in, disciplined OCXO (oven controlled crystal oscillator) as autonomous time base for providing several hours of accurate holdover in case that GNSS signals are not available.

Hardware redundancy can be achieved by using two time servers.

The time server comes in a rack-mountable enclosure; two units fit side- by-side in a 1RU height 19″ rack.

1.2 Key features

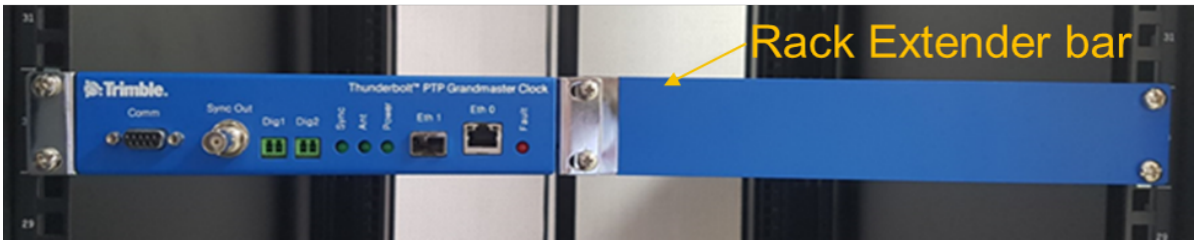
- IEEE-1588 Precision Time Protocol (PTP) grandmaster clock
- Network time server (NTP v4)
- Synchronous Ethernet
- Multi-GNSS receiver (GPS, GLONASS, Beidou and Galileo)
- 1 RJ45 dedicated management port
- 1 RJ45 port (NTP/PTP/SyncE)
- 1 SFP interface (NTP/PTP/SyncE)
- 1 BNC port (PPS and 10 MHz outputs)
- IPv4, IPv6 and VLAN support
- 1 EIA-232 (RS-232) serial port with ToD output (NMEA ZDA or RMC)
- Small foot print – ½ Rack 1U
- SNMP traps
- DC (default) and AC power options
- PTP/SyncE input
- PTP Freerun mode
- PTP APTS mode
- PTP T-BC mode

1.3 Physical specifications

1.3.1 ETSI standard 19" rack mounting

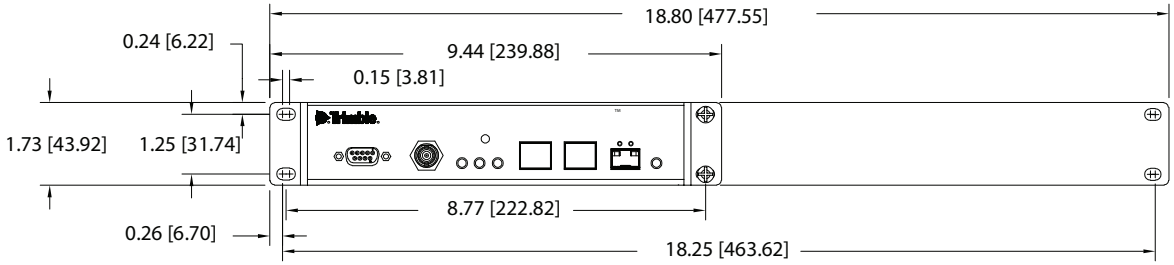
The time server can be installed in a 19" half rack size mount unit with 1U form factor.

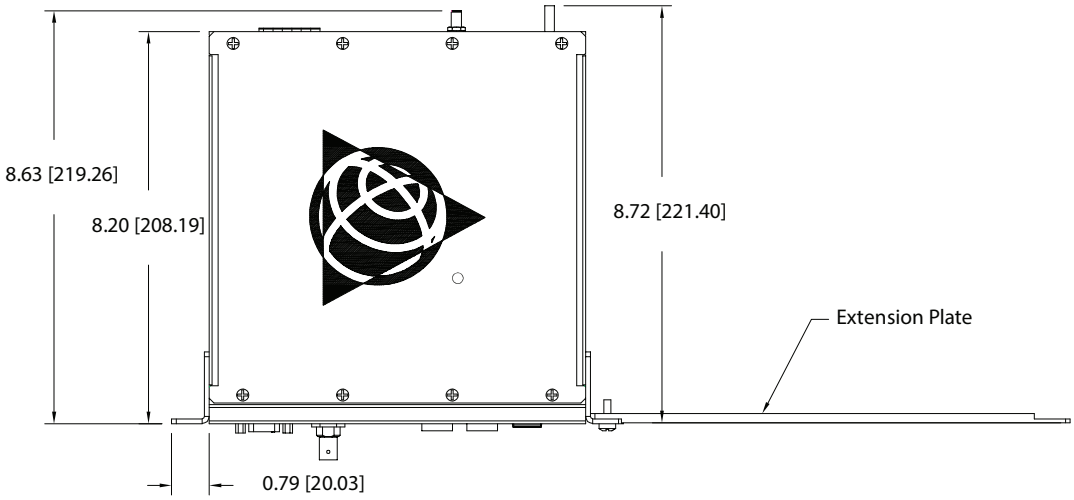
You can install one time server with a rack-mounting extender (included in the product box in the ETSI standard 19" rack)



or two time servers, installed side-by-side in a full-rack space for additional redundancy.

1.3.2 Mechanical spec diagram





1.4 Performance

The time server can support:

- 32 PTP clients at 128 packets per second in most profiles and configurations.

  > NOTE – When IEEE 1588, G.8265, and G.8275.2 profiles are used in unicast, two-step configuration, the time server can support only eight clients at 128 packets per second.

- A maximum of 500 PTP slaves in any profile.
- Up to four VLANs per port. A total of eight VLANs can be configured across the two Ethernet ports.

1.5 Front panel elements

1.5.1 Comm EIA-232 serial port

The EIA-232 (RS-232) serial port provides a craft interface to the time server through an EIA-232 female connector.

1.5.2 Sync out

The time server has a BNC female connector that provides 1PPS output. It can be configured for 10 MHz (see the set output command, page 100).

- PPS Voltage: 3.0 V
- PPS Output Impedance : 50 Ohms
- Default pulse width: 1000 ns
- 10 MHz: Square wave 3.0 V
- 10 MHz: Output Impedance 50 Ohms

1.5.3 Status LED

Alarm and status information is shown through the use of four LEDs. In a critical alarm condition, the dry contact relay output at the rear of the time server is closed.

LED	Color	Indication	Meaning
Power	Green	ON	System is powered on
		OFF	System does not have power
ANT	Green	ON	Reference acquired and tracking
		Blinking, 1/2 Hz	Reference being acquired, or no computing
		OFF	No reference active or antenna

LED	Color	Indication	Meaning
Sync	Green	ON	Locked
		Blinking, 1/2 Hz	Acquisition or Holdover
		OFF	Freerun or startup
Status	Red	OFF	No active alarms
		ON	Critical alarm
		Blinking, 1 Hz	Minor alarm condition
		Blinking, 1/2 Hz	Major alarm condition

1.5.4 Management Port (Eth 2)

The time server has one dedicated management Ethernet port. The RJ45 port provides connectivity to Ethernet LAN for the configuration of the unit.

1.5.5 Ethernet Port (Eth 1)

One RJ45 Ethernet port that provides NTP/PTP connectivity to Ethernet networks.

1.5.6 SFP Port (Eth 0)

The time server supports one SFP port, that provides NTP/PTP connectivity to Ethernet networks.

The following SFPs have been tested by Trimble:

Part Number	Type	Manufacturer
ABCU-5730ARZ	RJ45	Electrical Avago
SFP-1GBT-05	RJ45	Electrical Belfuse
SFP-1GBT-09	RJ45	Electrical w/SyncE Belfuse

1.6 Back panel elements

1.6.1 GNSS antenna connection

The time server has an SMA connector for the antenna input to the embedded GNSS receiver.

1.6.2 Power Input

The standard input power is -48 V DC, 330 mA. The time server provides a 5-pole terminal block to connect dual DC power inputs.

1.6.3 Alarm Relay

The Ttime server provides a 3.81 mm 3-pin terminal header for the dry relay connection. Both Normally Open (NO) and Normally Closed (NC) connections are available to the user. The relay closure is considered closed in Critical alarm condition.

1.6.4 Grounding

The frame ground connection on the time server is available through an M5 grounding terminal stud.

1.7 Use and care

The time server is a high-precision electronic instrument and should be treated with reasonable care. Typically, it doesn't need any care after the first setup. If you need to clean the unit, use a dry non-static tissue or a light moist tissue to remove dust or stain from the enclosure. Ensure that water does not enter anywhere in the enclosure. Do not use solvents, aggressive or abrasive cleaning products anywhere on the time server.

> CAUTION – There are no user-serviceable parts inside the time server. Any modification to the unit by the user voids the warranty.

1.8 Technical assistance

If you have a problem and cannot find the information you need in the product documentation, contact the Trimble technical support at 800-767-4822 or email tsgsupport@trimble.com.

2. Installation

2.1 Getting started

This section explains how to install and configure the time server.

Unpack and inspect the content of the box. The following items are included in the standard box:

- Thunderbolt GM200/TS200 time server
- Mounting brackets and installation accessories
- Dummy plate for a single-unit installation in a 19″ rack

2.2 Mounting the device to a rack

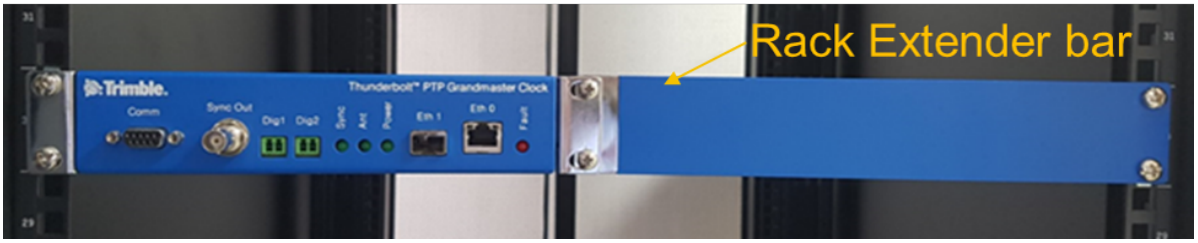
The time server should be installed indoor or outdoor in an environmental controlled cabinet.

ETSI Standard 19 Inch Rack Mounting

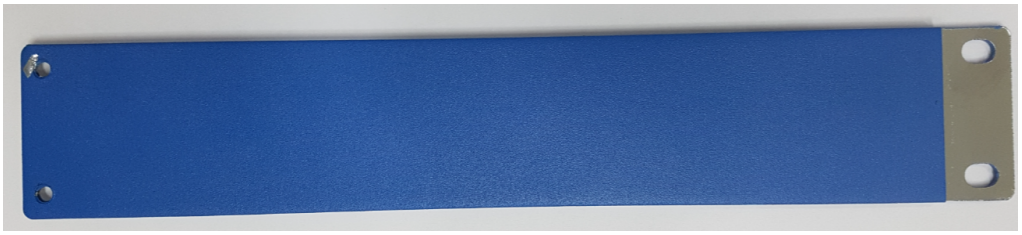
The time server supports 19" half rack size with 1U form factor.

You can install one time server with a rack-mounting extender, included in the product box in the ETSI standard 19" rack, or you can install two time servers side by side.

The following figure shows a single time server installation.



The following figure shows a rack-mounting extender (included in the box).



The following figure shows a dual-time server installation.

NOTE – Forced airflow is not required.

2.3 Connecting power

The time server supports single- or dual-redundant AC or DC power supplies. The standard option is 48 V DC. The unit can operate from -36 V DC to -72 V DC.

The DC input is reverse polarity protected. Reversing polarity with 48 V DC options will not damage the unit and the unit will operate normally.

> NOTE – The power cable should be routed separately from the data (signal) cables.

The table below shows the DC power interface information:

Item	Description	Note
Interface name	DC power	
Connector type	Terminal block	
Number of power inputs	Dual -48 V DC input	
Maximum DC power input range	-36 V DC to -72 V DC	
Maximum AC power Input Range	85 V AC ~ 264 V AC input	With AC/DC power adapter accessory
Overall power consumption	Max 16 W	Normal 8 W
Wiring	Solid Wire: 30 AWG ~ 12 AWG/ 0.05 to 3.3 MM² Stranded Wire: 30 AWG ~ 12 AWG / 0.05 to 3.3 MM² Torque for screws: 4.0 lb-In / 0.45 Nm	Wire stripe length : 9 mm recommended
Power damage protection	• Overcurrent protection • Overvoltage protection • Reverse power polarity input protection • Power line surge protection	

Item	Description	Note
Related alarms generation	No related alarm generation for DC power interface connection and operation	

The time server is powered by -48 V DC with the default power input terminal block.

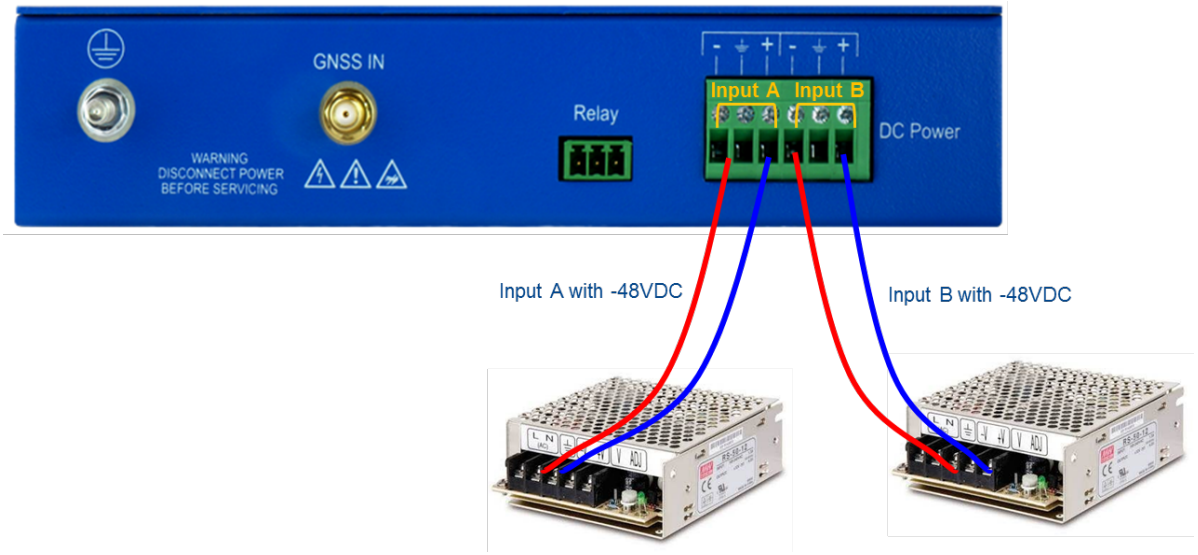
However, if you use a Trimble AC/DC power adapter accessory, you can power the time server with AC power with 100 A ~ 240 V AC range.

The time server does not have any alarms related with power input failure or related operation except for 'Relay' operation.

2.3.1 DC Power connection

The image below shows how to connect dual -48 V DC.

The time server supports reverse power polarity input protection, so you can connect -48 V DC and GND cable to "-" and "+" as a pair to each input terminals without considering order.

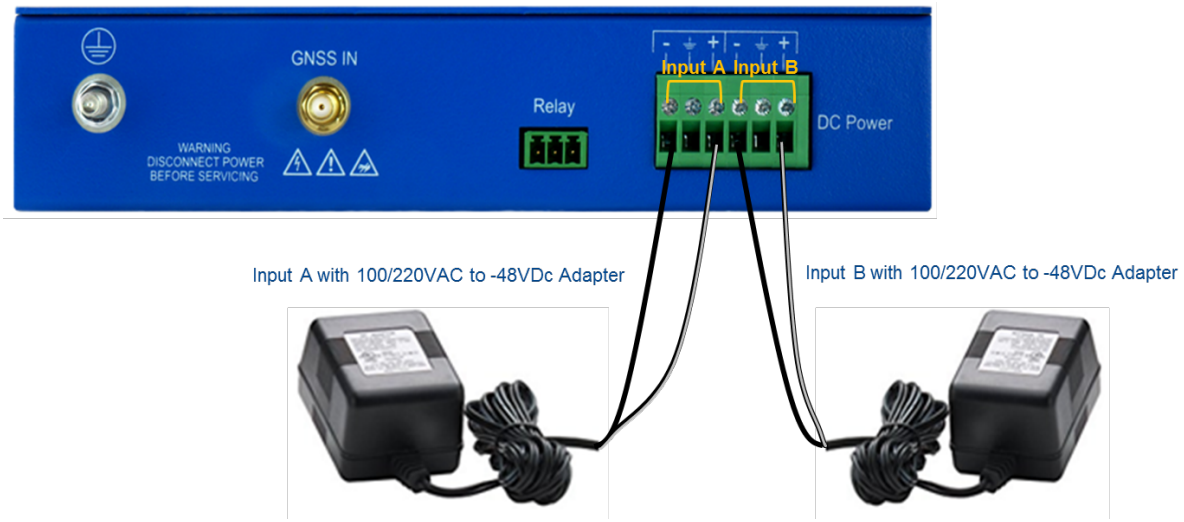


2.3.2 AC power connection

The image below shows how to connect dual 100/220 VAC power.

To supply 100/220 V AC power, you must use the Trimble AC/DC Power Adapter Accessory (P/N TPN 120852).

The time server supports reverse power polarity input protection, so you can connect the two strip lines from AC/DC adapter to "-" and "+" as a pair to each input terminals without considering order.



2.3.3 Grounding the device

The time server M5 terminal stud on the back panel is used for grounding.

The time server is suitable for connection to the Central Office and CPE. The grandmaster clock must be in a restricted access location where only craft personnel are allowed access.

The time server must be grounded via a copper ground conductor. The unit must be installed and connected to the common bonding network (CBN).

All bare grounding connection points to the time server must be cleaned and coated with an antioxidant solution before connections are made.

All surfaces that are un-plated must be brought to a bright finish and treated with and antioxidant solution before connection is made.

All non-conductive surfaces must be removed from all threads and connection points to ensure electrical continuity.

The DC power returns must be treated as DC-I (Isolated from Frame Ground).

The time server requires a ring terminal with a 14-AWG wire that utilizes 15 in-lbs to secure to primary ground.

There are to be no breaks in the outer shield of the GNSS cable.

2.3.4 Powering-Up

After verification of the input power source, switch on the power supply to the time server. The green power LED should turn ON.

2.4 GNSS considerations

For a full description of how to choose the correct antenna cable/antenna combination, see the chapter GNSS Antenna, page 43.

When connected to a GNSS antenna, the time server can receive GNSS signals without user intervention—the factory default is GPS and GLONASS. You can enable Beidou in place of GLONASS or enable single-constellation mode.

The Trimble family of Bullet™ antennas is best matched with the time server. The Bullet antenna has following versions:

- Bullet III — GPS-only antenna
- Bullet GG — GPS and GLONASS antenna
- Bullet L1/L2 — GPS dual-band – L1 and L2 frequencies
- Bullet 40dB — GPS L1 high-gain (40dB) antenna
- Bullet GB — GPS and Beidou antenna
- Bullet 360 — GPS, GLONASS, Beidou, and Galileo antenna

When a GNSS antenna is connected, the antenna LED is green.

2.4.1 Selecting a site for the GNSS antenna

It is important that the GNSS antenna has the fullest possible view of the sky. In most cases, this means installing the antenna on a high point, such as roof top. Avoid overhanging objects such as trees and towers. Also take care to place the antenna away from low-lying objects such as neighboring buildings that may block a portion of the sky near the horizon. If a full view of the sky is not possible, mount the antenna aiming towards the Equator to maximize the southern view of the sky (choose a northern view in the Southern Hemisphere).

Use the criteria below to select a good outdoor site for the antenna. The best locations provide:

- Unobstructed views of the sky and horizon.
- Low electromagnetic interference (EMI) and radio frequency interference (RFI) – away from high-power lines, transmitting antennas, and powerful electrical equipment.
- Convenient access for installation and maintenance.
- Reasonable access for the antenna cable to reach the time server.

2.5 Communication ports

The time server has four communications ports on the front panel:

- 1 × serial port (RS-232)
- 1 × management port autosensing Ethernet (eth2) 10/100/1000 Base-T (RJ-45)
- 1 × traffic port autosensing Ethernet (eth1) 10/100/1000 Base-T (RJ-45)
- 1 × traffic port SFP (Small Form-Factor Pluggable)

Either the serial port or Ethernet eth2 (RJ-45) is the dedicated management port to configure the time server.

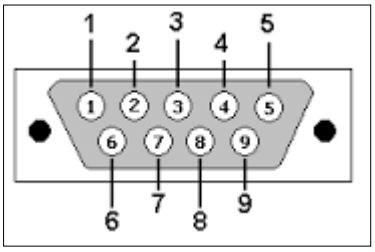
2.5.1 Serial port

A bi-directional EIA standard RS-232 is located on the front panel. The serial port provides access to the command line interface (CLI) for limited status and configuration of the time server.

Use a straight-through cable with the following setting:

Data Rate	115200 baud
Parity	None
Data Bits	8
Stop Bits	1

Serial Port Pin Assignment



Pin	RS-232 Signal	Description on Echo Side
1	DCD	PPS
2	RxD	Data Transmit
3	TxD	Data Receive
4	DTR	Not Used
5	GND	Ground
6	DSR	Not Used

Pin	RS-232 Signal	Description on Echo Side
7	RTS	Not Used
8	CTS	Not Used
9	RI	Not Used

The table below shows the COMM interface:

Item	Description	Notes
Interface Name	COMM	
Connector Type	DB-9	EIA-232(RS-232)
Required cable	USB (v2.0) to serial (DB-9) cable or serial (DB-9) to serial cable (DB-9)	
Usage	Local serial console for CLI TOD output : NMEA-0183 format (selectable RMC or ZDA)	
Related SW tool	Terminal program	Ex., Teraterm, Putty
Serial Configuration	Baud rate : 115,200 Parity : None Data Bits : 8 Stop Bits : 1	
Console ID/PW	Trimblesuper / Tbolt_<Serial Number>	Supervisor level only

2.5.2 Management Ethernet port

The time server supports one 10/100/1000 Base-T Ethernet port that allows connection to standard CAT-5 / CAT-5e / CAT-6 cables with a RJ-45 male connector.

The Ethernet port features an LED that indicates the state of the port. The port is designated as “Ethernet-2”. The user can use this port to gain access to the web interface (HTTPS) or command line interface (TELNET/SSH).

The factory default settings for the Ethernet-2 network port are:

- IP Address: 192.168.2.250
- Mask: 255.255.255.0
- Gateway: 0.0.0.0

The table below shows the Eth2– RJ45 interface:

Item	Description	Notes
Interface Name	Eth2	
Connector Type	RJ45	
Initial operating status	Enabled	
Required cable	Recommended UTP CAT-5E	
Specification	10/100/1000Base-T	
Auto negotiation mode	Supports 1000Base-X auto-nego mode only	
Usage	Management only for remote access	Telent, SSH, web interface, and NMS(SNMP v2c and v3)
Related SW tool	Terminal Program, Trimble web interface and NMS	Ex., Teraterm, Putty
Connection information	Default IP address : 192.168.2.250	Netmask : 255.255.255.0
Connection ID / PW	trimblesuper / Tbolt_<Serial Number>	Supervisor level
Port LED	Left side LED: Link Right side LED: Act	
Related Alarms Generation	Occurred 'Eth-Por2-Down' when Eth2 Link is off Occurred 'Eth-Same-Subnet' when Ethernet interfaces have same IP address in subnet class B	Cleared when Eth2 link is on. Cleared when Ethernet interfaces have a different subnet.

NOTE – If the time server is upgraded from version 1.2.0.0 or lower, the default PW is **trimblesuper** for supervisor level.
After applying the factory configuration, the default password is changed to **Tbolt_<serial number>** in v1.4.0.0.

The 'Eth2' interface is dedicated for management only to connect remote management system such as telnet, SSH, Trimble web interface, and NMS with SNMP v2c/v3.

It supports 10/100/1000Base-T with Auto-nego mode only.

It is recommended to use UTP-CAT5E cable or above.

2.5.3 PTP/NTP/SyncE electrical Ethernet port

The time server supports one 10/100/1000 Base-T Ethernet port that allows connection to standard CAT-5 / CAT-5e / CAT-6 cables with RJ-45 male connector.

The Ethernet port features an LED that indicates the state of the port. The port is designated as "Ethernet-1". For security reasons, this port is not designed for communication purposes. This port is designed for providing NTP/PTP/SyncE.

The factory default settings for the Ethernet-1 network port are:

- IP Address: 192.168.1.250
- Mask: 255.255.255.0
- Gateway: 0.0.0.0

> NOTE – The Ethernet interface should not be connected to a cable longer than six meters. If a distance greater than six meters is required, then the Ethernet interface should be connected to a switch to comply with GR-1089.

The table below shows the Eth1 – RJ45 interface:

Item	Description	Notes
Interface Name	Eth1	
Connector Type	RJ45	
Initial operating status	Disabled	
Required cable	Recommended UTP CAT-6 or CAT-6E	
Specification	10/100/1000Base-T	
Auto negotiation mode	Supports 1000Base-X auto-nego mode only	
Usage	Input and Output for PTP, NTP and SyncE	
PTP Accuracy	ITU-T G.8272 PRTC Class A	

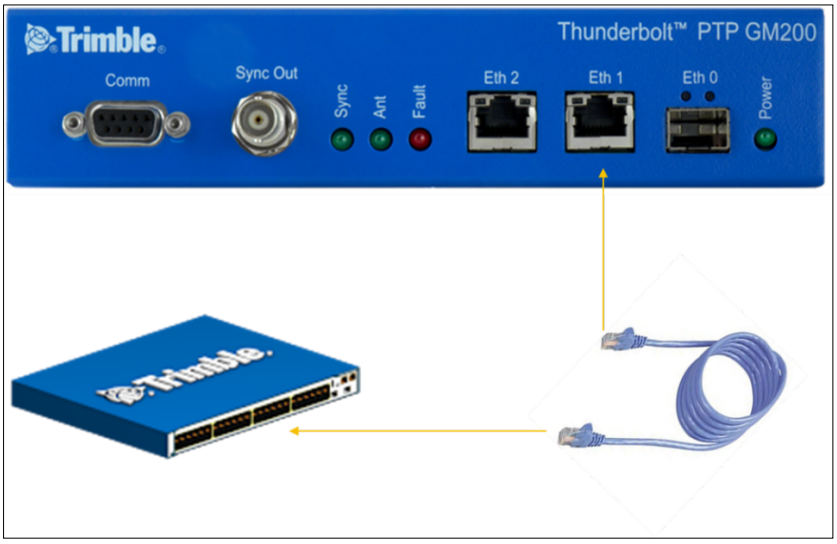
Item	Description	Notes
Port LED	Left side LED: Link Right side LED: Act	
Related Alarms Generation	Default: Ignored, no alarm asserted Asserted 'Eth-Port1-Down' when Eth1 Link is off. Asserted 'Eth-Same-Subnet' when Ethernet interfaces have same IP address in subnet class B.	 Cleared when Eth1 link is on. Cleared when Ethernet interfaces have different subnet.

The Eth1 interface is dedicated for synchronization signal input and output to support PTP (IEEE 1588), NTP, and SyncE.

It supports 10/100/1000Base-T with Auto-nego mode.

It is recommended to use UTP-CAT6 or UTP-CAT6E cable.

When it is linked on, the left side LED on the RJ45 connector indicates for "Link" connection and the right side LED indicates for "Act" states.



2.5.4 PTP/NTP/SyncE SFP Ethernet port

The time server supports one 10/100/1000 Base-T Ethernet port that allows connection to standard CAT-5 / CAT-5e / CAT-6 cables with electrical SFP or fiber cables with optical SFP.

The Ethernet port features an LED that indicates the state of the port. The port is designated as "Ethernet-0". This port is not designed for communication purposes for security reasons. This port is designed for providing NTP/PTP/SyncE.

The factory default settings for the Ethernet-0 network port are:

- **IP Address**: 192.168.0.250
- **Mask**: 255.255.255.0
- **Gateway**: 0.0.0.0

The table below shows the Eth0 – SFP interface:

Item	Description	Notes
Interface Name	Eth0	
Connector Type	SFP	
Initial operating status	Disabled	
Required cable	Single mode or Multi-mode optic fiber	
Specification	1000Base-X	
Auto negotiation mode	Supports 1000Base-X auto-nego mode and 1000Base-X forced mode (auto-nego off mde)	No support for Forced mode on electrical SFP module
Recommended SFP Module	1000Base-SX, LX, BX and electrical SFP (10/100/1000Base-T SFP)	
Recommended SFP module Vendor	**ABCU-5730ARZ**: RJ45 - Electrical (**Avago**) **SFP-1GBT-05**: RJ45 - Electrical (**Belfuse**) **SFP-1GBT-09**: RJ45 - Electrical w/SyncE (**Belfuse**)	
Usage	Input and Output for PTP, NTP and SyncE	To support SyncE with an electrical module, it should be a verified one by Trimble.
PTP Accuracy	ITU-T G.8272 PRTC Class A	
Port LED	Left side LED: Link Right side LED: Act	

Item	Description	Notes
Related Alarms Generation	Default: Ignored, no alarm asserted Asserted 'Eth-Port0-Down' when Eth0 Link is off. Asserted 'Eth-Same-Subnet' when Ethernet interfaces have same IP address in subnet class B.	Cleared when Eth0 link is on. Cleared when Ethernet interfaces have different subnet.

The Eth0 interface is dedicated for synchronization signal input and output to support PTP (IEEE 1588), NTP, and SyncE.

Eth0 supports 1000Base-X with supporting "1000Base-X auto-nego" mode and "1000Base-X forced mode" when the "auto-nego" mode is off based on user configuration.

Also it supports Electrical SFP module to support 10/100/1000Base-T auto-nego mode on SFP interface.

2.5.5 Sync Out

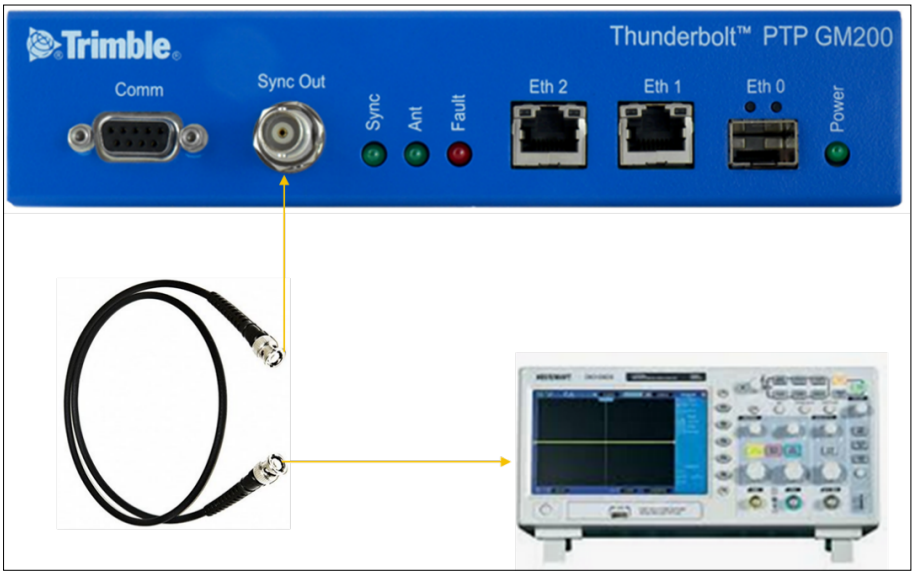
The following table shows the Sync Out interface:

Item	Description	Notes
Interface Name	Sync Out	
Connector Type	BNC (Female), 50Ω	Female type
Specification	3.3 V DC CMOS level	
1PPS Accuracy	± 15 ns (1-sigma) to GPS time	When the time server is locking with GNSS
Required cable and connector	50Ω coaxial cable with BNC (male) connector for the time server side	
Usage	1PPS output (default) or 10 MHz output	By user configuration
Related Alarms Generation	No related alarm generation for 'Sync Out' interface connection	

The Sync Out interface is BNC (Female) connector with 50 Ω.

This interface can output 1PPS or 10 MHz or others as configured by user.

The coaxial cable: use 50 Ω cable with RG-58 or above specification cable in short distance.



2.5.6 Relay Interface connection

Relay 'Open' and 'short' (close) operations are directly related with Alarm operation.

The alarm conditions are: CRI: Critical, MAJ: Major, MIN: Minor and IGN: Ignore.

This Relay interface only reacts when a "CRI" alarm occurred or on Power off; it does not react for MAJ, MIN, and IGN alarms. However, when the time server is in the Holdover mode, the relay reacts as for a "CRI" alarm.

Alarm conditions (CRI, MAJ, or MIN) can energize the relay and are programmable through the user interface.

① & ② Pins

- When Power off or a CRI alarm occurs on the time server, these pins are CLOSED (shorted) with 0Ω.
- When the time server is in normal operation (without any CRI alarms), these pins are OPEN with Ω as NO (normally open).

② & ③ Pins

- When Power off or a CRI alarm occurs on the time server, these pins are OPEN with Ω.
- When the time server is in normal operation (without any CRI alarms), these pins are CLOSED (shorted) with 0Ω as NC (normally closed).

3. GNSS Antenna

A good GNSS antenna and a good installation site is the key to get the best performance from a GNSS receiver.

This chapter explains the requirements for the antenna and provides recommendations for a good installation.

3.1 GNSS antenna requirements

The antenna receives the GNSS satellite signals and passes them to the receiver. The GNSS signals are spread spectrum signals in the 1551 MHz to 1614 MHz range and do not penetrate conductive or opaque surfaces. Therefore, the antenna must be located outdoors with a clear view of the sky. The internal GNSS receiver requires an active antenna with integrated Low-Noise Amplifier (LNA). The received GNSS signals are very low power, approximately -130 dBm, at the surface of the earth. Trimble's active antenna includes a pre-amplifier that filters and amplifies the GNSS signals before delivery to the receiver.

The on-board circuits provide DC supply voltage on the SMA coax connector for the external, active GNSS antenna. The antenna supply voltage is fully protected against short circuit by the on-board Open/Short detection with integrated current limiter. The time server has a full antenna monitoring circuit on board.

3.1.1. Antenna power supply on RF output

Make sure that the current draw of the antenna is above the open circuit and below the short circuit detection thresholds below

Voltage:	+5 V DC +/-0.5 V
Current detection:	Open circuit < 10 mA
	Short circuit > 100 mA

3.1.2 Antenna gain requirements

The time server requires an active GNSS antenna with built-in LNA for optimal performance. The antenna LNA amplifies the received satellite signals for two purposes:

a. Compensation of losses on the cable.

b. Lifting the signal amplitude in the suitable range for the receiver front-end.

Task b) requires an amplification of at least 15 dB, while 20 dB is the optimum for the time server. This would be the required LNA gain if the antenna was directly attached to the receiver without cable in-between.

The cable and connector between the antenna and the receiver cause signal loss. The overhead over the minimum required 15 dB and the actual LNA gain of the antenna is available for task a). So, in case of a 30 dB LNA gain in the antenna, 15 dB are available for compensating losses.

Or in other words, the attenuation of all elements (cables and connectors) between the antenna and the receiver can be up to a total of 15 dB with a 30 dB LNA. With a different antenna type, take the difference between 15 dB and the antenna's LNA gain as the available compensation capability. Subtract the insertion losses of all connectors from the 15 dB (or whatever the number is) and the remainder is the maximum loss, which your cable must not exceed.

As the GNSS signals are hidden in the thermal noise floor, it is very important that the antenna LNA doesn't add more noise than necessary to the system; therefore, a low-noise figure is even more important than the absolute amplification.

Trimble does not recommend having more than 35 dB remaining gain (LNA gain minus all cable and connector losses) at the antenna input of the receiver module. The recommended range of remaining LNA gain at the connector of the receiver module is 20 dB to 30 dB, with a minimum of 15 dB and a maximum of 35 dB.

It is not recommended to use additional amplifiers in the RF path. That includes dedicated inline amplifiers, as well as active splitters with built-in amplifiers. Using additional amplifiers adds noise to the system and that may degrade the performance of the GNSS receiver. It

also increases the risk of overloading the RF front end of the GNSS receiver if the resulting total gain exceeds the recommended gain range.

As a rule of thumb, the satellite signal strength indicators (CNo values) of the strongest satellite signals—usually seen on satellites at a high elevation—should be at, or near, to 48 dBHz and weaker satellites should be seen at lower CNo values to below 20 dBHz.

If none of the satellite signals is ever stronger than 44 dBHz, then check the antenna installation regarding the antenna placement and the cable attenuation. Likewise, if multiple CNo signals are exceeding 52 dBHz and if there are no values in the range of 20 or less, then check the antenna installation for too much overall gain.

3.1.3 Considering coaxial cable loss and delay

The following table shows cable types appropriate for different cable lengths to ensure proper GNSS signal strength. If the time server does not receive the appropriate signal strength, it will not be synchronized with GNSS and it will not provide PTP service for slave devices.

To calculate the **cable loss**:

RF in Gain in the time server: GNSS Antenna Gain - (Surge Protector + adapters + Cable Loss) ≥ 20 dB

Cable type	dB / 100 ft	dB / 100 meter	Max length for 18 dB loss at 1575 MHz (feet/meter)
RG-6	12	40	150/45
RG8 (and 8/U)	9.6	31	185/58
RG-8X	16.8	55	107/33
RG-58	19.6	64	92/28
RG-59	14.7	48.2	122/37
LMR-400	5.3	17.2	340/105
LMR-600	3.4	11.2	530/161

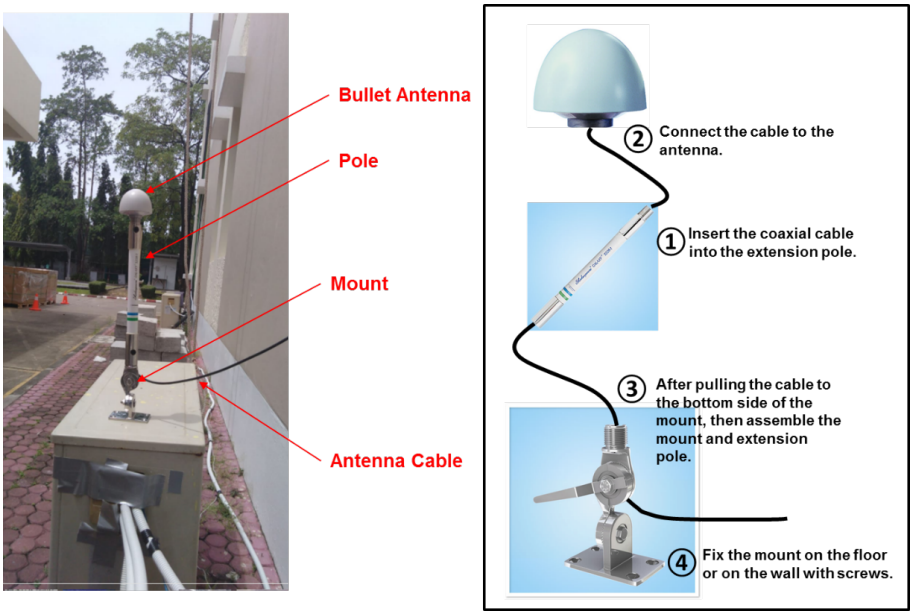
When you use a long coaxial cable, you must also consider the **coaxial cable delay**. Typical delay with RG-59 is around 1.24 ns/ft or around 4 ns/1meter.

You can compensate the cable delay time by using a CLI command.

3.2 Antenna placement

3.2.1 Mounting bracket for GNSS antenna

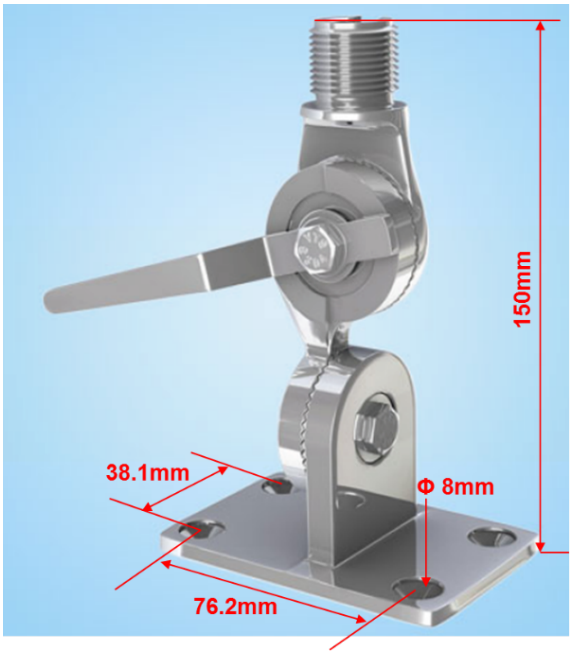
The mounting bracket installation and dimensions for the Trimble Bullet™ 360 antenna are:



The thread specification of the Bullet antenna is a 3/4" NPT thread, dimensions according to ANSI/ASME B1.20.1. It is also called a 1"-14 marine thread, because it has 14 threads per inch.

The Bullet antenna thread should fit both specifications.

In case of an NPT thread with tapered type, the geometry of the thread shape must meet the standard, but the tolerance of the base diameter can be fairly large without violating the standard, due to the conical shape of the thread.



3.2.2 Sky visibility

GNSS signals can only be received on a direct line-of-sight between the antenna and satellite. The antenna should see as much as possible of the total sky.

Seen from the northern hemisphere of the earth, more satellites will be visible in the southern direction rather than in northern direction. The antenna should therefore have open view to the southern sky. If there are obstacles at the installation site, the antenna should be preferably placed south of the obstacles to not block the sky-view to the south.

If the installation site is in the southern hemisphere of the earth, then the statements above are reversed—more satellites will be visible in the northern direction. Near to the equator, it doesn't matter.

Partial sky visibility causes often poor Dilution of Precision (DOP) values due to the geometry of the visible satellites in the sky. If the receiver can only see a small area of the sky, the DOP has a high degree of uncertainty and will be worse compared to a condition with better geometric distribution. It may happen that a receiver is seeing six satellites, all close together, and still get a much worse DOP than a receiver that sees four satellites, but all in different corners of the sky. The receiver's DOP filter rejects fixes with high DOP (high uncertainty), therefore it can take longer to get the first acceptable fix if sky visibility is partly obstructed.

3.2.3 Multipath reflections

Multipath occurs when the GNSS signals are reflected by objects, such as metallic surfaces, walls, and shielded glass for example. If possible, the antenna should not be placed near a wall, window, or other large vertical objects.

3.2.4 Jamming

Jamming occurs when the receiver function is disturbed by external radio frequency (RF) sources that interfere with GNSS signals or saturate the antenna LNA or receiver front-end. A good indicator to detect jamming is switching off all other equipment except the GNSS. Watch the satellite signal levels in this condition. Then switch on other equipment and see if the signal levels go down. A drop of signal levels indicates interference to GNSS from the other equipment. This method cannot, however, detect all possible kinds of jamming. Spurious events are hard to catch. Low frequency fields, like 50 Hz, are unlikely to jam the receiver. Broadband sparks are a potential source of spurious jamming. There is no general installation rule or specification though because the effect of jamming highly depends on the nature of the jamming signal and there are countless potential variations, so it is not possible to standardize a test scenario.

3.2.5 Ground plane

A metal plate or surface under the antenna can block signal reflections from below. This is a good method to mitigate reflections, if the receiver is mounted on high masts or other elevated sites.

3.2.6 GNSS antenna cabling

Trimble recommends low-loss coaxial cabling.

Using any length of coaxial cable will add some time delay to the GPS signal, which affects the absolute accuracy of the computed time solution. The time delay is dependent on the type of dielectric material in the cable, and ranges from 3.3 to 6.5 ns/meter.

The Antenna Cable Delay advances the Hardware Clock slightly to cancel out the signal delay caused by the length of the GPS antenna cable. To calculate the adjustment, select the signal propagation rate for the appropriate cable type and multiply it by the length of the cable.

For example, the standard RG-59 antenna cable has a propagation rate of 4.07 ns/meter. The delay for a 25-meter cable will be 101.75 ns (25 x 4.07 =101.75).

The outer shield on the GNSS cable must be grounded to the chassis via the cable shell to the connector ground on the chassis. The connector ground is tied to the chassis. The chassis is connected to the primary ground, which utilizes a ring terminal with a 14 AWG

wire connected to the rack. There are to be no breaks in the outer shield of the GNSS cable. Reference *ANSI/NFPA 70*, the *National Electrical Code (NEC)*, in particular *Section 820.93*.

> NOTE – The GNSS antenna cable should only be connected when the unit is properly earth grounded.

3.2.7 Lightning considerations

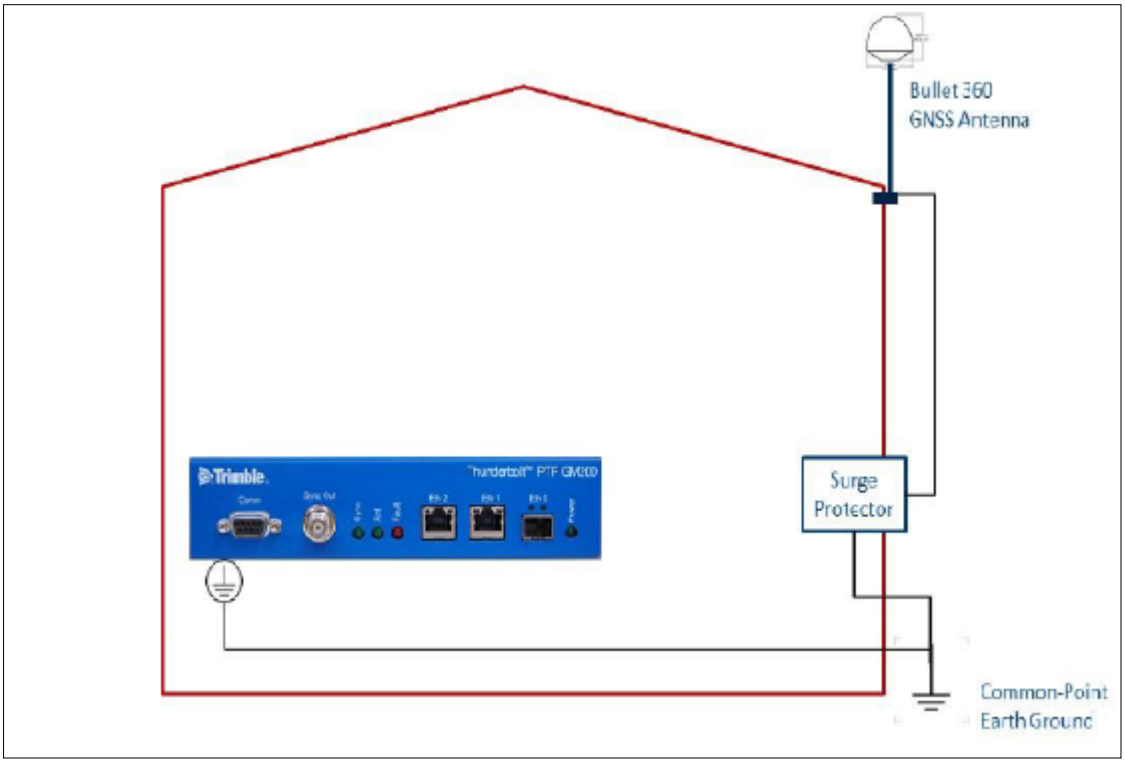
Although you cannot protect the antenna from a direct lightning strike, the connected devices can be protected from secondary effects through protection devices.

Trimble recommends installing an in-line lightning arrestors in the antenna line to protect the receiver and connected devices. In-line lightning arrestors are mounted on a low-impedance ground, between the antenna and the point where the cable enters the building.

3.2.8 Installing surge protection

The surge protection must be installed at the cable entrance into the building with a proper earth/ground connection.

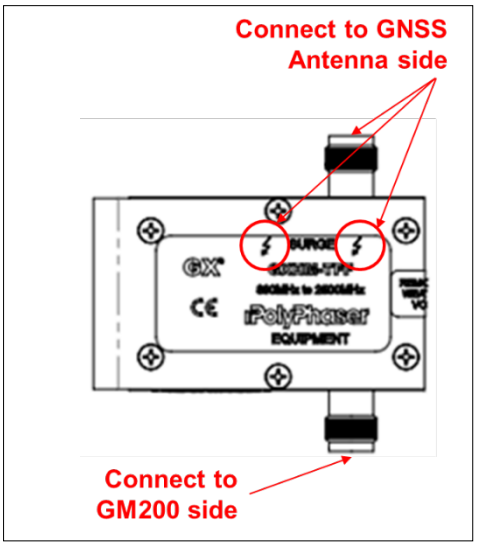
The image below shows how to connect and place the surge protector.



It is recommended to use a minimum 6 AWG (13.3 mm) wire or larger.

> NOTE – Refer to local electrical codes.

The image below shows the direction of coaxial cable connection between GNSS antenna and the time server.



NOTE – Frame GND in the surge protector must be connected properly to a building GND to bypass the surge to the earth GND.

3.3 GNSS tuning settings

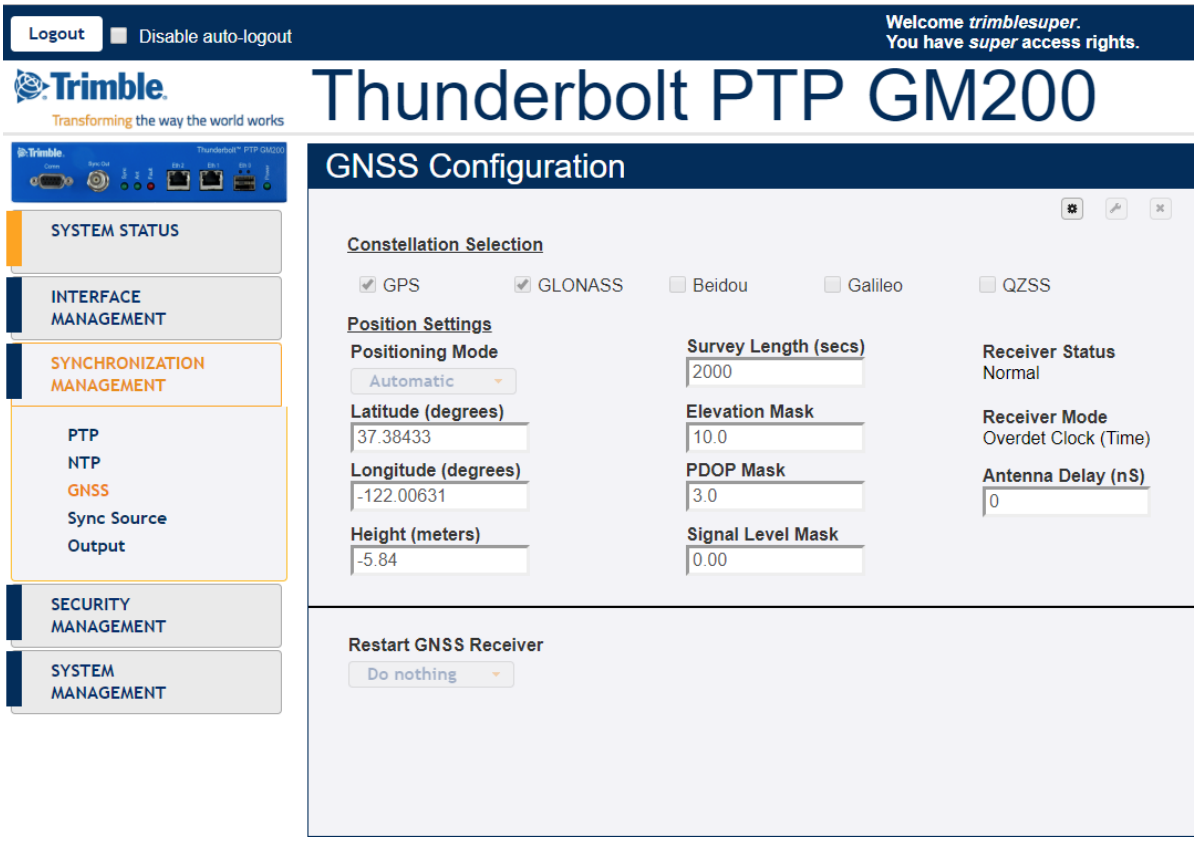
The default GNSS settings are suitable for most installations of the time server. These can include antenna installations with good- or less-than-ideal views of the sky.

The factory settings should not be changed unless there are specific identified reception problems or timing issues. Trimble recommends that you first discuss any changes with your local Trimble representative.

> NOTE – The exception is the Antenna Delay setting that must be changed because it needs to be custom to the specific cable length of the installation.

The tuning settings should only be changed once all the antenna position and cabling instructions listed earlier in this chapter have been followed correctly. The settings can be changed either by using the web interface (see GNSS, page 180) or using the CLI commands (see The get gnss command displays the current settings of the GNSS receiver., page 95 / Use the set gnss command to change the GNSS receiver settings., page 95) .

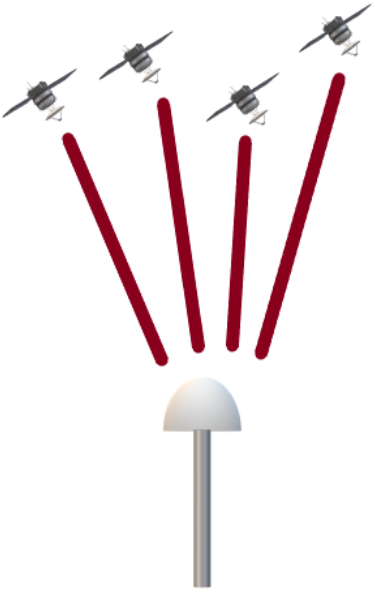
For the following setting descriptions, the **GNSS Configuration** web page for GNSS is used for demonstration purposes. The CLI commands are also available and are described in Command Line Interface Reference, page 69.

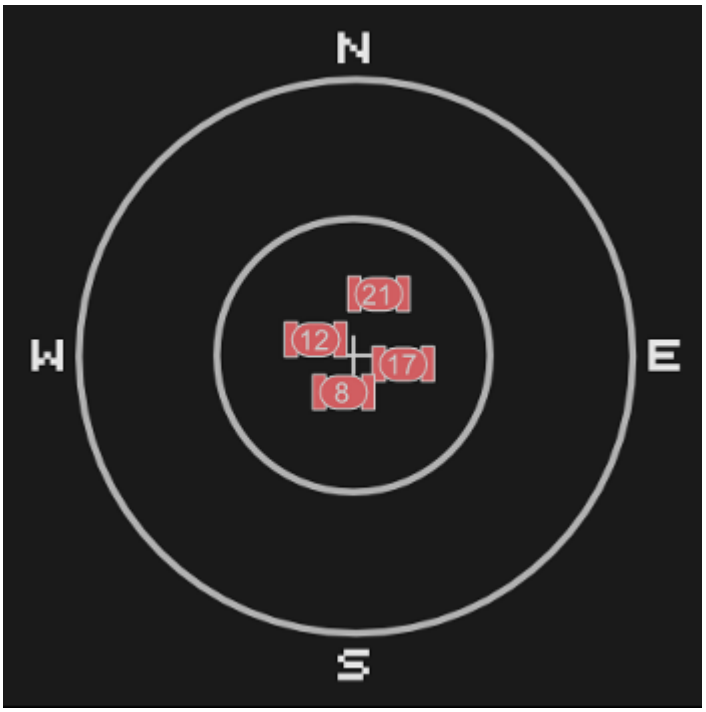


3.3.1 PDOP mask

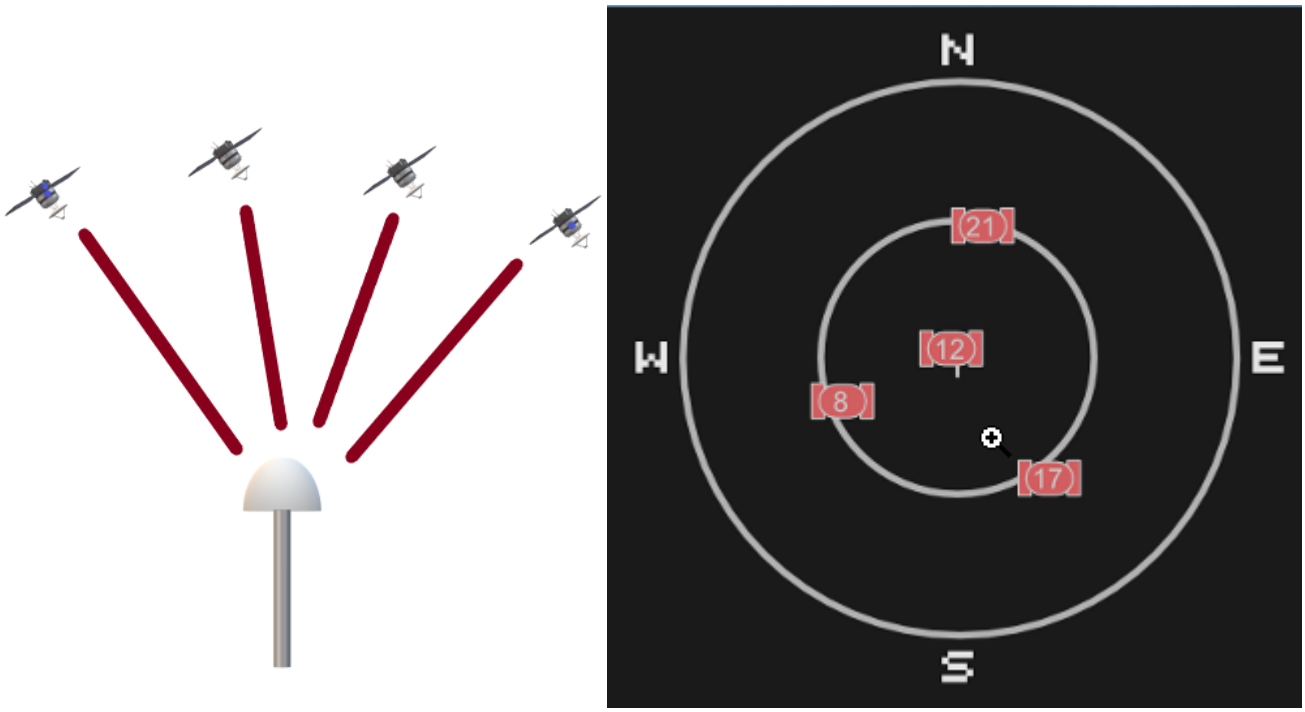
Position Dilution of Precision (PDOP) is a measure of the error caused by the geometric relationship of the satellites used in the position solution. Satellite sets that are tightly clustered together in the sky have a high PDOP and contribute to lower position accuracy. Satellites that when viewed by the receiver are widely separated apart have a low PDOP and contribute to better position accuracy.

Satellites with poor geometry (High DOP):





Satellites with good geometry (Low DOP):



The Dilution of Precision indicates the confidence level of a position fix. Low DOP values indicate a high confidence level, while high DOP values indicate a low confidence level. High DOP values are caused by poor geometry of the visible satellites. Lowering the DOP mask will exclude fixes with poor (high) DOP and will thereby improve the quality of the reference position by only accepting fixes with high confidence level. A too low DOP mask setting may, however, cause extended self-survey times, because less position fixes will pass the mask criteria, so that it takes longer to collect the amount of position fixes to complete the self-survey. The default DOP mask is 3. It is configurable by the user, if needed. For most applications, a PDOP mask of 3 offers a satisfactory trade-off between accuracy and GPS coverage.

Permitted range: 0.0 to 10.0. Default: 3.

> NOTE – PDOP is applicable only during self-survey or whenever the receiver is performing position fixes.

3.3.2 Survey Length

Default value is 2000 seconds. At power-on, the time server performs a self-survey by averaging 2000 position fixes. The number of position fixes until survey completion is configurable. The receiver mode during self-survey is 2D/3D Automatic, where the receiver

must obtain a three-dimensional (3-D) position solution. The very first fix in 2D/3D Automatic mode must include five satellites or more. After a successful first fix, only four satellites are required. If fewer than the required number of satellites are visible, the time server suspends the self-survey. 3D mode may not be achieved when the receiver is subjected to frequent obscuration or when the geometry is poor due to an incomplete constellation.

Once the survey is completed, the receiver automatically moves into over-determined mode, where the average value of the position calculations is saved and used for the timing solution.

Over-determined clock mode is used only in stationary timing applications. This is the default mode for the time server once a surveyed position is determined. The timing solution is qualified by the T-RAIM algorithm, which automatically detects and rejects faulty satellites from the solution.

To improve the consistency of the time solution, the length of the self-survey can be extended to 14400 seconds (four hours). Four hours allows for the satellites to move either completely, or halfway, through their trajectory. That should allow the PDOP to be minimized at least sometime during that period if some of the satellites are blocked. This allows the maximum amount of time that the unit can average a position with what will generally be the best PDOP that is going to be available with the current antenna placement.

The self-survey time can be extended to 86400 seconds (24 hours) that allows the entire constellation to be visible, as well as any diurnal movement due to ionospheric model errors. This will provide a very good position fix average, that will utilize all the satellites that the receiver will observe in the sky over a day. Obviously, 24 hours to wait for Over Determined mode is much longer than the default 33 minutes (2000 seconds). This may be a factor in the user application, but otherwise lengthening the self-survey period can potentially improve our solution.

Permitted range: 60 to 259200. Default: 2000.

3.3.3 Elevation mask

Generally, signals from low-elevation satellites are of poorer quality than signals from higher elevation satellites. These signals travel farther through the ionospheric and tropospheric layers and undergo distortion due to these atmospheric conditions. For example, an elevation mask of 10° excludes very low satellites from position fix computations and reduces the likelihood of potential errors induced by using those signals.

Permitted range: 0.0 to 90.0. Default: 10.

3.3.4 C/No mask

The quality of received GNSS satellite-signals is reported as C/No value (Carrier-to-Noise power ratio). Low C/No values can result from low-elevation satellites, partially obscured signals (for example due to dense foliage) or reflected RF signals (multipath).

Multipath can degrade the position and timing solution. Multipath is commonly found in urban environments with many tall buildings and a preponderance of mirrored glass. Reflected signals tend to be weak (low C/No value), since each reflection diminishes the signal.

If the antenna has a clear view of the sky (outdoor antenna placement), a C/No mask of 35 dB-Hz is recommended for optimal results. However, for indoor use or operation with an obscured view of the sky, the mask must be low enough to allow valid weak signals to be used. For indoor operation, a C/No mask of 0 dB-Hz (zero) is recommended.

Permitted range: 0.0 to 55.0. Default: 0.

3.3.5 GNSS IN interface

This table shows the possible constellation options you can select.

GPS	Galileo	GLONASS	BeiDou	QZSS
√				
	√			
		√		
			√	
√	√			
√		√		
√			√	
√	√			√
√		√		
√			√	√
√				√

If you select a single constellation, then the PPS and Time alignment is automatically set to the same constellation.

4. Startup Operation

When the time server is turned on, it automatically begins to acquire and track GNSS satellite signals.

During the satellite acquisition process, the time server is not in PTP operation mode but in GNSS acquiring mode to establish its accurate position so that it can generate accurate time/phase signals.

In its default configuration, the time server takes around six minutes to lock with GNSS satellites and start operating PTP/NTP if the network configuration is done appropriately and the connected GNSS antenna has a clear view of the sky.

If the connected GNSS antenna is installed in a position with a limited sky view, the PTP operation mode takes longer to enable (up to 30 minutes), depending on the number of valid GNSS satellites that it is tracking.

In cold start, Trimble recommends that the PTP service is started 33 minutes later in OD (Over Determined) mode from the boot up, as the time server should lock with GNSS satellites and calculate accurate position itself during self-survey mode.

4.1 User levels

The time server provides a hierarchy of CLI users that permit an increasing level of access to system parameters.

- User: This is the basic login level. The login ID for this level is “trimble”.
  This only allows for viewing of status, nothing can be changed other than their password.
- Admin: This is the middle level. The login ID for this level is “trimbleadmin”.
  This user can configure everything about the unit, except user accounts.
- Supervisor: This is the highest level. The login ID for this level is “trimblesuper”.
  This allows configuration of everything, including user accounts. By default, this is the Trimble user access level.

> NOTE – See the CLI command Use set user command to update the user configuration. or the Usersection of the web interface.

4.1.1 Initial default login password

> NOTE – There is a change in default password to comply with the *California State Bill SB-327 – Information privacy: connected devices* bill, which requires that the pre-programmed password is unique to each device manufactured. The SB-327 bill is effective since 1 January 2020.
>
> To meet this requirement, Trimble has removed the default **trimble** and **trimbleadmin** accounts. Only the user **trimblesuper** is available by default, with the default password as outlined in this section.

Starting with v1.4.0.0, the unique password is based on the serial number of the unit. The format is:

User name: trimblesuper
Password: Tbolt_<serialnumber>

For example, if the serial number is 1234567890, the password will be "Tbolt_1234567890".

As a 'Best security practices', Trimble recommends changing the default user credentials of the 'trimblesuper' account. If required, the user accounts of 'trimble' and 'trimbleadmin' can be added with unique passwords to allow user and admin level access as were previously available by default.

4.2 Startup configuration

4.2.1 Default configuration values for the time server startup

Default setting of ...	Description	Notes
GNSS constellation	GPS and GLONASS	
Mask	Elevation Mask: 10.0 deg Signal level Mask: 0.0 dB/Hz PDOP Mask : 3.0	
Survey mode (position fix mode)	Automatic	
Self Surveying	2,000 times	Around 33 minutes
GNSS Antenna Power feeding	Enable	5 V DC
GNSS cable delay Compensation	0 (Zero)	
Network Interface IP address	Eth0(disabled): 192.168.0.250, 255.255.255.0 Eth1(disabled): 192.168.1.250, 255.255.255.0 Eth2(enabled): 192.168.2.250, 255.255.255.0	Eth0 and Eth1 are disabled as a default configuration.
PTP configuration	Eth0(disabled): ITU-T G.8275.1 Eth1(disabled): ITU-T G.8275.1	User must enable each PTP interfaces manually after GNSS locking and all related alarm are cleared.
NTP configuration	Eth0: NTPv4 (Only for PN: 111224-10) Eth1: NTPv4 (Only for PN: 111224-10)	Automatically enabled after GNSS locking and all related alarm are cleared.
Required FW version	System : v1.6.0.0 or higher Hardware : v18.3.15 or higher GNSS : v1.5.0.0 or higher	

4.2.2 General conditions for normal startup of the time server

The following parameter values and actions are required in default configuration for a correct PTP/NTP operation startup.

Conditions	Description	Notes
GNSS antenna status	Should be **OK**.	**Open** or **Short** are not valid statuses on start-up.
Required minimum GNSS number for self-surveying after cold start	At least five satellites with > 35 dB each for C/No value.	
Required minimum GNSS number for self-surveying after warm start	At least four satellites with > 35 dB each for C/No value.	
GNSS receiver mode after cold restart	Start with **Self Survey** mode for 33 minute. After **Self Survey** mode, get into **OD** (Over Determined mode).	If the time server is moved over 100 meters away from the first self-surveyed position, it automatically restarts for self-survey.
GNSS receiver mode after warm restart	Start with **OD** (Over Determined) mode after first GNSS tracking.	If the time server is moved over 100 meters away from the first self-surveyed position, it automatically restarts for self-survey.
First GNSS signal receiving time after power-up	Normally less than two minutes after showing the Login prompt in CLI.	
Time of week information	Current GPS time	

Conditions	Description	Notes
UTC Offset	18	In case of cold start, this information shows around 12 minutes after the first GNSS tracking.
Leapsecond status	0	
GNSS receiver status	Normal	
Required minimum GNSS satellite tracking number after OD mode	At least two satellites with > 35 dB each for C/No value.	
First PTP packet generation time (PTP/NTP operation mode Enable)	Normally around six minutes after showing the login prompt in CLI.	With clear sky view for the installed GNSS antenna.

4.2.3 Alarm status for PTP startup of the time server

Alarms are set during the boot-up sequence, because the time server does not receive any GNSS signals in initialization stage.

These alarms are cleared sequentially. When all alarms are cleared in GNSS locking mode, the PTP and NTP operation for both Eth0 and Eth1 are enabled. Then, the time server starts generating PTP/NTP packets.

However, those alarms may be occurring during user operation, based on alarm alert conditions.

Alarms list in the initial status	Description	Notes
GNSS-Comm-Loss	Should be cleared immediately right after the time server boots-up normally	Set at boot-up or can be set during user operation
GNSS-Time-Bad	Should be cleared immediately when the time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation

Alarms list in the initial status	Description	Notes
UTC-Corr-Unk	Should be cleared when the time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
GNSS-Track-No	Should be cleared when the time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
GNSS-PPS-LOSS	Should be cleared when the GNSS antenna is connected normally and when the time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
Time-Set-Bad	Should be cleared when the time server is in GNSS acquiring mode	Set at boot-up or can be set during user operation
Freq-Hold-Exceed	Should be cleared when the time server is in GNSS acquiring mode	Set at boot-up or can be set during user operation
Freq-Hold	Should be cleared when the time server is in GNSS acquiring mode	Set at boot-up or can be set during user operation
Freq-loop-unlock	Should be cleared when the time server is in GNSS acquiring mode	Set at boot up or can be set during user operation
Freq-Out-Bad	Should be cleared when the time server is in GNSS acquiring mode	Set at boot up or can be set during user operation
PPS-Sync-Bad	Should be cleared when the time server is in GNSS locking mode	Set at boot-up or can be set during user operation
Time-sync-Bad	Should be cleared when the time server is in GNSS locking mode	Set at boot-up or can be set during user operation

Alarms list in the initial status	Description	Notes
PTP-System-Bad	Should be cleared when the time server is in GNSS locking mode	Set at boot-up or can be set during user operation
Eth-Port0-Down	Depends on user operating situation	Can be set during user operation
Eth-Port1-Down	Depends on user operating situation	Can be set during user operation
Eth-Port2-Down	Depends on user operating situation	Can be set during user operation

4.3 Initial installation procedure

The table below describes the sequence of the initial installation using the default configuration for a cold start.

Trimble recommends that you ***do not*** add RF splitter(s) between the GNSS antenna and the time server (to distribute the GNSS RF signal to more than one time server), since it can be a weak point at the GNSS reference and location redundancy perspective.

Seq #	Initial installation	Checking and CLI commands	Notes and Check point
1	Install a GNSS antenna at the roof top with a clear sky view.		
2	Install a surge protector between the GNSS antenna and the time server.		
3	Install an appropriate coaxial cable.		
4	Install all required network configuration.		
5	Start the time server.		
6	Login prompt.	Log in	Takes around two minutes after power up
7	Check the system firmware version.	> view version	Check version 1.6.0.0 or later
8	Check the hardware firmware version.	> view version hardware	Check version 18.3.15 or later
9	Check the GNSS firmware version.	> view version gnss	Check version 1.5.0.0 or later

Seq #	Initial installation	Checking and CLI commands	Notes and Check point
10	Check the product information.	> view prodconf	Check ... - Serial number - HW production date - Product option information - Product P/N - Hardware version - other information
11	Check the cable delay configuration.	For adding cable delay compensation: > set gnss adelay [value] For checking applied value: > get gnss	Check 'Antenna delay : [value]'
12	First GPS time showing.	> view freq	Takes less than two minutes from the login prompt - Check current GPS time
13	Check the GNSS 'Acquiring' status.	> view freq	Check 'Mode : Acquiring'
14	Check the antenna status.	> view gnss	Check 'antenna : OK'
15	Check the GNSS signal status.	> view gnss	Check ... - 'Available SVs' number : 5 or more - 'SVs Used' number : 5 or more

Seq #	Initial installation	Checking and CLI commands	Notes and Check point
16	Enable the network interface.	> set network eth0 addr 192.168.0.250 mask 255.255.255.0 bcast 192.168.0.255 > set network eth0 enable > set network eth1 addr 192.168.1.250 mask 255.255.255.0 bcast 192.168.1.255 > set network eth1 enable > set network eth2 addr 192.168.2.250 mask 255.255.255.0 bcast 192.168.2.255 > set network eth2 enable	Or user IP configuration NOTE – Each Ethernet interface MUST have different IP address for Subnet Class B.
17	Check the network configuration.	> get network eth0 > get network eth1 > get network eth2 Or > get network	- Check IP address configuration - Check Status : Connected 1000MB or 100MB or 10MB for each connected interfaces NOTE – If using ITU-T G.8275.1 profile, the IP address should not be an issue since it is an L2 multicast profile.
18	Check the survey mode.	> view pos	Check 'Automatic (2D/3D)' for Self Survey mode
19	Check the OD mode.	> view pos	Check around 33 minutes after the Automatic (2D/3D), showing 'Overdet Clock(time)' for OD mode

Seq #	Initial installation	Checking and CLI commands	Notes and Check point
20	Check GNSS 'LOCK' status	> view freq	Check 'Mode : Lock'
21	Check alarm status	> view alarm	Check for clearing all alarms
22	Set the PTP interface enable.	> set ptp eth0 enable > set ptp eth1 enable	As a default, both Eth0 and Eth1 will be enabled with G.8275.1 profile
23	Check the PTP operation status.	> get ptp Or > get ptp eth0 > get ptp eth1	Check first for both Eth0 and Eth1 with ... - Enabled : Yes - Mode : Master - Clock ID : 001747FFFE7xxxxx-1 - Profile : G8275.1 - Operational Mode : normal - ETC
24	Check the PTP locking status on the PTP slave device.		Check the Master Clock ID in Slave device. It must be same as the time server Clock ID.
25	Finished.		

5. Command Line Interface Reference

This chapter describes the Command Line Interface (CLI) conventions, prompts, features, and command syntax used.

5.1 CLI overview

The Command Line Interface (CLI), also called the ASCII command set, can be used to control the time server from a terminal connected to the RS-232 serial port, or the Ethernet port via Telnet/SSH access.

5.2 Command line format

The command line format is as follows:

```
[action] command [parameter] [data] enter (↵)
```

The type of actions are:

Config	Configure the device parameters
Get	Retrieve specific information
Set	Configure specific system parameters
View	Display system information. This information cannot be altered by the user.

Help is available on the following topics:

help intro	an introduction to the time server
help commands	a list of CLI commands available
help syntax	description of the syntax used in help descriptions
help howto	a list of "how to" help topics
help whatif	a list of "what if" help topics
help alarm	a descriptive list of potential alarm conditions within the system

Help on an individual command is available by typing help and the command name. For example, "help view".

TIP – The time server has an extensive online, user-level context-aware, help system.

NOTE – After any configuration change via the SET command, issue a “config save” command to store the user configuration.

5.3 CLI command set

This section provides details of all CLI commands, by function and describes the topic “help commands”.

> NOTE – After any configuration change via the SET command, you must issue a *config save* command to store the user configuration.

5.3.1 Fault management

Include "alarm" messages.

5.3.1.1 *get alarm*

The *get alarm* command retrieves information about the current system alarm configuration.

Command Syntax:

```
get alarm [ <n> [<n>] . . . ]↵
```

Where:

<n> Alarm number to get configuration. More than one alarm number can be passed. If no number is specified, then the configuration of all alarms is sent.

Level: User, Admin, and Supervisor

5.3.1.2 *set alarm*

The *set alarm* command enables system alarms to be configured.

This is a multi-option command of the format:

Command Syntax:

```
set alarm <n> <level> <settime> <clrtime> ↵
```

Where:

<n> Alarm number to get configuration. More than one alarm number can be passed. If none given, then the configuration of all alarms is sent.

<level>	Alarm level. One of: IGN: This alarm condition is ignored. No indication given. NFY: This alarm condition is a notification only. MIN: This is a minor alarm condition. MAJ: This is a major alarm condition. CRI: This is a critical alarm condition.
<settime>	Alarm set time. The time, in seconds, that the alarm condition must be active before the alarm is asserted. Range is 0 to 86400 (1 day).
<clrtime>	Alarm clear time. This is the time, in seconds, that the alarm condition must be inactive before it the alarm is cleared. Range is 0 to 86400 (1 day).

NOTE – For any entry, but default and <n>, a '-' character may be used to retain the current setting for that entry.

Level: Admin and Supervisor

5.3.1.3 *view alarm*

The *view alarm* command displays the currently active alarms within the system. If there is no active alarm, then the command returns “No active alarms”.

Command Syntax:

```
view alarm <n> <all> ↵
```

Where:

<n>	The alarm number to view
<all>	View all alarms

Level: User, Admin, and Supervisor

5.3.1.4 *get dlog*

The *get dlog* command retrieves the current data logger configuration.

Command Syntax:

```
get dlog ↵
```

Level: User, Admin, and Supervisor

5.3.1.5 *set dlog*

The *set dlog* command allows data logging to be started or stopped.

Command Syntax:

```
set dlog start[holdover]| stop ↵
```

Where:

start	Start the datalogger; if no *holdover* option is given, then the logging will not perform holdover cycling.
holdover	Start the datalogger with holdover cycling.
stop	Stop the datalogger.

Level: User, Admin, and Supervisor

5.3.1.6 *view dlog*

Use the *view dlog* command to display collected data from the datalogger.

Usage:

```
view dlog gnss
```

```
view dlog pos
```

```
view dlog freq
```

5.3.1.7 *download*

Use the *download* command to download log files.

Command Syntax:

```
download[sats|pos|freq]↵
```

Options:

sats	Download TEXT log file of the satellites the receiver has been tracking over time
pos	Download TEXT log file of position information of the receiver over time
freq	Download TEXT log file of the oscillator statistics over time

Level: User, Admin, and Supervisor

5.3.1.8 *view logs*

The *view logs* command displays the system messages. Each message includes the data and time of the event, and a short description of the event itself.

Command Syntax:

```
view logs [<type>] [<level>] [head|tail] [all|-n X] [clear]
↵
```

Where <type> can be one of :

<alarm>	View only alarm log information.
<freq>	View only Time/Frequency control log information.
<gnss>	View only GNSS log information.
<cfg>	View only configuration log information.
<cli>	View only CLI log information.
<comm>	View only communication type log information.
<ptp >	View only PTP log information.
<synce	View only SyncE log information.

Where <level> can be a combination of :

<error>	View only error conditions in the log information.
<warning>	View only warning conditions. These are events that may be significant but are generated by the system in normal operation.
<notice>	View only notice log information. These are normal, but significant conditions.
<info>	View only informational log information. These are normal, but insignificant conditions.

Other options:

<head>	View the beginning of the log (earliest). The default is <tail>.
<tail>	View the end of the log (latest).
<all>	View the entire log.
<-n X>	View only a count of "X" from the log. The default is 20.
<clear>	Clear the system message log. Use this sparingly as any traceability of cause/effect will be lost.

NOTE – System event messages are normally listed with the newest event first. If 'head' is specified, then the oldest event is presented first.

EXAMPLE –

```
view logs -n 10 gnss head
view logs all
view logs clear
```

Level: Admin and Supervisor

5.3.1.9 *view pos*

The *ping6* command displays the position information of the receiver.

Command Syntax:

```
view pos[stream] ↵
```

Where :

stream	View a continuous stream of frequency control data

Level: User, Admin, and Supervisor

5.3.1.10 *view realtime*

Use the *view realtime* command to show/change the current level of the messages display.

This command enables the real-time event message level to be changed for this session (not stored).

The default is level 1 (alarms only).

Command Syntax:

```
view realtime [<level>] ↵
```

Where the <level> value means:

0	No events will be shown in real time
1	Only alarm events will be shown in real time (default)
2	All events will be shown in real time

EXAMPLE –

```
view realtime
view realtime 2
```

Level: User, Admin, and Supervisor

5.3.1.11 *view summary*

The *view summary* command displays a summary of the frequency control, GNSS tracking status, and receiver positioning information.

Command Syntax:

```
view summary ↵
```

Level: User, Admin, and Supervisor

5.3.1.12 *view stream*

The *view stream* command displays a continuous stream of system performance data, which includes frequency control data and GNSS tracking information.

Command Syntax:

```
view stream ↵
```

Level: Supervisor

5.3.1.13 *get syslog*

The *get syslog* command displays the current settings for the syslog server connection configuration. There are no options for this command.

Command Syntax:

```
get syslog ↵
```

Level: User, Admin, and Supervisor

5.3.1.14 *set syslog*

Use the *set syslog* command to configure the syslog server connection. By default, this connection is disabled.

Command Syntax:

```
set syslog [enable/disable] [addr <ip>] [port <port>] ↵
```

Where:

enable	Enable the sending of syslog messages to the syslog server. No messages will be sent until the address is configured with the address of a valid syslog server, regardless of whether the service is enabled or not.
disable	Disable the sending of syslog messages to the syslog server. This does not effect any other settings.

<ip>	Valid IP address for the syslog server. This may be either an IPv4 type address or an IPv6 type address. Only one address type at a time is supported. The corresponding 'source' information in the syslog message will be either the IPv4, or IPv6, address of the Grandmaster, depending on the format of this setting.
<port>	Valid port for the syslog server. Setting of this value allows deviation from the syslog specification. The default port is 514.

EXAMPLE –

```
set syslog enable addr 192.168.2.100
set syslog disable
set syslog port 4022
```

The last example would set the syslog port to a non-standard port for the protocol. This should be used only in controlled environments.

Level: Supervisor

5.3.1.15 *view temp*

The *view temp* command displays the current system temperature in degree Celsius (°C).

Command Syntax:

```
view temp ↵
```

Level: User, Admin, and Supervisor

5.3.1.16 *view gnss stream*

View the current GNSS receiver tracking information as a continuous streaming output. To stop the streaming, press one of the following keys on your terminal:

ctrl-C, q, Q, x, or X.

5.3.1.17 *help whatif*

The *whatif* command gives some information about scenarios you may encounter and how to recover from those.

Command Syntax:

```
help whatif ↵
```

1. You have an FPGA-Load-Bad alarm.

   This indicates an out-of-date FPGA load, which can be fixed by a supervisor level person applying a hardware update load to the system. For more information, refer to config, page 89.

2. You have a PTP-System-Bad alarm.

   This indicates that the PTP system on one, or both, of the Ethernet ports was not able to start. This is usually due to a port not being functional. The **get network** information can be used to get information about the status of the network connections. If a port is unused, then the PTP operation on that port can be changed to disable the PTP operation, which clears the alarm.

Level: User, Admin, and Supervisor

5.3.1.18 *view uptime*

The *view uptime* command displays the current 'up-time' of the system, which is how long the timing system has been operational.

This command takes no options.

Command Syntax:

```
view uptime ↵
```

Level: User, Admin, and Supervisor

5.3.2 Security management

5.3.2.1 *view access*

The *view access* command shows the access level of the current logged in user.

Command Syntax:

```
view access ↵
```

Level: User, Admin, and Supervisor

5.3.2.2 *get auth*

The *get auth* command returns the current authentication settings. You can query specific settings with the options.

Command Syntax:

```
get auth <options> ↵
```

Where <options> are:

local	Get the local authentication settings
tacacs	Get the TACACS+ authentication settings
radius	Get the RADIUS authentication settings

Level: Supervisor

get auth local

The *get auth local* command returns the current settings for the local authentication parameters.

Command Syntax:

```
get auth local ↵
```

Level: Supervisor

get auth tacacs

The *get auth tacacs* command returns the current TACACS+ authentication settings.

Command Syntax:

```
get auth tacacs ↵
```

Level: Supervisor

get auth radius

The *get auth radius* command returns the current RADIUS authentication settings.

Command Syntax:

```
get auth radius ↵
```

Level: Supervisor

5.3.2.3 *set auth*

Use the *set auth* command to change the authentication settings.

This command is a multi-command type.

Command Syntax:

```
set auth <options> ↵
```

Where <options> are:

default	Set the authentication to the default settings.
type [options]	Set the authentication type options. See set auth type.
radius [options]	Set the RADIUS authentication options. See set auth radius.
tacacs [options]	Set the TACACS+ authentication options. See set auth tacacs.
https	Regenerate the HTTPS certificate. This will force web users to re-establish web access with the new certificate. The previous Trimble certificate must be removed from the browser, then the user will need to reconnect to the system with their browser. The certificates valid 'From' and 'To' date range is displayed.

NOTE – You cannot combine authentication <options> on one line, all command variants must be presented separately.

Level: Supervisor

set auth type

Use the *set auth type* command to change the authentication method used for user login. The authentication type is set on a per access portal type.

Command Syntax:

```
set auth type [local[<options>]/radius/tacacs][<portal
type>] ↵
```

Where the authentication type is one of:

default	Set the authentication to the default values, which is local for all portal types.
local	Use only the locally stored username and passwords. These are maintained with the *set user* commands. See set auth local for additional options.
radius	Use RADIUS as the authentication type. The RADIUS configuration can be set with *set auth radius*.
tacacs+	Use TACACS+ as the authentication type. The TACACS+ configuration can be set with *set auth tacacs[+].*
disable	Use to disable a portal. Only telnet may be disabled. To re-enable, select one of the other authentication types.

where <portal type> is a comma separated (only!) list of:

serial	Set the front serial port access to the authentication type. This setting is not valid for RADIUS or TACACS+ authentication types.
ssh	Enable SSH access for the authentication type.
telnet	Enable Telnet access for the authentication type.
web	Enable the webUI to use the authentication type.
snmp	Allow snmp to use the authentication type (experimental). This is not valid for RADIUS or TACACS+ authentication types.
all	This is a unique setting that enables all of the above.

NOTE – Only one authentication type may be set at a time.

This is a 'set' function and the only way to remove a portal assignment from an authentication type is by assigning that to another authentication type. That means that the settings of one type may alter the settings of another type, as only one authentication type may be enabled per portal. That means that if you issue:

```
set auth type local ssh
set auth type radius ssh
```

SSH will be using RADIUS authentication, not 'local'.

EXAMPLE –

```
set auth type local telnet
set auth type disable telnet
set auth type radius ssh,web
```

Level: Supervisor

set auth local

Use the *set auth local* command to configure the local password configuration requirements.

Command Syntax:

```
set auth type [local[<options>] ↵
```

Where <options> are:

minlen <n>	Set the measure of complexity related to the password length (see below for more information). Range: 2 < minlen < 30
lcredit <n>	Set the minimum number of required lowercase letters. Range: |lcredit| < 6
ucredit <n>	Set the minimum number of required uppercase letters. Range: |ucredit| < 6
dcredit <n>	Set the minimum number of required digits. Range: |dcredit| < 6
ocredit <n>	Set the minimum number of required other characters. These characters can be any printable character, except for space. Range: |ocredit| < 6
difok <yes|no>	Set if the user is required to enter a different password when changing their password (default 'yes').

pre <o>	Set a 'preconfigured' password criteria, where <o> can be: p0 : require a minimum of six characters, no other requirements (default). p1 : require at least one uppercase letter. The password must be at least six characters long. p2 : require at least one uppercase and two lowercase letters. The password must be at least six characters long. p3 : require at least one uppercase, two lowercase, and one number. The password must be at least six characters long. p4 : require at least one uppercase, two lowercase, one number and one 'other' character. The password must be at least six characters long.
timeout	Set the TACACS+ server timeout value. 1 to 60 seconds.

Level: Supervisor

Additional information

'minlen' is a measure of complexity, not simply length. It specifies a complexity score that must be reached for a password to be deemed as acceptable. If each character in a password added one to the complexity count, then minlen would simply represent the password length but, if some characters count more than once, the calculation is more complex. How this works is :

The minlen complexity measure is calculated in several steps:

- Every character in a password yields one point, regardless of the type of character
- Every lowercase letter adds one point, up to the value of **lcredit**
- Every uppercase letter adds one point, up to the value of **ucredit**
- Every digit adds one point, up to the value of **dcredit**
- Every special character adds one point, up to the value of **ocredit**

If **lcredit**, **ucredit**, **dcredit** and **ocredit** were all set to 0, only the password length would be used to determine if it is acceptable. No characters would add extra points to the complexity score.

When you set any of the lcredit, ucredit, dcredit or ocredit parameters to a negative number, then you MUST have at least that number of characters for each character class for the password to pass the complexity test.

> NOTE – You can combine settings. For example:
>
> ```
> set auth local p1 dcredit -1
> ```
>
> would set the criteria to be: require at least one uppercase, one digit, and a minimum length of six characters.
>
> Other examples:
>
> ```
> set auth local minlen 12
> set auth local pre p2 minlen 10
> ```

set auth radius

The *set auth radius* command configures the RADIUS server connection information.

Command Syntax:

```
set auth radius <options> ↵
```

Where <options> are:

default	Set the RADIUS server information to defaults.
addr	Set the primary server address for the RADIUS server.
saddr	Set the secondary server address for the RADIUS server.
port	Set the IP port for the RADIUS server (same for primary and secondary).
secret	Set the shared secret value for the RADIUS server (same for primary and secondary). This may contain any 'printable' character. It is recommended that the string is enclosed in "" to allow setting of characters that might be interpreted as parameter separators.
timeout	Set the RADIUS server timeout value. 1 to 60 seconds.

Level: Supervisor

set auth tacacs

The *set auth tacacs* command configures the TACACS+ server connection information.

Command Syntax:

```
set auth tacacs <options> ↵
```

Where <options> are:

default	Set the TACACS+ server information to defaults.
addr	Set the primary server address for the TACACS+ server.
saddr	Set the secondary server address for the TACACS+ server.
port	Set the IP port for the TACACS+ server (same for primary and secondary).
secret	Set the shared secret value for the TACACS+ server (same for primary and secondary). This may contain any 'printable' character. It is recommended that the string is enclosed in "" to allow setting of characters that might be interpreted as parameter separators.
service	Set the TACACS+ server service string.
protocol	Set the TACACS+ server protocol string.
timeout	Set the TACACS+ server timeout value. 1 to 60 seconds.

Level: Supervisor

5.3.2.4 *get auto*

The *get auto* command shows the current status of the auto-logoff setting for this session. The default is to automatically log off this port after approximately five minutes of inactivity.

Command Syntax:

```
get auto ↵
```

5.3.2.5 *set auto*

Use the *set auto* command to control the auto-logoff setting for this session. This allows the port to remain active even beyond the five minute timeout period of inactivity. This is effective only for this session (it is not stored). The default setting is ON.

This is useful when combined with *view realtime* setting to allow monitoring of events.

Command Syntax:

```
set auto [on|off] ↵
```

EXAMPLE –

```
set auto off
```

5.3.2.6 *get user*

The *get user* command retrieves the current user names, access levels, and email addresses for users that are at, or below your, access level.

Command Syntax:

```
get user ↵
```

Level: User, Admin, and Supervisor

5.3.2.7 *set user*

Use *set user* command to update the user configuration.

Command Syntax:

```
set user <adduser / deluser / level / passwd | email |
logout> ↵
```

Where:

adduser <uname> <level>	Add a new user, named <uname>, with access level <level>. <uname> can contain only letters and numbers, no spaces or punctuation is allowed. If the user already exists, no action is taken. <level> can be one of:
	user — This level can only view status and configuration, no changes to configuration.
	admin — All functions of 'user' with added ability to change most configuration settings.
	super — All functions of 'admin' with added ability to edit the user table.
deluser <uname>	Delete a user. You cannot delete yourself. If the user does not exist, an error is returned.
level <uname> <level>	Change the access level for a user. See 'adduser' for descriptions of levels.

passwd	Change the password. If you are changing your own password, you are prompted for your old password first. Only supervisors can change someone else's password. This can accept a username and, if one is given, you can change the password of the user. You will not be prompted for their old password. A blank password is not allowed.
email [<uname>] <email>	Change the email address for user. You will be queried for your password to allow changes. If no <uname> is given, then the current user is assumed. Only supervisors can use the optional '<uname>' parameter. This can accept a username and, if one given, you can change the email address of the user.
logout [options]	Log out the user with the given option selections. See *set user logout* for information about the options.

Level: Supervisor

5.3.2.8 *set user logout*

The *set user logout* command to log users out of the system. Users may log in through various methods on the system; this command allows logging out users with varying selection options.

Command Syntax:

```
set user logout [name (n)] [sid(s)] [service(svc)] ↵
```

Where:

<n>	The name of the user. Logged-in users with the name <n> are logged out. This affects all services and sessions.
<s>	The session ID to log out. Users logged in with this session ID are logged out. This limits the logout to only a single entry, since session IDs are unique. The session ID can be found using the *view user* command (see page 88).
<svc>	The service name to log out. All users connected to this service type will be logged out. This can affect more than one logged-in user; for instance, if a user has multiple logins from the same IP address, this will log out all of the sessions. Note that users with the same name logged in on a different service are not affected.

EXAMPLE –

```
set user logout sid 4

set user logout service 10.1.140.111

set user logout name trimble service 10.1.140.111
```

Level: Supervisor

5.3.2.9 *view user*

The *view user* command retrieves the list of currently logged-in users that are at, or below the current access level.

Command Syntax:

```
view user ↵
```

Level: User, Admin, and Supervisor

5.3.2.10 *quit*

Use the *quit* command to end a CLI session. You can use either "quit" or "q" to end the session.

Command Syntax:

```
quit ↵
```

```
q ↵
```

Level: User, Admin, and Supervisor

5.3.3 Configuration management

5.3.3.1 *config*

Use the *config* command to view, change, and select the time server configuration.

Command Syntax:

```
config <list / load / save / firmware / system> ↵
```

Where:

config list	Output configuration as a list of 'set' commands.
config load	Load the configuration previously dumped.
config save	Stores the current settings for restore on restarting the system.
config firmware	Utilities to handle firmware updates and loading.
config system	Restart or reboot the system.

NOTE – The *Config firmware* command is available only at the supervisor level.

Level: Admin and Supervisor

config firmware

Use the *config firmware* command to maintain the firmware versions used by the time server.

Command Syntax:

```
config firmware <list/stage/unstage/update> ↵
```

Additional help on each of the commands is available.

Level: Supervisor

config firmware list

Use the *config firmware list* command to view the currently available packages on the time server.

Command Syntax:

```
config firmware list <refresh> ↵
```

Where:

<refresh>	To rescan of the images available on the system

The list will show a unique ID for the firmware and the firmware file name. The ID is to be used to refer to the firmware in the *config firmware update* command.

Level: Supervisor

config firmware

Use the *config firmware* command to upload and activate the firmware.

Command Syntax:

```
config firmware <options> ↵
```

Where <options> are:

<download>	Use the *config firmware download* command to download and verify the image through an already configured setup. Please see *get update* (page 108) and *set update* (page 107) for available settings. Those settings must be completed first.
<activate>	Use the *config firmware activate* command to install the already downloaded and verified image in non-active rootfs partition. If this command is successful, the device will reboot so the newly updated firmware will be activated.
<revert>	Use the *config firmware revert* command to revert to the previous firmware (if available in the non-active rootfs partition).

NOTE – The firmware update restarts the system, which will cause a loss of network timing output.

EXAMPLE –

config firmware download

config firmware activate

Level: Supervisor

config load

Use the *config load* command to reset the time server configuration.

Command Syntax:

```
config load [user | factory | default] ↵
```

If no options are given, this command will prompt for an upload as generated by the *config list* commands.

If one of the options is given, then the appropriate settings are loaded.

NOTE – For security reasons, the list command and subsequent upload cannot be used to restore user settings.

IMPORTANT NOTE! – If the **factory** settings are loaded, then all users are removed and the 'trimble' user is restored.

IMPORTANT NOTE! – If the **default** settings are loaded, then all users are removed, current network settings are retained, and the 'trimblesuper' user is restored.

Level: Admin and Supervisor

config list

Use the *config list* command to output the configuration as a list of CLI commands.

Command Syntax:

```
config list ↵
```

You can make a backup of the configuration by issuing a list command and using copy and paste in your window to save the configuration to a file on your local PC. You can restore the configuration by opening a CLI session, issue a *config load* command and then "pasting" the list of commands saved earlier.

NOTES –

1. For security reasons, the list command and subsequent upload cannot be used to restore user settings.
2. The list command and subsequent upload cannot be used to restore the network settings.
3. To avoid network conflicts on a subsequent load, the *config list* command does not output the current Ethernet settings.

Level: Admin and Supervisor

config save

Use the *config save* command to save the current settings to the user settings. This allows operational changes from the factory settings, which can still be restored through the *config load* command.

Command Syntax:

```
config save ↵
```

This saved configuration will be loaded if the *config load user* command is issued.

Level: Admin and Supervisor

config system

Use the *config system* command to restart or reboot the system.

Command Syntax:

```
config system <options> ↵
```

Where <options> is one of:

reboot	Completely reboot the system. This performs a hardware reset of the system. This is very similar to the 'restart' option with the only difference being that the entire system is restarted, which means that all drivers, etc., are restarted on the system.
debuglog	Download a debug file for Trimble engineering. This file will be sent with the Z-Modem protocol. Send the resultant file to Trimble support when requested to help debug issues.

Level: Supervisor

5.3.3.2 *get comm*

The *get comm* command retrieves the current communication port settings.

Command Syntax:

```
get comm ↵
```

Level: User, Admin, and Supervisor

5.3.3.3 *set comm*

Use the *set comm* command to configure the port settings.

Command Syntax:

```
set comm [default] [baud <baud> ] [tod [type <t] [delay
<d>]
```

> NOTE – The **default** must be used by itself and restores the comm settings to their default values. The default baud rate is 115.2kbps-8-N-1.

Where:

<baud>	The baud rate. Valid rates are: 9600, 19200, 38400, 57600, 115200 and 230400.

tod <t>	Sets the serial port to output TOD on demand. This is used with the PPS output on the serial port (on the DCD pin). Option <t> selects the output type and can be one of: • **none**: Disable the TOD output (default) • **rmc**: Set NMEA RMC output • **zda**: Set NMEA ZDA output
delay <d>	Set a delay for the TOD output in µs. This delays the TOD message for <d> µs after the PPS. NOTE – When TOD is enabled, the TOD output will come out regardless of any other use of the serial port (i.e., system control).

NOTE – The setting does not affect the baud rate of the port if a user is currently logged into that port. The port baud rate changes once the user has logged out.

EXAMPLE –

```
set comm default
set comm baud 19200
set comm tod zda delay 1000
```

Level: Admin and Supervisor

5.3.3.4 *get date*

The *get date* command retrieves the current system date.

Command Syntax:

```
get date[full] ↵
```

Use the *get date full* command to retrieve the current system date and UTC time. The format of the output is:

B d Y [hh:mm:ss].

Where:

B	The full month string
d	The day of month (00-31)
Y	The full year, including century
hh:mm:ss	The time, returned only with the *full* option

Level: User, Admin, and Supervisor

5.3.3.5 *get freq*

Use the *get freq* command to retrieve the current operating mode of the control system.

Command Syntax:

```
get freq ↵
```

Level: User, Admin, and Supervisor

5.3.3.6 *set freq*

Use the *set freq* command to set the current operating mode of the control system. This command is only for testing purposes and is not meant to be used in normal operation.

> NOTE – This is not a 'setting' like other commands. The operational mode of the control system is not stored as part of the unit configuration.

Command Syntax:

```
set freq [halt|hold|lock|resync]↵
```

Where:

halt	Put the control loop into User Halt mode. In this mode, the frequency offset is 'frozen' and no computed compensation of the oscillator performance is used.
hold	Put the control loop into User Hold mode. In this mode, the frequency offset is compensated with the computed oscillator performance. If there is no data available to perform a holdover, then this is the same as 'User Halt'.
lock	Return the unit to normal operation. This does not command the unit to 'Lock' mode immediately, it merely takes it out of 'User Hold' or 'User Halt'; it is not a mechanism to override the operation of the control system.
resync	Command the unit to immediately force the output PPS to align with the current reference. Note that this can cause jumps in time.

> EXAMPLE –
>
> ```
> set freq hold
> set freq lock
> ```

Level: Supervisor

5.3.3.7 *view freq*

The *view freq* command displays the current frequency control information.

Command Syntax:

```
view freq <stream> ↵
```

If the option <*stream*> is used, then the measurements will be printed at a 1 Hz rate for logging. To stop the output stream, press **Ctrl-C**.

Level: User, Admin, and Supervisor

5.3.3.8 *get gnss*

The *get gnss* command displays the current settings of the GNSS receiver.

Command Syntax:

```
get gnss ↵
```

Level: User, Admin, and Supervisor

5.3.3.9 *set gnss*

Use the *set gnss* command to change the GNSS receiver settings.

Command Syntax:

```
set gnss [constellation <c>][elev <E>][level <L>]
[pdop <P>][adelay <d>][pos <p>][antenna [on|off]][restart
<r>] ↵
```

Where:

constellation <c>	Set the current constellation in use by the receiver to <c>, where <c> can be any valid combination of the following, separated by '|': • gps : GPS constellation • glo : GLONASS constellation • bds : Beidou constellation • gal : Galileo constellation • qzs : QZSS constellation (forces GPS on)
elev <E>	Set the satellite elevation mask (degrees) to <E>
level <L>	Set the acquisition/tracking signal level (dBHz) to <L>
pdop <P>	Set the PDOP mask level to <P>

adelay <d>	Set the antenna delay for the system. This affects all timing outputs from the system. The antenna delay setting affects the system time base of the time server. Negative numbers advance the internal time reference, positive numbers retard (delay) the time reference. To compensate for an antenna delay of 500 ns, enter **-500** as the antenna delay setting. <d> is in nanoseconds with a range of +/- 50000000 (50 ms).
pos <p>	Set the receiver position or mode. Where <p> is of the format: {<lat> <lon> <ht>} | auto | survey . Where: <lat> and <lon> are in degrees and <ht> in meters (HAE). NOTE – The position is validated by the receiver for accuracy and, if it is too far out of range (thereby making the timing of the unit inaccurate), the position is recomputed. **auto** sets the unit to not force a user-entered position on startup. If the unit has a stored position, then it is used on startup, with the same validation criteria as used for a user-entered position. **survey** forces the unit to recompute a surveyed position. The surveyed position is then used by the system on the next startup (to speed startup). This also forces **auto** mode. **Dynamic** forces the unit into a continuous position update mode. This allows for limited dynamic operation of the unit. The dynamics allowed are currently under investigation.
slength <s>	Set the survey length. This is the number of position fixes that will be averaged. Only fixes that match other criteria (PDOP) will be used in the average. Acceptable range is from 60 (1 minute) to 259200 (3 days).
antenna [on | off]	Enable/disable the power to the antenna. If power is turned off, then no status is generated, and no antenna alarm conditions are available (they will be cleared).

restart <r>	Restart the receiver using one of the following restart types: • Cold: data transmitted by satellites is cleared then receiver is restarted. • Warm: retain satellite data, just restart receiver. NOTE – The restart option is available at supervisor level access.

EXAMPLE –

```
set gnss constellation gps|bds elev 5 adelay 5000
set gnss pdop 4 elev 10
```

Level: Admin and Supervisor

5.3.3.10 *view gnss*

Use the *view gnss* command to display the current GNSS tracking information.

Command Syntax:

```
view gnss [stream] ↵
```

If the option **stream** is used, then the measurements will be printed at a 1Hz rate for logging. The output stream can be stopped with **Ctrl-C**.

EXAMPLE –

```
view gnss
view gnss stream
```

Level: User, Admin, and Supervisor

5.3.3.11 *help*

Use the *help* command to get an overview of the time server (help intro), to get a list of the available commands (help commands), or to get a description of an individual command.

Help is available for common tasks (HOWTOs), and to answer event or condition related questions (WHATIFs).

Command Syntax:

```
help [intro][commands][set]...[howto <n>] ↵
```

EXAMPLE –

```
help intro
help commands
help set
```

Level: User, Admin, and Supervisor

help howto

The *howto* command provides a list of frequently used tasks and help on the related CLI options.

Command Syntax:

```
help howto <n> ↵
```

Where <n> is a number from 1 to 12:

1 How to get current Alarm status?
2 How to set alarm number 2 with setTime as 2 and clearTime as 1?
3 How to enable Ethernet port 0/1?
4 How to set IP address of 192.168.0.9 on Ethernet 0 port?
5 How to set BNC output of even?
6 How to set periodic output of period 2 and value 1?
7 How to set serial port baud rate to 19200 bps?
8 How to add a new user called trimble1 with an access level of user?
9 How to delete an existing user Trimble?
10 How to change user password?
11 How to restore factory default settings?
12 How to reboot the system?

EXAMPLE –

```
help howto 4
```

5.3.3.12 *help set*

Use the *help set* command to set the system settings.

Command Syntax:

```
help set <alarm/comm/gnss/input/network/output/ptp/user> ↵
```

Level: Admin and Supervisor

5.3.3.13 *get input*

Use the *get input* command to generate a list of the frequency control input candidates.

Command Syntax:

```
get input <input type> ↵
```

Where <input type> is an option from the list:

GNSS	Use the GNSS receiver as source for time/frequency
synce0	SyncE input on interface 0 is valid source for frequency
synce1	SyncE input on interface 1 is valid source for frequency
ptp0	PTP input on interface 0 is valid source for time/frequency
ptp1	PTP input on interface 1 is valid source for time/frequency

If no parameters are passed, the candidacy of all inputs are returned.

EXAMPLE –

```
get input
get input gnss
```

Level: User, Admin, and Supervisor

5.3.3.14 *view input*

Use the *view input* command to display the statistics on the current input sources for frequency control.

Command Syntax:

```
view input <gnss> ↵
```

If no parameters are passed, the statistics for all currently enabled input sources is returned.

EXAMPLE –

```
view input
view input gnss
```

Level: User, Admin, and Supervisor

5.3.3.15 *get output*

The *get output* command returns the current output settings for the system. If no options are given, then all output settings are returned.

Command Syntax:

```
get output [<sel>]↵
```

Where <sel> may be:

bnc Get output settings for BNC output only

EXAMPLE –

```
get output bnc
get output
```

Level: Admin and Supervisor

5.3.3.16 *set output*

Use the *set output* command to set the output signal(s) for the system. If no output signal selection is entered, then all outputs are changed.

If an output is not valid for the given signal, then that output is turned off.

The **invert** (or **falling**) modifier inverts the active state of the output, which affects all levels for the given signal. That means that if the output is set **high** for example, the 'invert' option changes the output to 'low'. The **falling** modifier is an edge trigger.

NOTE – Note that this is a modifier and cannot be used alone.

The **width** option sets the pulse width for both BNC and digital.

NOTE – The 'periodic' output has its own width, set with the *set periodic* command.

The **delay** option allows you to set a delay for the timing. This is used to compensate for cable and other delays. The <d> value is in nanoseconds.

The output delay setting only affects the PPS pulse on the BNC connector. That value does NOT affect the system time base and has no effect on the PTP and NTP timestamps. Negative numbers advance the PPS pulse, positive numbers retard (delay) the PPS pulse. The output delay can be used for application-specific adjustments of the PPS timing, for example, the length of cable that is attached to the BNC output for conducting the PPS pulse signal. It has only a local impact, though. Clients in the LAN network do not see any effect from this value.

The output delay setting has an immediate effect on the PPS pulse. The output delay setting must NOT be used for compensating the antenna delay!

The PPS output alignment is always set to UTC, regardless of the constellation setting. This is because PTP outputs TAI time, which is most easily derived from GPS time, and the PPS alignment for TAI is defined to be UTC.

Command Syntax:

```
get output [<sel>] <off|low|high|pps|even|10mhz|periodic>
[invert|falling] [width <w>] [delay <d>]↵
```

Where <sel> may be:

bnc	Change settings for the BNC output signal

EXAMPLE –

```
set output bnc even
set output pps
```

Level: Admin and Supervisor

5.3.3.17 *get periodic*

The *get periodic* command returns the current settings for the periodic output selection.

Command Syntax:

```
get periodic ↵
```

Level: User, Admin, and Supervisor

5.3.3.18 *set periodic*

Use the *set periodic* command to set the periodic output.

Command Syntax:

```
set periodic [period <p>] [value <v>] [width <w>]↵
```

Where :

period <p>	Set the period for the output in seconds. The smallest value is 2 (otherwise use pps). The largest value is 100000.
value <v>	Set the value for the second count to generate the pulse. This can be from 0 to <p> - 1.
width <w>	Set the pulse width for the periodic output in nanoseconds. The range is 100 ns to 5E8 (1/2 second).

> EXAMPLE –
>
> `periodic period 2 value 1`
>
> The above would set a pulse output every two seconds, on the odd pulse.

Level: Admin and Supervisor

5.3.3.19 *view prodconf*

The *view prodconf* command displays the production configuration information that was set by Trimble manufacturing during production.

Command Syntax:

`view prodconf ↵`

> EXAMPLE –
>
> `view prodconf`

Returns:

Serial number
Build date
Premium bits (*this option is available only to supervisor level users*)
Product ID
Hardware ID
Extended S/N

Level: User, Admin, and Supervisor

5.3.3.20 *get system*

The *get system* command returns the current system wide host settings.

Command Syntax:

`get system ↵`

Level: User, Admin, and Supervisor

5.3.3.21 *set system*

Use the *set system* command to configure the various system wide settings.

Command Syntax:

`set system[<options>]↵`

Where <options> are:

hostname <hn>
: Set the hostname for the system to <hn>. Only the characters '.', '-', 0 to 9, a to z, and A to Z are valid within the hostname. The minimum size of the hostname is one alpha-numeric character. The maximum size of the hostname is 63 characters.

opermode <m>
: Set the operational mode for the system. <m> may be one of:

  gm
  : Grandmaster operating mode.
  PTP is not activated until the system is locked to the GNSS signal and the UTC correction information is available. PTP can be used to improve holdover time. See the APTS description below.

  bc
  : Boundary Clock operating mode.
  In Boundary Clock operating mode, the unit allows for a PTP input to enable steering of the time/freq operation. In BC mode, GNSS operation is suspended.

  freerun
  : Freerun operating mode.
  The PTP protocol is activated as soon as the system has booted, but without GNSS tracking. This means that the PTP timestamps will either be started from the PTP epoch, handset by the user, set from an NTP server (see timesource option), or from GNSS.
  The frequency control will be in Freerun mode until the GNSS tracks and locks. If the GNSS tracks and locks, the PTP timestamps are immediately set to the time based on the GNSS.

apts <e>
: If the unit is in Grandmaster mode, then this allows setting the APTS operation to <e>, where <e> can be 'enable' or 'disable'.

  In Grandmaster mode, GNSS is used as the primary reference source. If the GNSS fails, then APTS allows the unit to use PTP as a frequency source to provide better holdover operation.

ntpip none|<ip>	If the unit is in Freerun mode, then this allows setting of the IP address of an NTP server to use as a source to establish time. <ip> may be an IPv4 or IPv6 address or the keyword 'none'. If set to 'none', the unit will not attempt to establish time from an NTP source. If an IP address is provided, then the server will be queried on system startup to attempt to establish time in the system. If the server is unavailable at system startup, a sync is attempted every 15 seconds for a user settable timeout period (see the **ntpto** option). NOTE – Unlike the NTP server options, the NTP server to be queried is not limited to the timing Ethernet ports and time may be obtained through the management port, if the IP address is in that domain.
ntpto <t>	Set the NTP query timeout to <t> minutes. The default is 15 minutes. <t> has the range of 1 <= t <= 120 to allow the system to attempt to acquire time from an NTP server from one minute to two hours.
inband <e>	Enable/disable inband management, where <e> can be 'enable' or 'disable'. Once enabled, SSH/SNMP/HTTPS can be used with eth0/eth1 to manage the time server.

EXAMPLE –

```
set system hostname GM200.bdg11.flr3
set system opermode freerun ntpip 192.168.2.17 ntpto 60
set system inband enable
```

NOTE – Both Eth0 and Eth1 interfaces become the inband management interface if the inband management is enabled and it uses the current IP addresses of Eth0 and Eth1.

Level: Supervisor

5.3.3.22 *get time*

Use the *get time* command to retrieve the current system UTC time.

Command Syntax:

```
get time [full] ↵
```

If the option 'full', is entered, this returns both the date and time.

Use the *get time full* command to retrieve the current system date and UTC time. The format of the output is:

B d Y <hh:mm:ss>

Where :

B	is the full month string
d	is the day of month (00 to 31)
Y	is the full year, including century
hh:mm:ss	is the current UTC hour, minute, and second

Level: User, Admin, and Supervisor

5.3.3.23 *view uptime*

The *view uptime* command displays the current 'up-time' of the system, which is how long the timing system has been operational.

This command takes no options.

Command Syntax:

```
view uptime ↵
```

Level: User, Admin, and Supervisor

5.3.3.24 *view version*

Use the *view version* command to display the software and hardware version information for the product.

Command Syntax:

```
view version[<hardware|gnss>] ↵
```

Where:

<hardware>	View the hardware version of the time server.
<gnss>	View only the GNSS version.

> EXAMPLE –
>
> `view version view version hardware`

Level: User, Admin, and Supervisor

5.3.3.25 *view*

Use the *view* command to display both the current system status and system level operational information.

Command Syntax:

```
help view <X>] ↵
```

Where <X> can be:

access	View access level for logged in user
alarm	View currently active alarms on the system
dlog	View system data logging information
freq	View current frequency control information
gnss	View current GNSS tracking status
input	View statistics for input sources
logs	View system message log data
network	View network statistics
ntp	View current NTP stats
realtime	Configure the messages shown on this port
ptp	View current PTP stats
pos	View current receiver position information
stream	View a continuous stream of frequency control data
summary	View the frequency, GNSS, and position information with one option
temp	View the current system temperature
uptime	View the current 'up-time' of the system
user	View the current logged-in users
version	View the version information for the unit
prodconf	View the production configuration information
update	View the current update status

EXAMPLE –

```
view
view gnss
view logs
view dlog
```

NOTE – Some view options like logs, stream are visible to admin and/or supervisor levels.

Level: User, Admin, and Supervisor

5.3.3.26 *set update*

Use *set update* command to configure the firmware upgrade settings.

Command Syntax:

```
set update [options] ↵
```

Where <options> are :

defer	<1 or 0>	Enable or disable the deferred update.
remoteip	<ipv4 address>	Set the remote server ipv4 address as xxx.xxx.xxx.xxx.
remoteip6	<ipv6 address>	Set the remote server ipv6 address as x:x:x:x:x:x:x:x.
remoteport	<port number>	Set the remote server's accessible port.
protocol	<scp | http | https | ftp | tftp>	Set the remote server protocol type.
user	<user id>	Set the user id provided to access the remote server. If not necessary, set "any".
pass	<password>	Set the password provided to access the remote server. If not necessary, set "any".
image	<filename>	Set the image file name with its associated path expected to be downloaded.
cert	<cert string>	Saves the cert string passed through the CLI in the file, /rwdata/certs/update.crt. Note that the cert dtring should not have "end of line" characters and it should not contain the first and last lines. The string should also be inside " ". This requires manual modification of user generated cert files.

NOTE – Even though ID and password is not required to log into a firmware download server, "any/any" for ID/PW should be set to complete the configuration. If not, it may not start the firmware upgrade process.

EXAMPLE –

set update remoteip 192.168.1.72

set update remoteip6 2600:1700:c460:7f80:f184:d9c8:11a6:7bd5

set update remoteport 80

set update protocol http

set update user any

set update pass any

set update image /images/gm200.v2.0.pkg

set update defer 1

Level: Supervisor

5.3.3.27 *get update*

Use the *get update* command to generate the current firmware upgrade.

Command Syntax:

```
get update ↵
```

Level: Supervisor

5.3.3.28 *view update*

Use the *view update* command to display the status of the current firmware information and any upgrade information.

Command Syntax:

```
view update ↵
```

EXAMPLE –

```
view update
```

Level: User, Admin, and Supervisor

5.3.4 Network management

5.3.4.1 *get network*

The *get network* command displays the current network interface status.

Command Syntax:

```
get network [interface]↵
```

Where:

interface	(Optional) Is a network interface such as eth0, eth1 or eth2. If no interface is specified, all are displayed.

Level: User, Admin, and Supervisor

5.3.4.2 *set network*

The *set network* command configures the network connection. This is a multi-option command.

Command Syntax:

```
set network [<iface>] [default]|[disable]|[<ip>][autoneg
on|off] | [ip6-disable]
[<vlan>] [bond enable|disable|swap][synce <sop>] ↵
```

> NOTE – To restore the network settings to their default values, the *default* option must be used by itself.

Where:

<iface>	Network interface definition, where <iface> is one of: **eth0** – Network interface Ethernet 0 (timing port) **eth1** – Network interface Ethernet 1 (timing port) **eth2** – Network interface Ethernet 2 (management port) The iface may indicate a VLAN with the form: `<eth0|eth1|eth2|> [.vlanId]`
default	Restore network setting(s) to the default values. This cannot be used with other setting options.
disable	Completely disable this interface. This stops all activity from this interface. The interface is enabled by the command 'enable' or by setting any DHCP or IPAddr for this interface.
enable	Bring a previously disabled interface to the active, or 'up' condition. Note that, if the interface does not have valid parameters set, the interface may still not be usable. Enabling the interface can also be done by setting any DHCP or IPAddr for this interface.
ip6-disable	Disables IPv6 on this interface. Setting any IPv6 option will enable IPv6.
<ip>	IP configuration information for this port. This has the following format: `[dhcp|dhcp6|slaac] [addr <i>] [mask <m>] [gateway <g>] [bcast <bm>] [addr6 <i6>] [gw6 <g6>]`

Where:

dhcp	Sets the port to utilize Dynamic IP Address (Dynamic Host Configuration Protocol) for IPv4.
dhcp6	Sets the port to utilized Dynamic IP Address (Dynamic Host Configuration Protocol) for IPv6. Note that you can have DHCP for IPv6 and static addresses for IPv4 (and vice versa).
slaac	Sets the port to utilize the SLAAC (Stateless Address Auto-configuration) IPv6 address assignment.
<i>	IP address of the port, in xxx.xxx.xxx.xxx format.
<m>	Netmask for the port, in xxx.xxx.xxx.xxx format.
<g>	Gateway/Router IP address for the port, in xxx.xxx.xxx.xxx format.
<bm>	Broadcast mask for the port, in xxx.xxx.xx.xxx format.
<i6>	IPv6 address for the port. This must be in CIDR format, which is the IPv6 address with a /mask value. If no /mask value is given, the default mask size of 128-bits is assumed.
<g6>	IPv6 gateway address for the port. This must be in CIDR format, which is the IPv6 address with a /mask value. If no /mask is given, the default mask size of 128-bits is assumed. The gateway setting can be cleared by setting a CIDR address of "::".

<vlan> VLAN configuration parameters, valid only for non-management, non-VLAN ports, in the format:

```
[vlan <vl>] [prio <p>]
```

Where:

<vl>	Comma separated list of VLAN IDs to use as the current VLAN list. This list replaces any other VLAN list that is currently in use. To disable VLAN on the port, use the special ID of '-1'. This deletes all VLANs associated with this port. Value VLAN ID numbers are from 0 to 4094, with the addition of '-1' to disable the VLAN entirely.
prio	Set the priority byte for the VLAN to <p>. The assigned priority only applies to the specified VLAN interface.
<p>	Can be a number between 0 (lowest) to 7 (highest).

bond <b> Set the bonding for the timing ports. If the interface is given and it is anything other than Eth0, then an error is returned. The bonded ports assume the settings for port Eth0 and that port is made active. Eth1 is put into standby mode.

Where <b>:

enable	If bonding is disabled, then port Eth1 is bound to port Eth0. The settings for port Eth0 become the settings for the bonded port and Eth1 is put into standby. If bonding is already enabled, then this does nothing.
disable	If bonding is enabled, then this disables bonding. If bonding is disabled, then this does nothing.
swap	If bonding is disabled, then this is ignored. If bonding is enabled, then swap the active/standby ports. This puts the currently active port into standby, and makes the standby port active.

<autoneg> Media auto-negotiation enable, only valid for fiber SFP interfaces. This enables/disables 1000BASE-X auto-negotiation.

<sop> Set the syncE options for this interface. This is only valid for non-management ports.

Where <sop>:

off	Disable syncE operation for this port.
output	This port is a syncE output. This port cannot be used as an input source for the loop control.
input	This port is a syncE input. This makes it valid to be selected as an input source for the loop control.

> NOTE – Input is only valid for non-SFP ports.

> NOTE – SyncE is not supported by all SFP types. SyncE output can only be used on optical SFPs, as well as the following electrical SFPs: Belfuse SFP-1GBT-09.

EXAMPLE –

```
set network eth0 addr 192.168.0.9 mask 255.255.255.0 bcast
192.168.0.255

set network eth0 gateway 192.168.0.1

set network eth0 addr6 dead:beef:cafe::1/24 gw6 1234:567:1:1::/24

set network eth1 dhcp

set network eth1 vlan 200,300

set network eth1.200 addr 192.168.1.12 mask 255.255.255.0 bcast
192.168.0.255

set network eth0 vlan -1

set network bond enable

set network eth0 synce output

set network eth1 synce input
```

Level: Admin and Supervisor

5.3.4.3 *view network*

Use the *view network* command to view the current network interfaces statistics.

Command Syntax:

```
view network <eth0 | eth1 | eth2> ↵
```

If no interface name is entered, then statistics for all interfaces are shown.

> EXAMPLE –
>
> ```
> view network
> view network eth1
> ```

Level: User, Admin, and Supervisor

5.3.4.4 *get ntp*

The *get ntp* command displays the current NTP broadcast setting for eth0 or eth1 ports. If no option is given, then all ports are returned. If you want to view the current NTP statistics, then use the *view ntp* command (see page 117).

If NTP broadcast is enabled, then this command returns the broadcast settings, otherwise it will return '**broadcast disabled**'.

Command Syntax:

```
get ntp <eth0 | eth1 | iff> ↵
```

Where:

<iff> If encryption is enabled, then this will show the IFF certificate information to provide to the clients. This is ONLY available if you are connected through a secure connection (SSH or local serial port). Copy the information from the terminal into a file, name the file as shown in the information, and then that distribute the file securely to your clients. (This option is available only at the supervisor level user)

> EXAMPLE –
>
> ```
> get ntp
> get ntp eth0
> get ntp iff
> ```

Level: User, Admin, and Supervisor

5.3.4.5 *set ntp*

The *set ntp* command configures the NTP broadcast information.

Command Syntax:

```
set ntp [<eth0 | eth1>] <options> ↵
```

The port information (eth0|eth1) must be supplied for options marked with an '*'. They are optional on other commands, unless noted.

Where <options>:

disable	Disable NTP for the given port. This stops all NTP traffic for the port.
enable	Enable NTP for the given port. This starts NTP traffic for the port.
default	Restore default settings for the port, if supplied. If no port is supplied, then all ports are affected. This option cannot be used with any other options.
*bcast <ip>|off	Set broadcasting on/off for the port. If an <ip> address is entered, it must be in the same domain as the domain of the port. This is to keep from broadcasting to the whole internet.
*interval <n>	Set the broadcast time interval to <n> where <n> is the broadcast time interval, in seconds to the power of two. For example, a minpoll value of 4 sets the broadcast time interval to 2^4 or 16 seconds. Allowable values are from 4 (16 sec) to 17 (36.4 hours).
*ttl <t>	Set the time-to-live hops to <t>. Allowable values are from 1 to 7, or '-'. Note that a value of '-' sets the default maximum hop value allowed.
encrypt on|off	Set the encryption of the NTP messages on/off.
host (hn)	Set the hostname for the encryption certificate to <hn>. Only the characters '-', '_', 0 to 9, A to Z, and a to z are valid within the hostname. The maximum size of the hostname is 32 characters.
group <gn>	Set the group name for the encryption certificate to <gn>. Only the characters '-', '_', 0 to 9, A to Z, and a to z are valid within the group name. The maximum size of the group name is 32 characters.

peer <pl>	Set the peer list to <pl>. <pl> may be a comma separated list of up to four peers to use. This list must contain no spaces and can be made up of a mixture of IPv4, IPv6, or valid hostnames. The other allowable <pl> option is '-', which disables peering (regardless of where it is in the list).
iff	This renews the IFF certificate for NTP certification. You should do this approximately every 30 days to keep the certificate valid.

EXAMPLE –

```
set ntp eth1 bcast 10.1.140.225 interval 4

set ntp eth0 encrypt on host Trimble group MyGroup1

set ntp peer 192.168.0.80,10.1.140.80,time.nist.gov
```

NOTE – Any changes to NTP configurations requires the shutting down and restarting of NTP.

NOTE – IP address changes (as through DHCP) are not service disrupting to NTP.

NOTE – NTP encryption is the public key authentication (autokey).

Level: Admin and Supervisor

5.3.4.6 *view ntp*

The *view ntp* command displays the current NTP status.

Command Syntax:

```
view ntp [stream]↵
```

If the option "stream" is entered, then the measurements will be printed at a 1 Hz rate for logging. The output stream can be stopped with Ctrl-C.

> EXAMPLE –
>
> ```
> view ntp stream
> ```

Level: User, Admin, and Supervisor

The Status word is a 16-bit word, shown in hex, arranged as:

Leap	Source	Count	Event

Below is the descriptions of the fields.

The Leap field displays the system leap indicator bits, coded as follows:

Code	Message	Description
0	leap_none	normal synchronized state
4	leap_add_sec	insert second after 23:59:59 of the current day
8	leap_del_sec	delete second 23:59:59 of the current day
C	leap_alarm	never synchronized

The Source field displays the current synchronization source, coded as follows:

Code	Message	Description
0	sync_unspec	not yet synchronized
1	sync_pps	pulse-per-second signal (Cs, Ru, GPS, etc.)
2	sync_lf_radio	VLF/LF radio (WWVB, DCF77, etc.)
3	sync_hf_radio	MF/HF radio (WWV, etc.)
4	sync_uhf_radio	VHF/UHF radio/satellite (GPS, Galileo, etc.)
5	sync_local	local timecode (IRIG, LOCAL driver, etc.)
6	sync_ntp	NTP

7	sync_other	other (IEEE 1588, openntp, crony, etc.)
8	sync_wristwatch	eyeball and wristwatch
9	sync_telephone	telephone modem (ACTS, PTB, etc.)

The **Count** field displays the number of events since the last time the code changed. Upon reaching 15, subsequent events with the same code are ignored.

The **Event** field displays the most recent event message, coded as follows:

Code	Message	Description
00	unspecified	unspecified
01	freq_not_set	frequency file not available
02	freq_set	frequency set from frequency file
03	spike_detect	spike detected
04	freq_mode	initial frequency training mode
05	clock_sync	clock synchronized
06	restart	program restart
07	panic_stop	clock error more than 600 s
08	no_system_peer	no system peer
09	leap_armed	leap second armed from file or Autokey
0a	leap_disarmed	leap second disarmed
0b	leap_event	leap event
0c	clock_step	clock stepped
0d	kern	kernel information message
0e	TAI	leapsecond values update from file
0f	stale	leapsecond values new NIST leapseconds file needed

In example, with GNSS, the NTP status changes to 0115, which means:

There are no leap second events pending, we are synchronized to a PPS signal, there has been 1 event update: the clock is synchronized.

5.3.4.7 *ping*

Use the *ping* command to validate a route to another IP system on the network.

Command Syntax:

```
ping[eth0|eth1|eth2] <ipaddr> ↵
```

Where :

<eth0>	Network interface Ethernet 0
<eth1>	Network interface Ethernet 1
<eth2>	Network interface Ethernet 2
<ipaddr>	Valid IPv4 address of the unit, in xxx.xxx.xxx.xxx format

NOTE – If no port is given, then the management port is assumed. Because the ports may be on separate physical networks, you need to ensure that you are using the network interface corresponding to the device you are attempting to ping. If you have a VLAN in Eth0 or Eth1, set the Ethernet port number and VLAN ID as in the example.

EXAMPLES –

```
ping eth1 192.168.1.10
ping eth1.100 192.168.1.100
```

Level: User, Admin, and Supervisor

5.3.4.8 *ping6*

Use the *ping6* command to validate a route to another IP system on the network.

Command Syntax:

```
ping6[eth0|eth1|eth2] <ipaddr> ↵
```

Where :

<eth0>	Network interface Ethernet 0
<eth1>	Network interface Ethernet 1
<eth2>	Network interface Ethernet 2
<ipaddr>	Valid IPv6 address of the unit without any mask information

NOTE – If no port is given, then the management port is assumed. Because the ports may be on separate physical networks, you need to ensure that you are using the network interface corresponding to the device you are attempting to ping. If you have a VLAN in Eth0 or Eth1, set the Ethernet port number and VLAN ID as in the example.

EXAMPLES –

```
ping6 eth1 2200:1::10
ping6 eth1.100 2200:1::100
```

Level: User, Admin, and Supervisor

5.3.4.9 *get ptp*

The *get ptp* command returns the current user settable PTP settings. If a valid profile has been selected, then this command only returns the parameters that are outside the default settings for that profile.

If you want to view the current PTP operation, then use command *view ptp* (see page 126).

Command Syntax:

```
get ptp <eth0/eth1> ↵
```

If no option is given, then all port settings are returned.

Level: User, Admin, and Supervisor

5.3.4.10 *set ptp*

The *set ptp* command configures the PTP interface.

Command Syntax:

```
set ptp [<eth0 | eth1>] <options> ↵
```

Where <options> are:

default	Restore the default settings for the user profile.
disable	Disable this PTP port. PTP on the interface must be disabled before any configuration changes are allowed.
enable	Enable this PTP port. By default, all ports are enabled.
mode <m>	Set the current clock mode. <m> may be one of:
	master — This port is to operate as a GM output.
	slave — This port is to operate as a slave clock, making this available to be selected as an input.
	Setting the current clock mode is valid only if the unit is configured for Boundary Clock operation.
	When the unit has been configured for Boundary Clock operation setting, one port mode automatically sets the other port to the opposite. For example, if the BC mode is enabled, setting eth1 to "slave" automatically sets eth0 to "master".
profile <p>	Set the current profile, <p> may be one of:

	g.8275	Select the G8275.1 profile. This profile cannot be used with VLAN and PTP.
	g.8275.1	Select the G8275.1 profile. This profile cannot be used with VLAN and PTP.
	g.8275.2	Select the G.8275.2 profile.
	g.8265	Select the G.8265.1 profile, with Option-II clock class output.
	g.8265.1	Select the G.8265.1 profile, with Option-I clock class output.
	1588	Select IEEE-1588 operational defaults.
	power	Select the Power (C37.238 2011) profile.
	smpte	Select the SMPTE (ST-2059-2) profile.
	telecom	Select the IEEE-1588 Telecom v2 profile .
	enterprise	Select the enterprise (prelim) profile.
	802.1as	Select the 802.1AS (gPTP) profile.
dscp <d>	Set the DSCP (Differentiated Services Code Point) field to <d> for the PTP traffic generated from this port. This may be disabled (default) by either setting <d> to '0' or '-'.	

The following options allow altering profiles. The ability to alter profile settings is determined by the profile selected. In addition, the profile may limit the allowable values.

ai <n>	Set the announce interval.
ar <n>	Set the announce receipt timeout. The number of announce intervals allowed to pass without the receipt of an announce message.
class <n>	Set the clock class.
df <n>	Set the duration field (for unicast grant messages). Range: dependent on profile, absolute range 10 to 1000. Most profiles have a default value of 300.
dm <a>	Set the delay mechanism, may be one of E2E or P2P.
domain <n>	Set the domain number for the profile.
dr <n>	Set the delay request interval.
pdr <n>	Set the pdelay request interval (only some profiles)

grantor <g>

For PTP unicast input profiles only: this allows setting the unicast Grandmasters to use as the 'grantor' for the requests. <g> may be a comma separated list of up to three Grandmasters to use. This list must contain no spaces and be made up of the same transport types (that is, no mixing of IPv6 and IPv4 addresses).

> NOTE – Before the PTP grantor is assigned an IPv6 address, the user must set the PTP Transport to IPv6.

ipmode <a>

Set the IP Mode of operation. <a> may be one of:

multi	Set multicast mode.
uni	Set unicast mode.
hybrid	Set Hybrid mode; allow multicast for GM announcement, but time information is delivered through unicast requests from slave clocks.

pri1 <n>

Set the priority 1 value. This must be a number from 0 to 255.

pri2 <n>

Set the priority 2 value. This must be a number from 0 to 255.

si <n>

Set the sync interval.

sm <n>

Set the step mode. 1 -> one-step, 2 -> two-step.

transport <a>

Set the transport mechanism. <a> may be one of:

IPv4	IPv4 transport.
IPv6	IPv6 transport.
Eth	802.3 transport (not compatible if VLANs are assigned).

ttl <t>

Set the multicast ttl value for the transmission. This setting is only available if the profile selected allows multicast. Any valid TTL may be set (1 to 255) but, realistically, the user should limit their value to be between 1 and 6. Please be aware that a profile may limit the range even further than the 1 to 6 values.

l2mac <a>

Select the layer 2 multicast MAC used:

def	Forwardable MAC (01-1B-19-00-00-00) (default)
alt	Non-forwardable MAC (01-80-C2-00-00-0E)

NOTES –

- Stop the PTP interface before setting up.
- When you configure the APTS or BC mode, the PTP slave port should be configured first and then configure the PTP master port.
- You must reboot the system after the PTP slave mode is enabled.

NOTE – Selecting or changing to a different profile sets all PTP parameters to the default values for the profile, which includes the PTP operational mode.

EXAMPLES –

```
set ptp eth1 disable profile g8275 domain 30 ttl 3

set ptp eth1 profile g2875.2 mode slave grantor 192.168.2.10 ai -3 si -
7 dr -7
```

NOTE – The user must disable PTP on the port where the operational changes are required.

Level: Admin and Supervisor

5.3.4.11 *view ptp*

The *view ptp* command displays the current PTP statistics.

Command Syntax:

```
view ptp <eth0/eth1> <phase/stream> ↵
```

If the option **<phase>** is used, then only the phase offset between the PTP hardware clock and the system clock is returned (for either or both ports).

When a unicast PTP profile is configured, this command shows a list of all PTP slaves taking synchronization from the time server.

> EXAMPLE –
>
> ```
> view ptp eth0
> ```

Level: User, Admin, and Supervisor

5.3.4.12 *get snmp*

The *get snmp* returns the current SNMP settings. SNMP needs to be configured for trap generation and to set the SNMP community strings.

Command Syntax:

```
get snmp ↵
```

Level: User, Admin, and Supervisor

5.3.4.13 *set snmp*

Use the *set snmp* command to configure the SNMP trap information.

Command Syntax:

```
set snmp <options> ↵
```

Where <options> are:

enable	enable SNMP with the current options.
disable	Disable SNMP operation.
v2c <on/off>	Enable/disable v2c agent operations.
	readonly <r> — Set read-only v2c agent community string ID to <r>.
	readwrite <w> — Set read-write v2c agent community string ID to <w>.
v3 <on/off>	Enable/disable v3 agent operations.
authtype <t>	Set the v3 agent authorization type where <t>:
	<none> — No authentication (other than username) is required.
	<auth> — SHA password authentication is required.
	<priv> — SHA password is required and AES encryption is active.
port <p>	Set the port number SNMP.
community <c>	Set the community string ID for SNMP.
readonly <r>	Set the read-only community string ID to <r>.
readwrite <w>	Set the read-write community string ID to <w>.

gentraps	Test generation of all alarm traps (set and clear) that can be generated by the system. No functionality is affected, only the traps are generated. This command cannot be used with any other commands.

EXAMPLE –

```
set snmp enable v2c off v3 on authtype priv

set snmp v2c on v3 off readonly "indivisible" readwrite "diversity"
```

Level: Admin and Supervisor

5.4 List of "How to" help topics

The *howto* command shows a list of frequently used tasks and help on the related CLI options.

The list of frequently used tasks:

1. How do I get the current alarm status?
2. How do I set the alarm of level major, alarm number 2 with setTime as 2 and clearTime as 1?
3. How do I disable Ethernet port 0/1?
4. How do I set an ip address of 192.168.0.9, and set a netmask and a gateway address on ethernet 0 port?
5. How do I set BNC output to even?
6. How do I set the periodic output of period 2 and value 1?
7. How do I set the serial port baud rate to 19200 bps?
8. How do I add a user called trimble1 with an access level of user?
9. How do I delete an existing user trimble?
10. How do I change the user password?
11. What is the password recovery procedure?
12. How do I restore factory default settings?
13. How do I reboot the system?

Command format:

```
help howto <n>
```

Where: <n> is one of the above topic numbers.

EXAMPLE –

```
>
> help howto 1
How to get current Alarm status:
get alarm
>
```

5.4.1 How do I get the current alarm status?

```
get alarm
```

5.4.2 How do I set the alarm of level major, alarm number 2 with setTime as 2 and clearTime as 1?

You must have admin or higher access level.

```
set alarm 2 maj 2 1
```

5.4.3 How do I disable Ethernet port 0/1?

You must have admin or higher access level.

```
set network eth0 disable
set network eth1 disable
```

5.4.4 How do I set an ip address of 192.168.0.9, and set a netmask and a gateway address on ethernet 0 port?

You must have admin or higher access level.

```
set network eth0 addr 192.168.0.9 netmask 255.255.255.0
gateway 192.168.0.1
```

5.4.5 How do I set BNC output to even?

You must have admin or higher access level.

```
set output bnc even
```

5.4.6 How do I set the periodic output of period 2 and value 1?

You must have admin or higher access level.

```
set periodic period 2 value 1
```

5.4.7 How do I set the serial port baud rate to 19200 bps?

You must have admin or higher access level.

```
set comm baud 19200
```

5.4.8 How do I add a user called trimble1 with an access level of user?

You must have admin or higher access level.

```
set user adduser trimble1 user
```

5.4.9 How do I delete an existing user trimble?

You must have supervisor access level.

```
set user deluser trimble
```

5.4.10 How do I change the user password?

```
set user passwd <new_passwd>
```

5.4.11 What is the password recovery procedure?

Disconnect all the Ethernet connections to the time server and then cycle the power.

On startup, the front serial port can be logged into with the username **trimblesuper** and a password **Tbolt_<sn>**, where <sn> is the serial number of the unit.

5.4.12 How do I restore factory default settings?

You must have admin or higher access level.

```
config load factory
```

5.4.13 How do I reboot the system?

You must have supervisor access level.

```
config system reboot
```

5.5 List of "What if" help topics

The *whatif* command provides information about some scenarios you may encounter and how to recover from those.

5.5.1 What if you have an FPGA-Load-Bad alarm

This is an indication of an out-of-date FPGA load.

A supervisor level person applying a hardware update load to the system can remedy this. The supervisor can see config, page 89 section for more information.

5.5.2 What if you have a PTP-System-Bad alarm

This is an indication that the PTP system on one, or both, of the ethernet ports was unable to be started. This is usually due to a port not being functional. The The get network command displays the current network interface status. information can be used to get information about the current status of the network connections.

If a port is known to be unused then an admin can change the PTP operation on that port to disable the PTP operation, which will clear the alarm.

6. Web Interface

This chapter describes the configuration and status pages of the web interface.

6.1 Home page

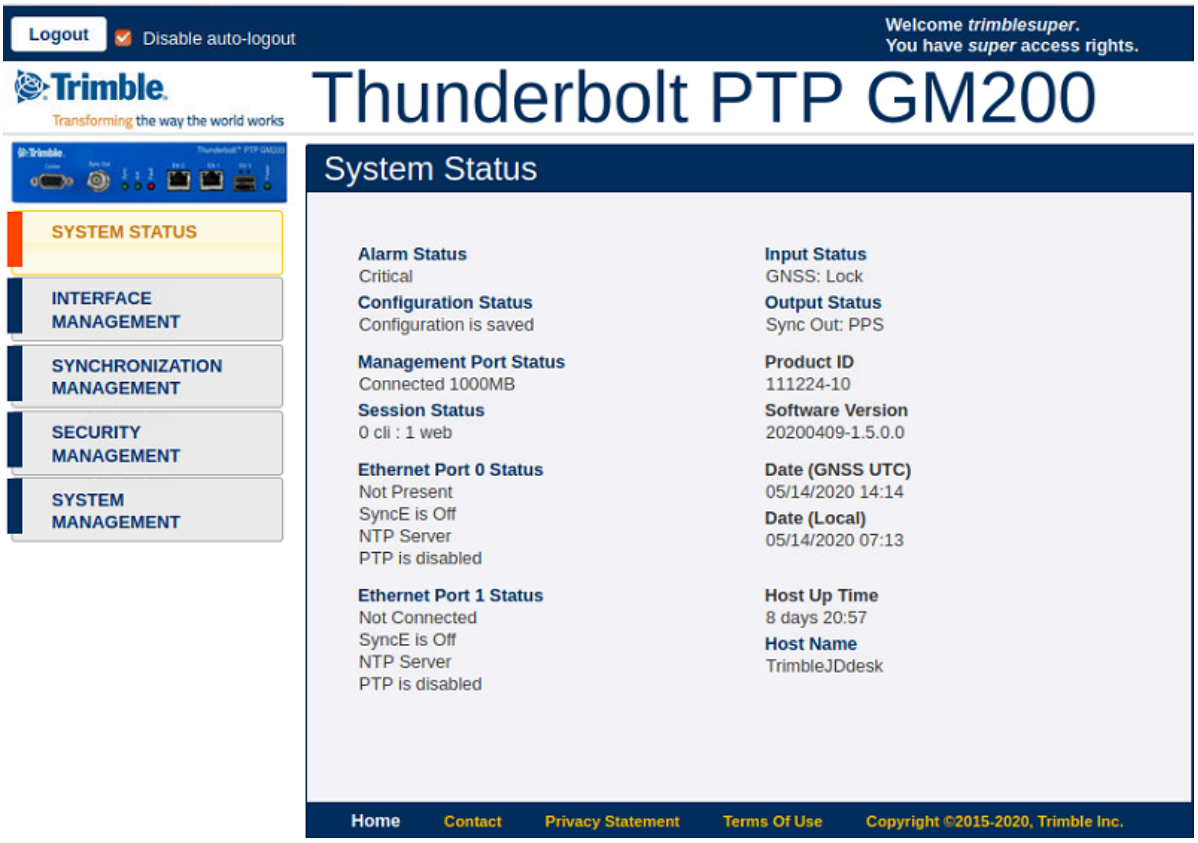
To launch a web browser and open a connection to the time server, enter the URL that specifies the IP address:

http://192.168.2.250

Web access is permitted only through Ethernet port 2. The default IP Address for Ethernet port 2 is 192.168.2.250.

> NOTE – Internet Explorer 11, Firefox, and Chrome browsers are supported on Windows® and Linux operating systems. Trimble recommends using the Chrome browser for better rendering of the web pages.

Entering the IP address will open the main or home page.



The main page displays a brief status of the time server. The components of this page are:

- Alarm Status: Shows the list of active alarms.
- Input Status: Shows the input reference of the time server.
- Configuration Status: Shows the status of the current configuration saved.

- **Product ID**: Shows the Trimble part number of the time server.
- **Management Port Status**: Shows the status of the Management Ethernet port.
- **Software Version**: Displays the current firmware version on the unit.
- **Time (UTC)**: Displays the time in UTC format.
- **Up Time**: Displays how long the unit is powered on.
- **Ethernet Port 0 Status**: Displays the status of PTP/NTP/SnycE Ethernet Port 0.
- **Ethernet Port 1 Status**: Displays the status of PTP/NTP/SnycE Ethernet Port 1.

Log into the time server to view or change system parameters. The login option is available at the top left of main landing page.

Refresh Rate

The main page is refreshed at a rate of one second.

6.2 Login page

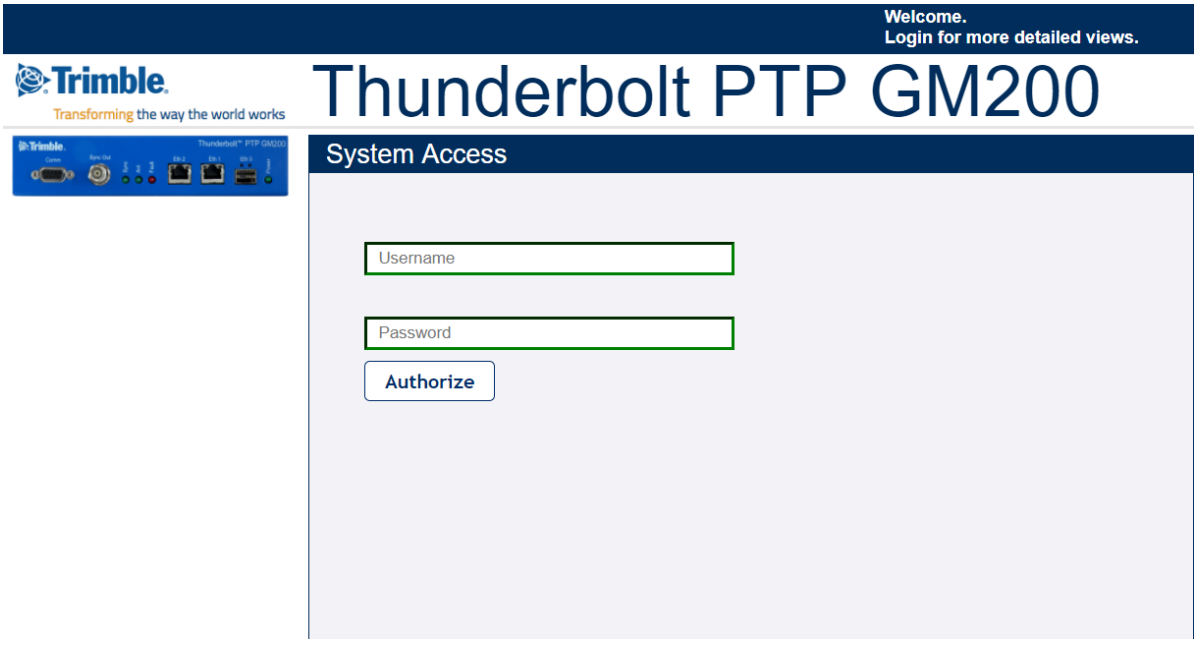
Log in to view the status of the system. The login page requires a valid username and password.

> NOTE – There is a change in default password to comply with the *California State Bill SB-327 – Information privacy: connected devices* bill, which requires that the pre-programmed password is unique to each device manufactured. The SB-327 bill is effective since 1 January 2020.
>
> To meet this requirement, Trimble has removed the default **trimble** and **trimbleadmin** accounts. Only the user **trimblesuper** is available by default, with the default password as outlined in this section.

Starting with v1.4.0.0, the unique password is based on the serial number of the unit. Here is the format:

User name: trimblesuper
Password: Tbolt_<serialnumber>

For example, if the serial number is 1234567890, the password will be Tbolt_1234567890.



As a 'Best security practices' Trimble recommends to change the default user credentials of the 'trimblesuper' account.

6.3 Editing a configuration page

All configuration pages have three icons on the top right of the configuration area. Numbered from left to right they are:

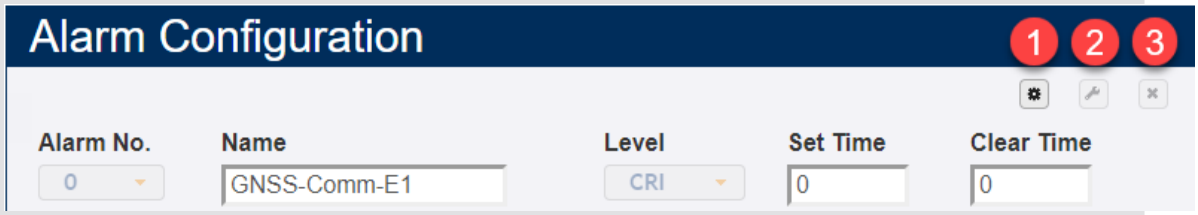
❶ – **Enable System Configuration** – put the screen in edit mode. Editable fields and pull down items will change from greyed to highlighted.

❷ – **Set** – Sets the configuration. You will need to SAVE the configuration in a separate step.

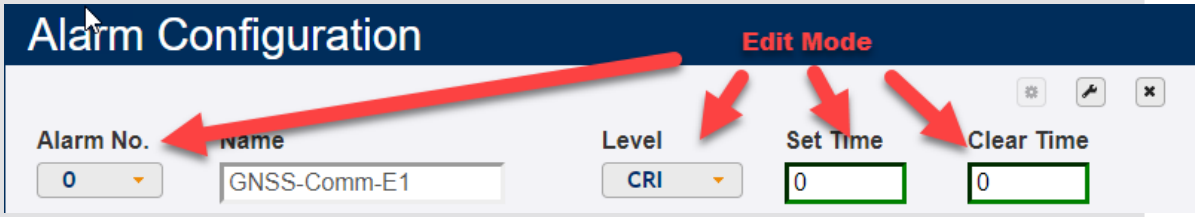
❸ – **Exit** – Returns the screen to read only mode.

EXAMPLES –

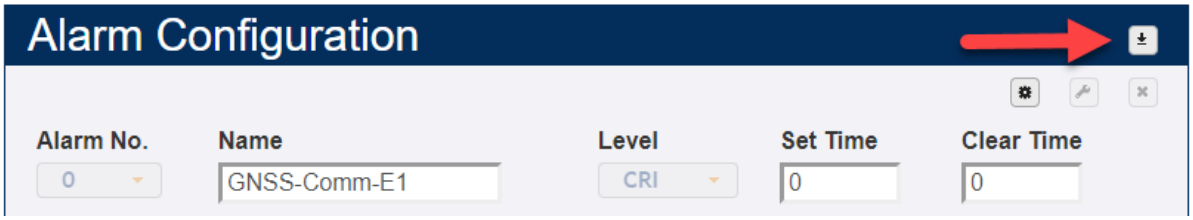
Alarm Configuration – Read Only



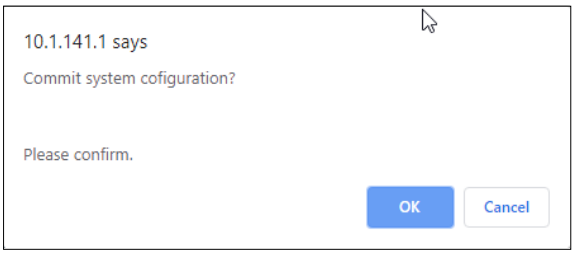
Alarm Configuration – Edit Mode



To save the configuration, click **Save System Configuration**:



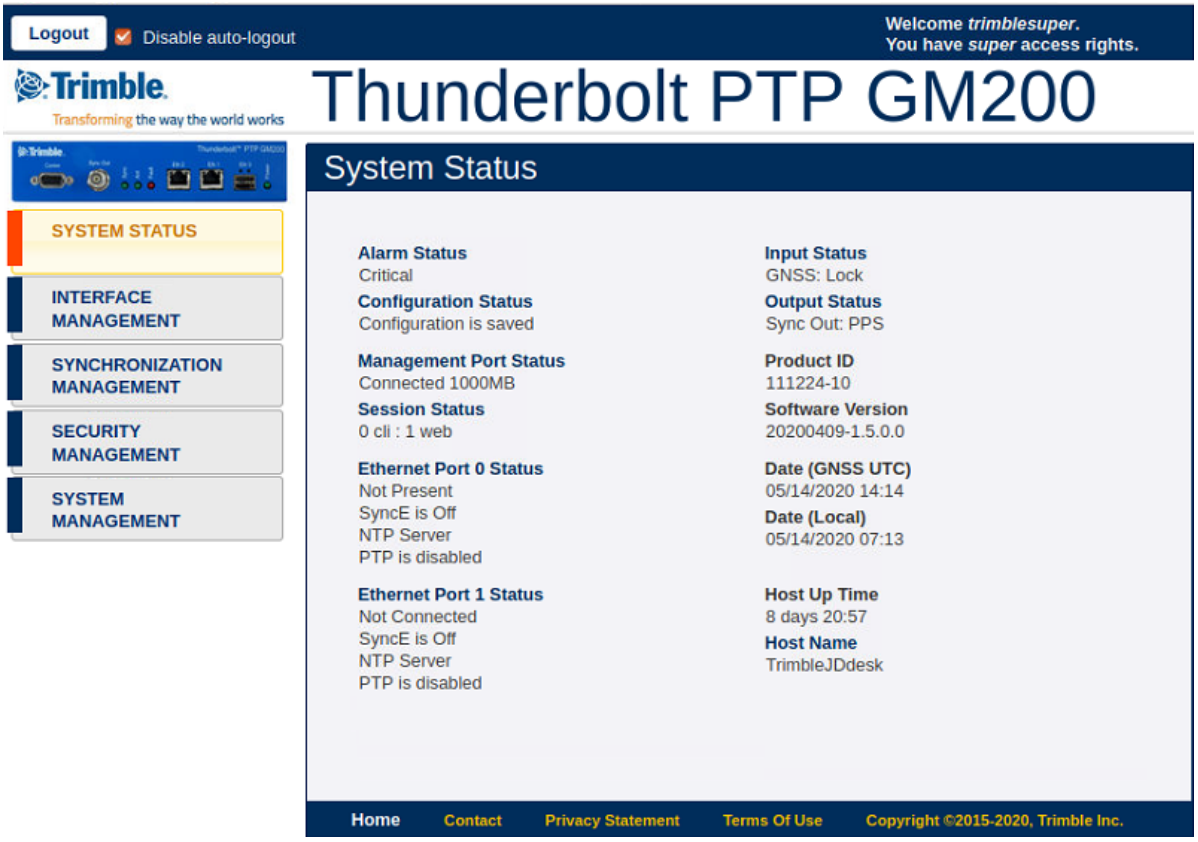
Then click **OK** in the confirmation box to commit the system configuration:



6.4 SYSTEM STATUS menu

After entering the valid credentials, the System Status page appears. It is organized in two frames—the navigation and content.

The start page gives general status information of the time server. By using the navigation menu on the left side of the screen, you can view a number of configuration pages, which are described in following pages.



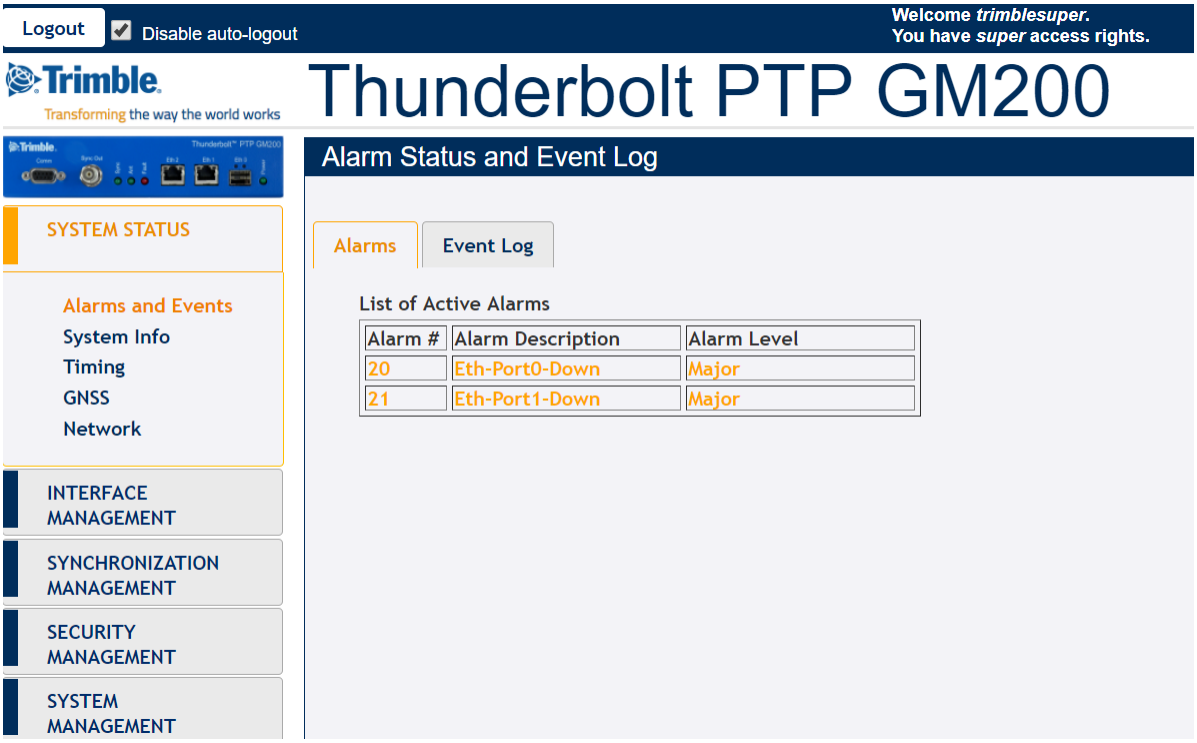
6.4.1 Alarms and Events

This page shows the currently active alarm conditions on the system.

6.4.1.1 Alarms

This tab provides the details of each alarm and the alarm level.

To access this tab, select SYSTEM STATUS / Alarms and Events / Alarms.



Alarm #: Alarm code.

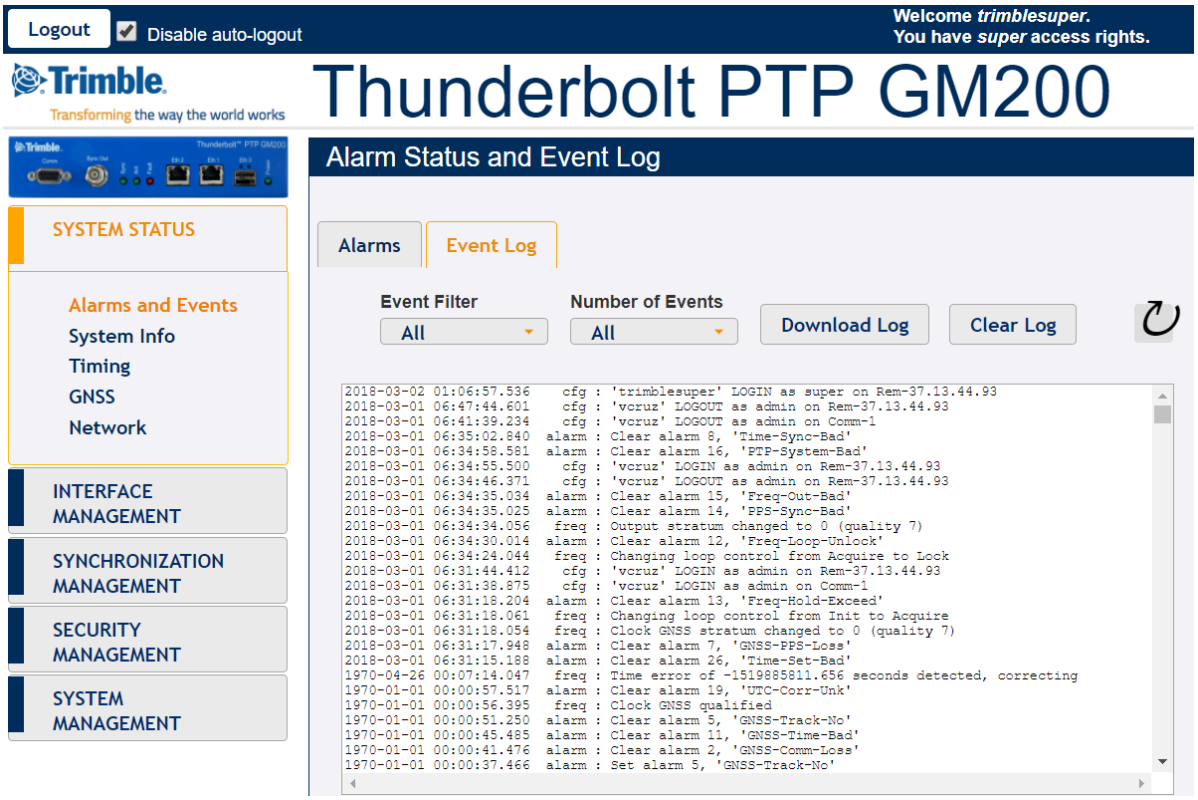
Alarm Description: Description of the alarm condition.

Alarm Level: Severity of alarm condition; can be notification only, minor, major, or critical.

6.4.1.2 Event Log

The **Event Log** page provides the list of system messages and notifications.

To access this tab, select **SYSTEM STATUS** / **Alarms and Events** / **Event Log**.



Event Filter: All, Alarms, Frequency, GNSS, Config Mods, Errors, Warnings, Notices, Information.

Number of Events: All, 10, 25, 50, 100.

Download Log: Select this button to download a text file with the message logs.

Clear Log: Select this button to clear all message logs.

6.4.2 System Info

The **System Information** page provides overall system information.

To access this page, select **SYSTEM STATUS** / **System Info**.

Product ID or Model: The model number of the time server.

Time (UTC): Displays the time in UTC format.

Hardware ID: Displays the hardware part number.

Up Time: Displays how long the unit is powered on.

Serial Number: The unique serial number of the time server.

CPU Load Average: A figure of merit for the operating system "load".

Extended S/N: Displays the extended serial number.

System Temperature: Displays the temperature of the time server.

Software Version: Displays the current firmware version on the unit.

Memory - Active: The amount of memory occupied by the system.

Hardware Build Date: The date of the firmware build.

Memory - Available: The amount of free memory remaining.

Download Support Info: The support info can be downloaded as a file.

Realtime Graph View: Displays the real-time graph of the following values:

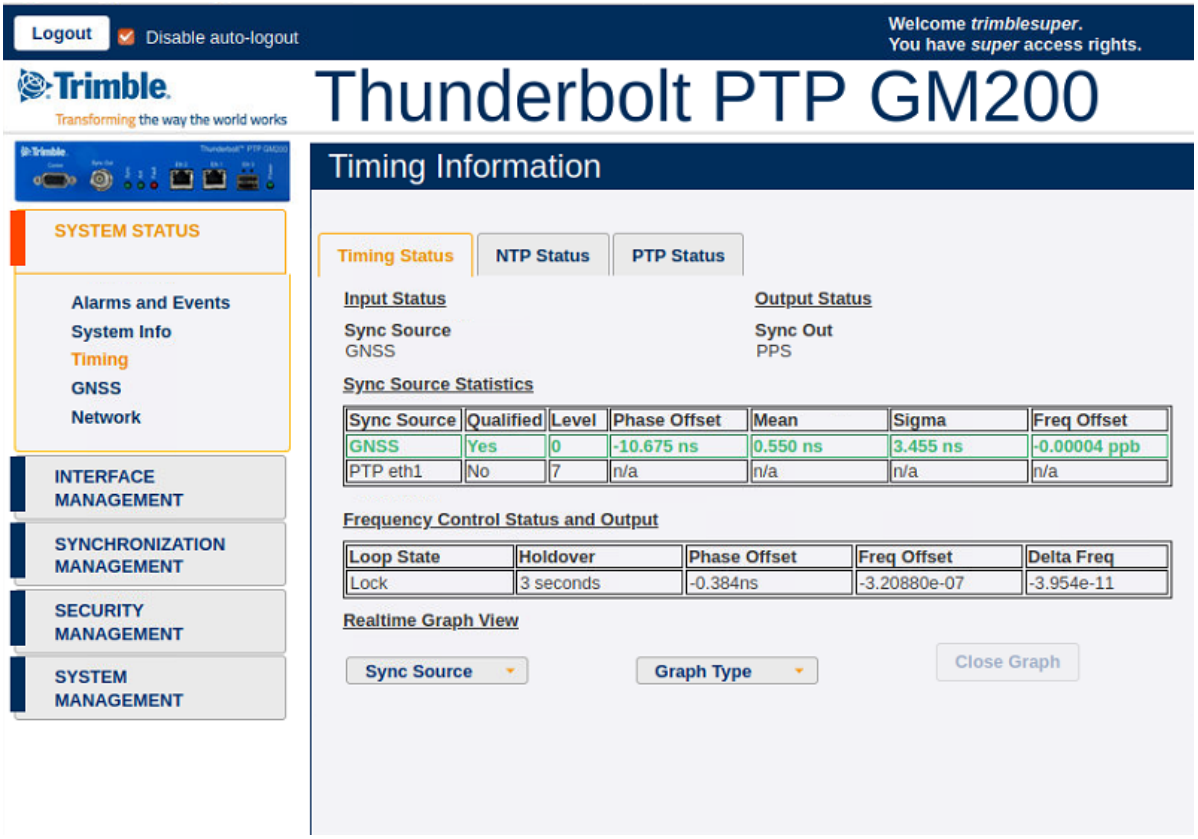
- CPU Load
- Temperature
- Mem – Active
- Mem - Available

6.4.3 Timing

6.4.3.1 Timing Status

This tab provides the status information of the system clock.

To access this tab, select SYSTEM STATUS / Timing.



Input Status

Sync Source	Indicates the current sync source

Output Status

BNC Output	Indicates the current configuration of BNC connector

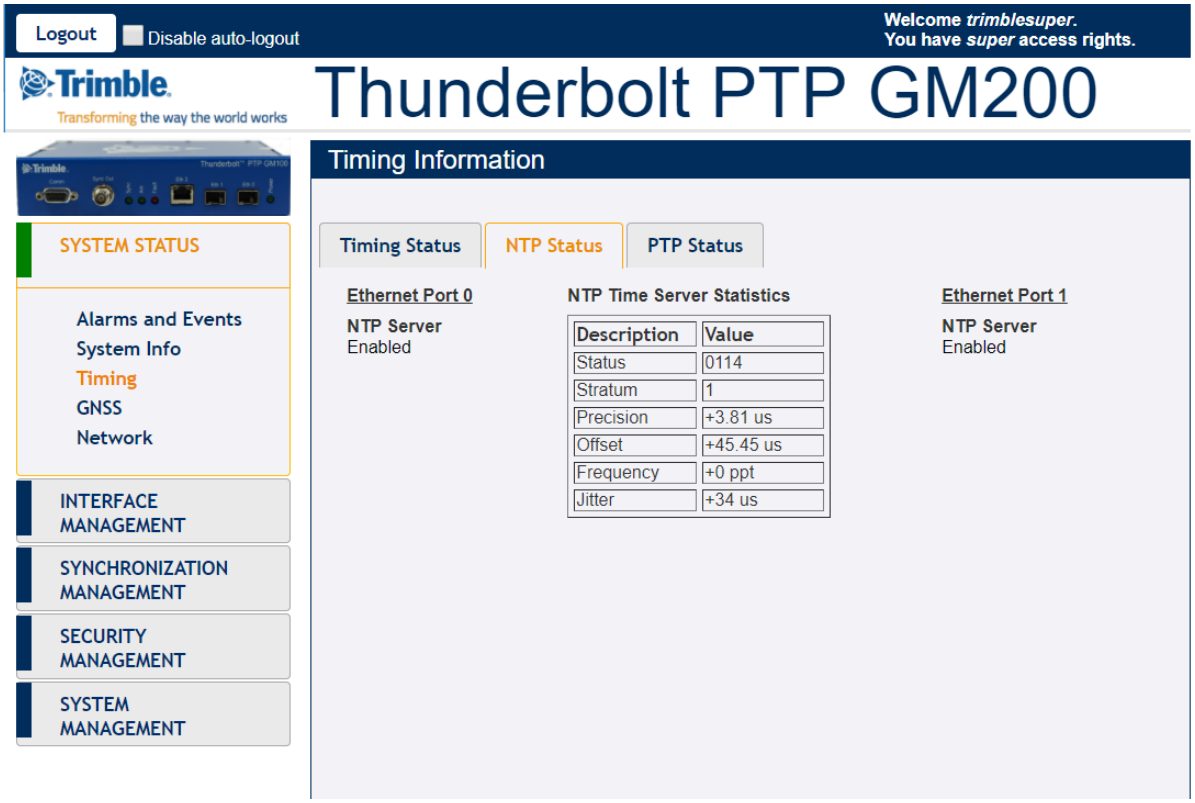
Sync Source Statistics

Sync Source	Distinguishes the name of the Sync Source
Phase Offset	GMC output PPS with reference to the sync source
Frequency Offset	The absolute frequency offset of the internal OCXO with reference to sync source
Mean	The mean phase offset
Sigma	The standard deviation of phase offset.

Control Loop Status	Status of system control loop of the system.
Phase Offset	Control loop output with reference to the sync source
Frequency Offset	The frequency offset of control loop of the time server
Holdover	The estimated holdover time available

6.4.3.2 NTP Status

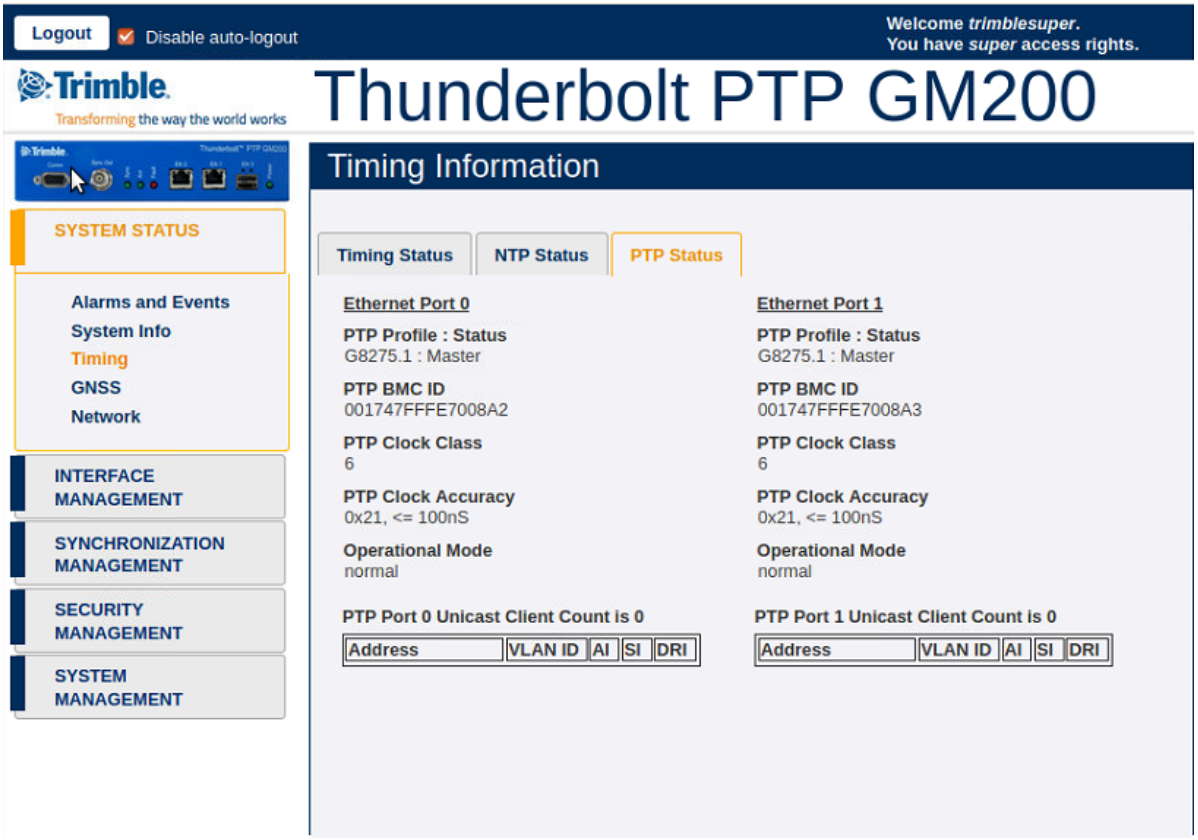
To access this tab, select SYSTEM STATUS / Timing / NTP Status.



Ethernet Port	Identifies the Ethernet port – Eth0 or Eth1
NTP Status	Shows the status of port connection (For more information on the *view ntp* command, see The view ntp command displays the current NTP status., page 117)
NTP Time Server Statistics	Shows the statistics of various server parameters

6.4.3.3 PTP Status

To access this tab, select SYSTEM STATUS / Timing / PTP Status.



Ethernet Port	Identifies the Ethernet port – Eth0 (RJ45) or Eth1 (SFP)
PTP Status	Shows the status of port connection
PTP Clock ID	Identifies the PTP clock ID
PTP Statistics	
Description	Name of the Statistic
Value	Value
Operational Mode	PTP Operational Mode: Normal or Freerun When the operational mode is configured for 'normal', the system will operate in a traditional GrandMaster manner, requiring a (GNSS) frequency and time reference to be established before starting PTP. When the operational mode is configured for 'freerun', the system will start PTP as soon as the system is booted and interfaces are functional.

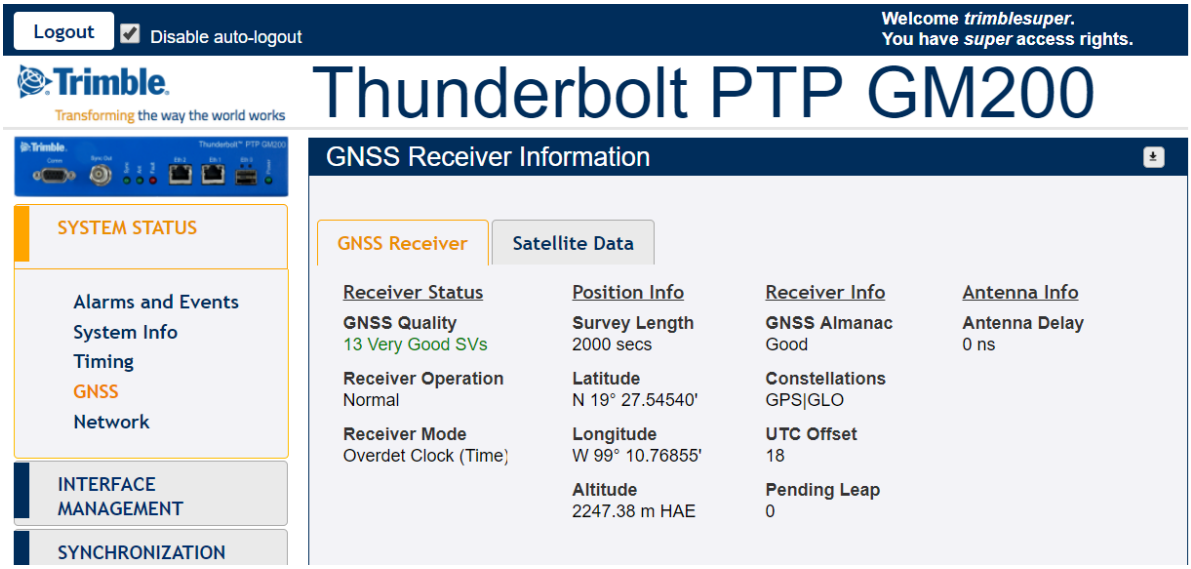
PTP Port 1/2 Unicast Clients	Only available for unicast PTP profiles. The table will show either PTP slaves (when port configured as PTP GM) or PTP Master (when port is configured as PTP Slave).

6.4.4 GNSS

This page displays GNSS receiver status information.

6.4.4.1 GNSS Receiver

To access this tab, select SYSTEM STATUS / GNSS / GNSS Receiver.



Latitude: The latitude of the time server.

Longitude: The latitude of the time server.

Altitude: The altitude of the GNSS receiver.

Receiver Status: The current status of the receiver (doing fixes, in clock mod).

GNSS Almanac: The status of the GNSS almanac.

Constellations: Current constellations that are being used.

GNSS Quality Status: A metric used to provide the user with a snapshot of the number of satellites with Very Good, Good, or Poor Signal Strength/Quality, coloured Green, Orange and Red respectively:

- Quality is Very Good if there are at least 4 SVs that have SNR > 35
- Quality is Good if there are at least 4 SVs that have SNR > 20
- Quality is Poor if there are no SVs that have SNR > 20

Antenna Delay: Displays the compensation delay of antenna cable.

The **antenna delay** setting affects the **system time base** of time server. Negative numbers advance the internal time reference, positive numbers retard (delay)

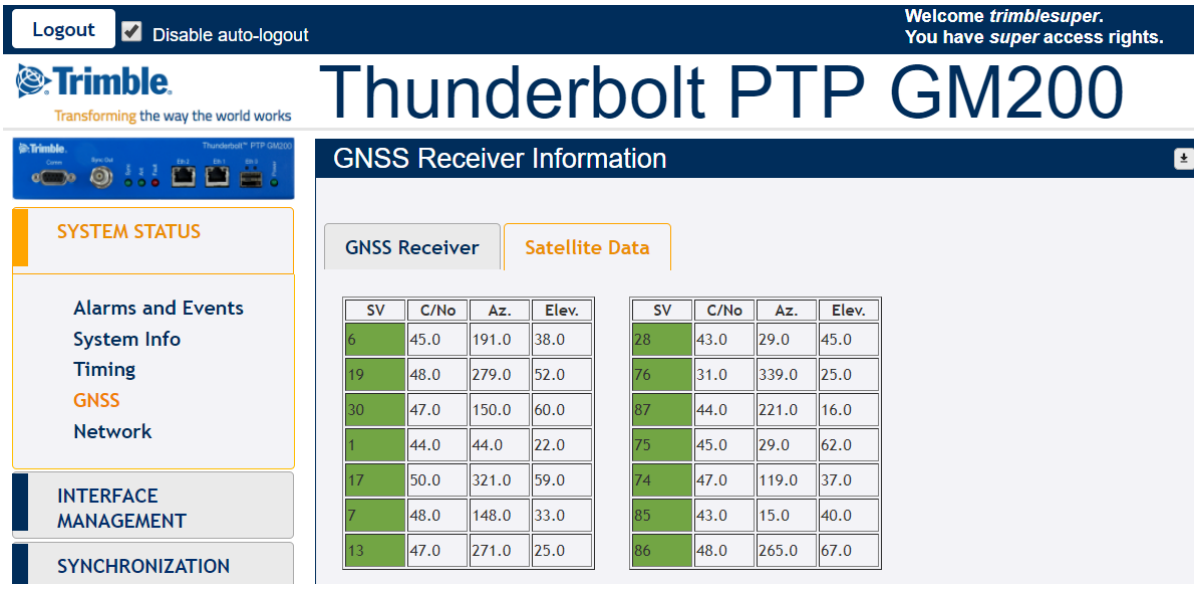
the time reference. To compensate for an antenna delay of 500 ns you would enter -500 as the antenna delay setting. <d> is in nanoseconds with a range of +/- 50000000 (50 ms).

All PTP and NTP timestamps are derived from the system time base, which means that you want to make sure that the antenna delay is correctly compensated because that value affects the PTP and NTP clock accuracy in the LAN network.

Note that, since this setting affects the disciplined oscillator of the time server, the effect of changing the antenna delay value is not seen immediately on the system output. The antenna delay value will advance (or retard) the internal GNSS time measurements, which go into the oscillator's PLL control loop, which will then gradually steer the disciplined oscillator toward that new value. If the value is jumped too far after the time server has achieved lock (remember, this is normally an installation setting), then the unit may issue a "PPS-Sync-Bad" and/or a "Freq-Loop-Unlock" alarm. After a while, when the time base has moved to the new value, these alarms will be cleared.

6.4.4.2 Satellite Data

To access this tab, select SYSTEM STATUS / GNSS / Satellite Data.



SV: Satellite vehicle.

C/No: Carrier-to-Noise power ratio.

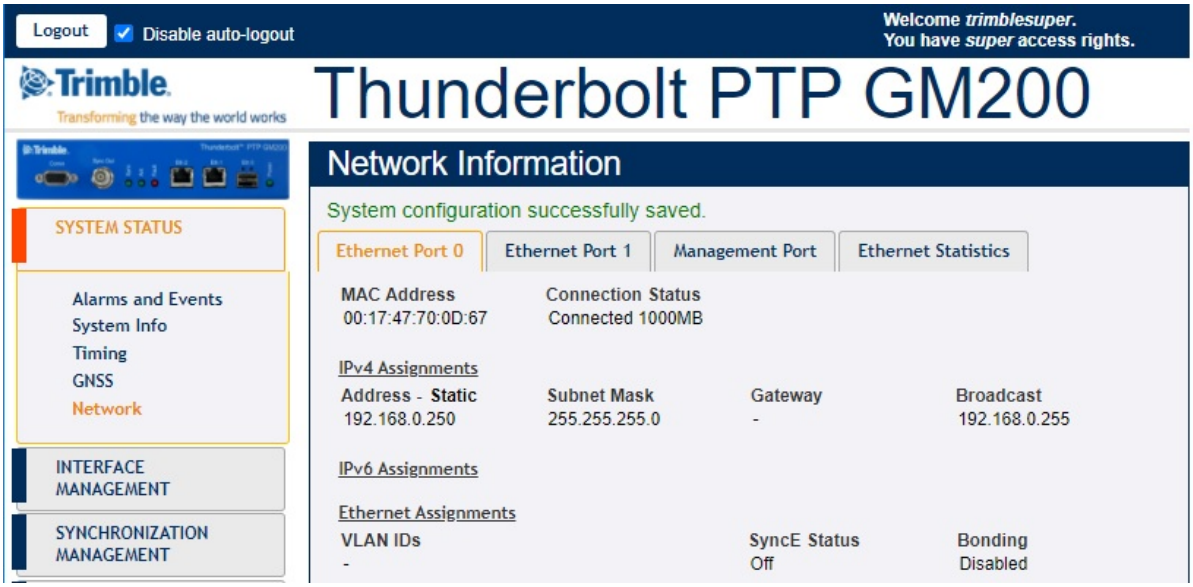
AZ: Azimuth.

Elev: Elevation.

6.4.5 Network

6.4.5.1 Ethernet Port 0

To access this tab, select SYSTEM STATUS / Network / Ethernet Port 0.



IPv4: IP address of the port.

IPv4 Subnet Mask: Subnet mask being used.

IPv4 Gateway: Default gateway.

IPv4 Broadcast: Broadcast IP address.

IPv6 Address/Mask: IPv6 Address of the Ethernet interface with the subnet mask.

IP Assignment: Either static or DHCP.

Connection Status: Status of Ethernet connection.

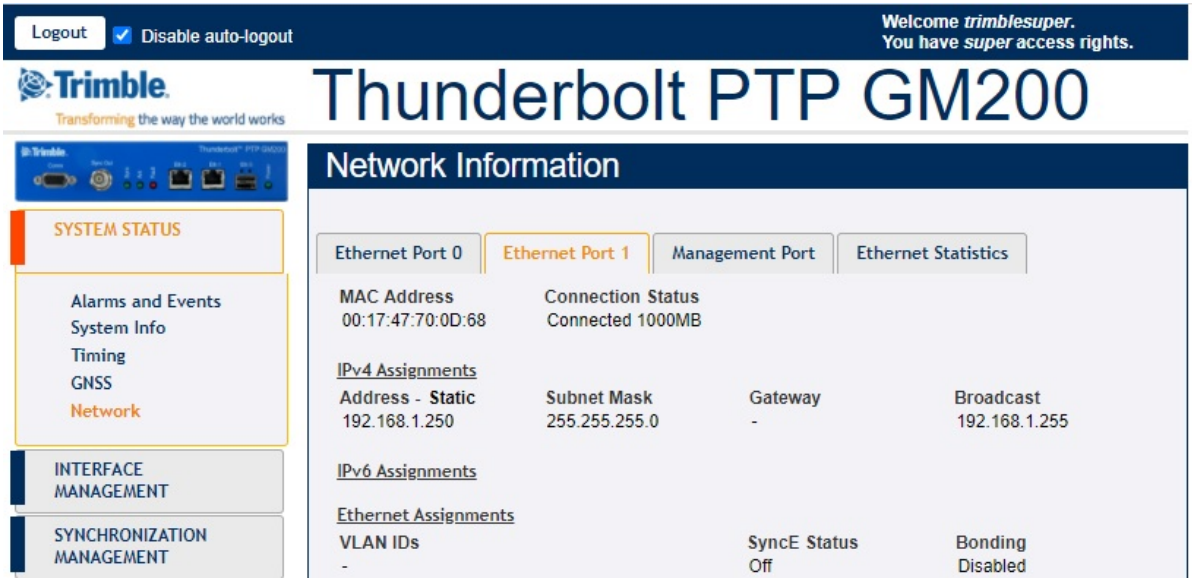
MAC Address: The MAC address of the port.

SyncE Status: Status of Synchronous Ethernet.

Bonding: Status of Network Bonding.

6.4.5.2 Ethernet Port 1

To access this tab, select SYSTEM STATUS / Network / Ethernet Port 1.



IPv4: IP address of the port.

IPv4 Subnet Mask: Subnet mask being used.

IPv4 Gateway: Default gateway.

IPv4 Broadcast: Broadcast IP address.

IPv6 Address/Mask: IPv6 Address of the Ethernet interface with the subnet mask.

IP Assignment: Either static or DHCP.

Connection Status: Status of the Ethernet connection.

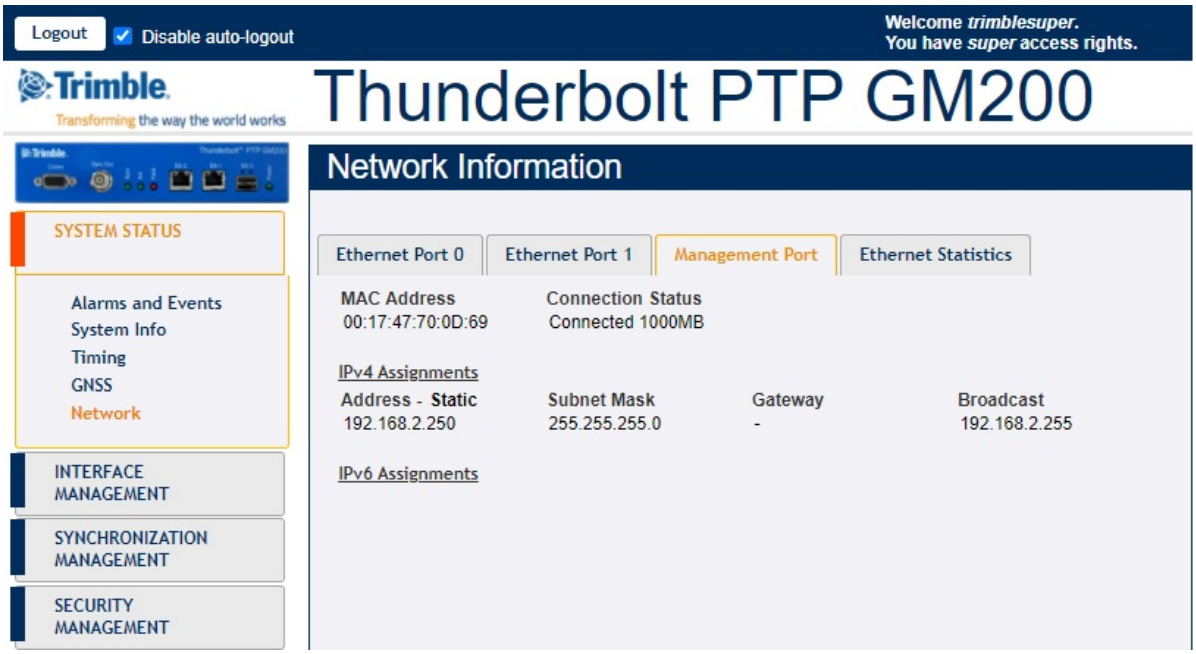
MAC Address: The MAC address of the port.

SyncE Status: Status of Synchronous Ethernet.

Bonding: Status of Network Bonding.

6.4.5.3 Management port

To access this tab, select SYSTEM STATUS / Network / Management Port.



IPv4: IP address of the port.

IPv4 Subnet Mask: Subnet mask being used.

IPv4 Gateway: Default gateway.

IPv4 Broadcast: Broadcast IP address.

IPv6 Address/Mask: IPv6 address of the Ethernet interface with the subnet mask.

IP Assignment: Either static or DHCP.

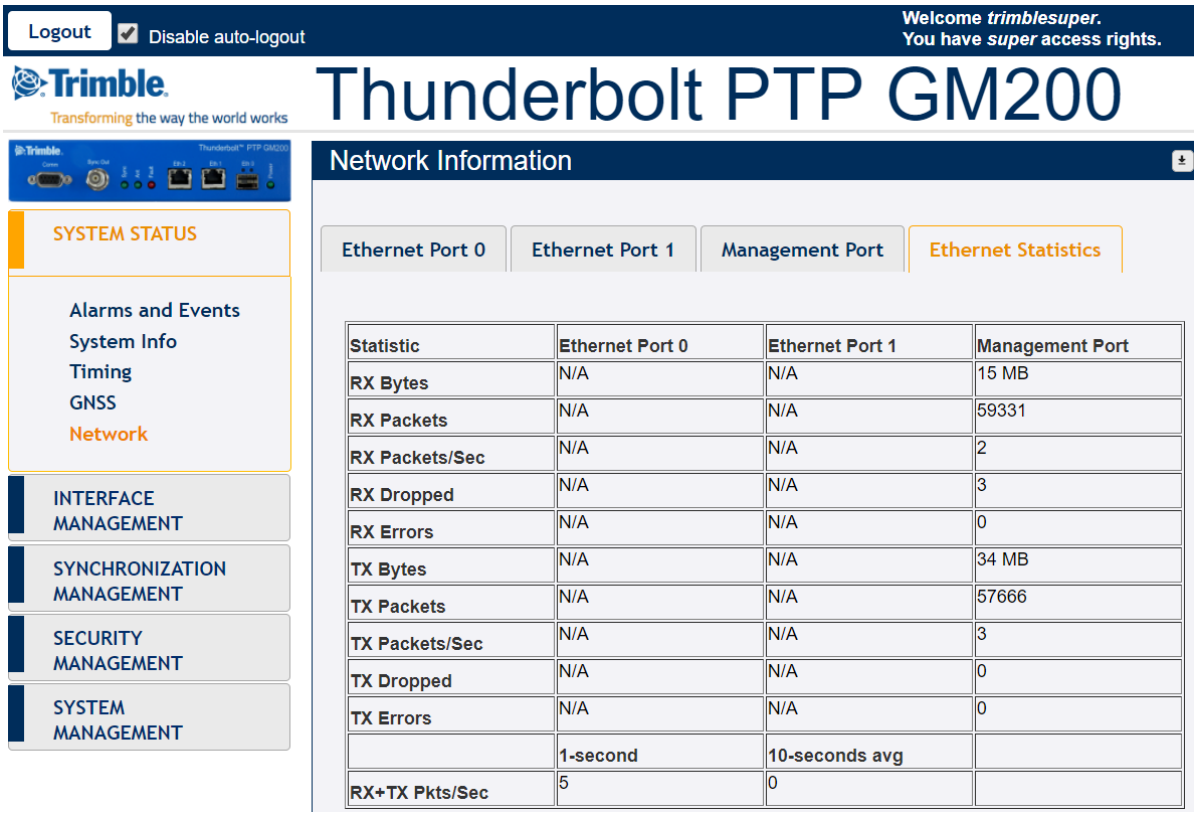
Connection Status: Status of the Ethernet connection.

MAC Address: The MAC address of the port.

6.4.5.4 Ethernet Statistics

Displays the following Ethernet statistics.

To access this page, select SYSTEM STATUS / Network / Ethernet Statistics.



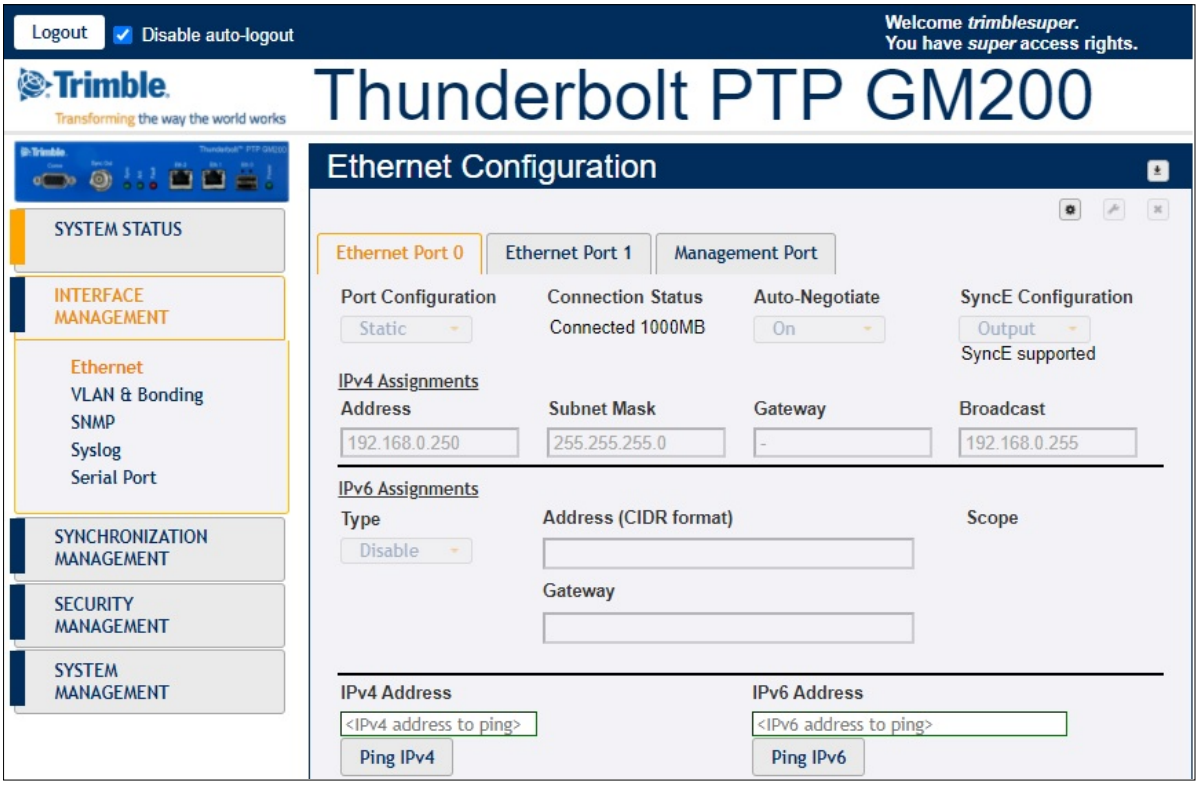
Statistic	Ethernet Port 0	Ethernet Port 1	Management Port
RX Bytes	N/A	N/A	15 MB
RX Packets	N/A	N/A	59331
RX Packets/Sec	N/A	N/A	2
RX Dropped	N/A	N/A	3
RX Errors	N/A	N/A	0
TX Bytes	N/A	N/A	34 MB
TX Packets	N/A	N/A	57666
TX Packets/Sec	N/A	N/A	3
TX Dropped	N/A	N/A	0
TX Errors	N/A	N/A	0
	1-second	10-seconds avg	
RX+TX Pkts/Sec	5	0	

6.5 INTERFACE MANAGEMENT menu

6.5.1 Ethernet

6.5.1.1 Ethernet Port 0

To access this tab, select INTERFACE MANAGEMENT / Ethernet / Ethernet Port 0.



Port Configuration: DHCP, Static, Default, or Disable this interface.

Connection Status: Either Connected or Not Connected.

Auto-Negotiate: Either On or Off.

SyncE Configuration: Output, Input, or Off.

IPv4 Address: IPv4 address of the port.

IPv4 Subnet Mask: Subnet mask being used.

IPv4 Gateway: Default gateway IPv4 address.

IPv4 Broadcast: Broadcast IPv4 address.

IPv6 Mode: DHCPv6, SLAAC, or Static.

IPv6 Address: IPv6 address of the Ethernet interface.

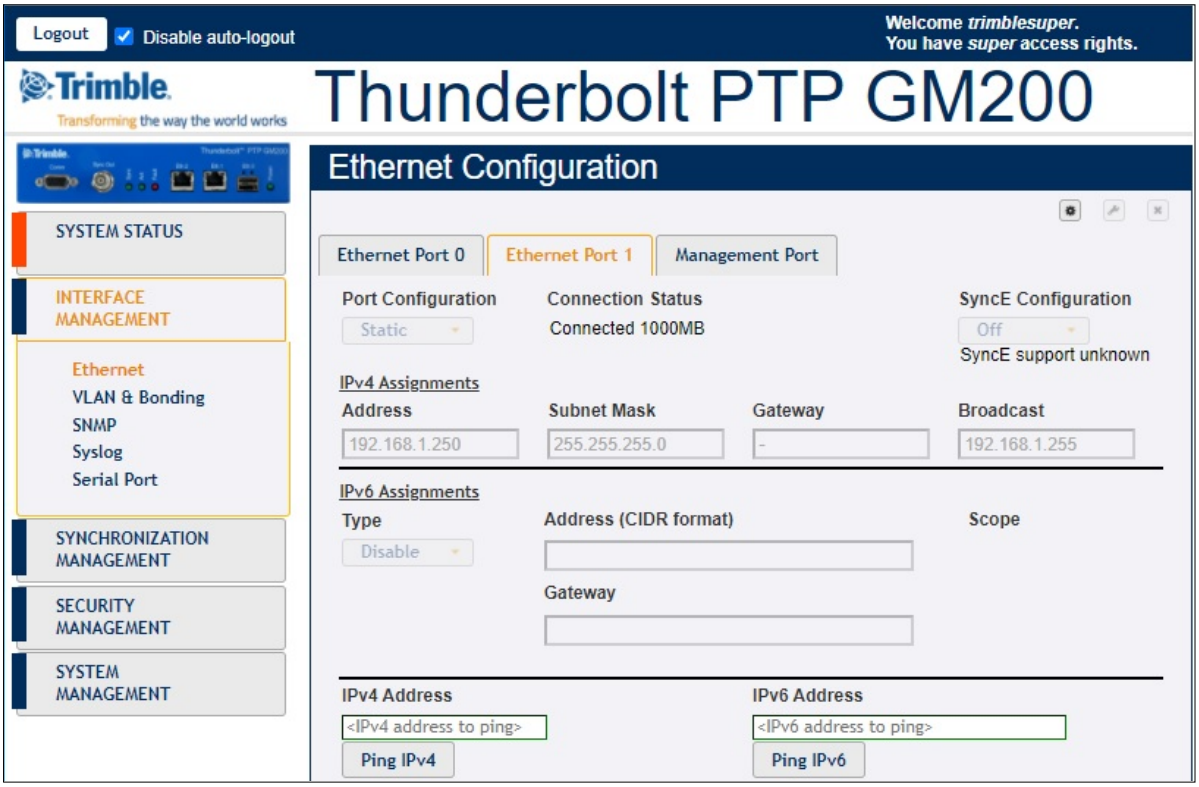
IPv6 Gateway: IPv6 gateway address for the port.
This must be in CIDR format which is the IPv6 address with a /mask /value.
If no /mask is given the default mask size of 128-bits is assumed.
The gateway setting can be cleared by setting a CIDR address of "::".

Ping IPv4: Enter IPv4 address to test ping.

Ping IPv6: Enter IPv6 address to test ping.

6.5.1.2 Ethernet Port 1

To access this tab, select **INTERFACE MANAGEMENT** / **Ethernet** / **Ethernet Port 1**.



Port Configuration: Either DHCP, Static, Default, or Disable this interface.

Connection Status: Either Connected or Not Connected.

SyncE Configuration: Either Output, Input, or Off.

IPv4 Address: IPv4 address of the port.

IPv4 Subnet Mask: Subnet mask being used.

IPv4 Gateway: Default gateway IPv4 address.

IPv4 Broadcast: Broadcast IPv4 address.

IPv6 Mode: DHCPv6, SLAAC, or Static.

IPv6 Address: IPv6 address of the Ethernet interface.

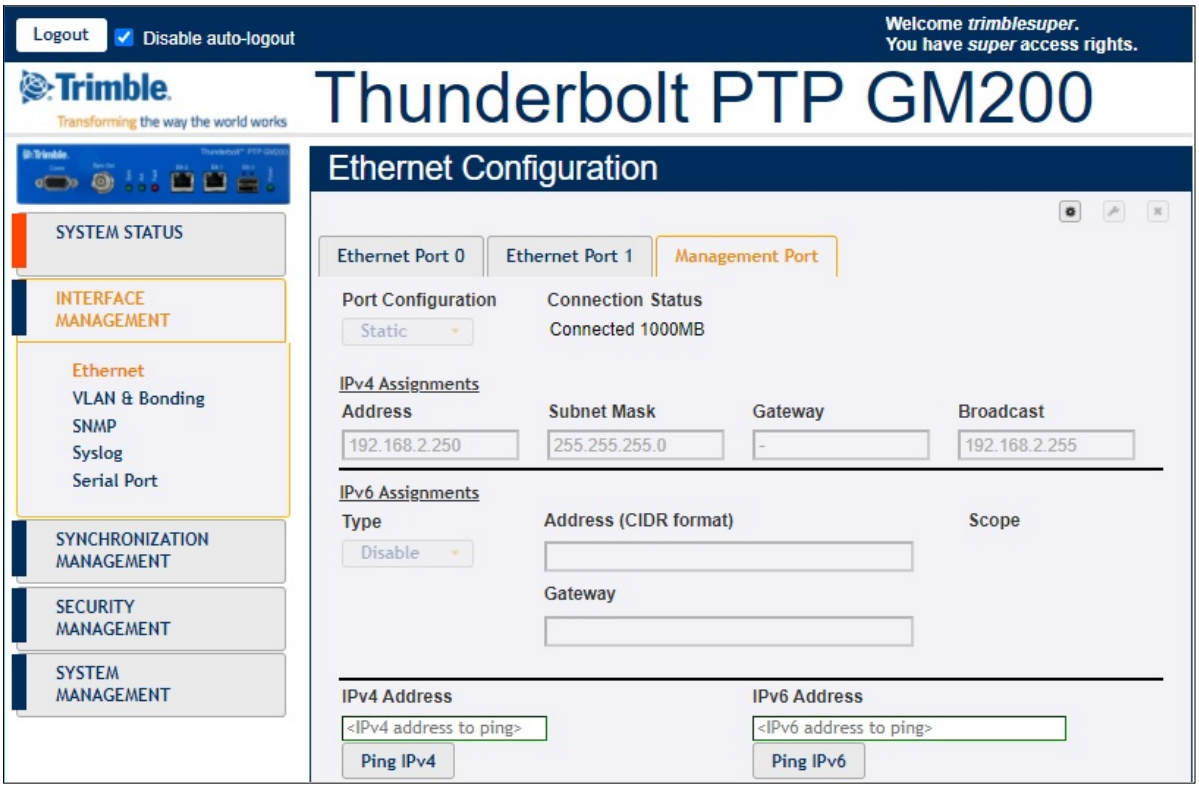
IPv6 Gateway: IPv6 gateway address for the port.
This must be in CIDR format which is the IPv6 address with a /mask /value.
If no /mask is given the default mask size of 128-bits is assumed.
The gateway setting can be cleared by setting a CIDR address of "::".

Ping IPv4: Enter IPv4 address to test ping.

Ping IPv6: Enter IPv6 address to test ping.

6.5.1.3 Management Port

To access this tab, select **INTERFACE MANAGEMENT** / **Ethernet** / **Management Port**.



Port Configuration: DHCP, Static, Default, or Disable this interface.

Connection Status: Either Connected or Not Connected.

IPv4 Address: IPv4 address of the port.

IPv4 Subnet Mask: Subnet mask being used.

IPv4 Gateway: Default gateway IPv4 address.

IPv4 Broadcast: Broadcast IPv4 address.

IPv6 Mode: DHCPv6, SLAAC, or Static.

IPv6 Address: IPv6 address of the Ethernet interface.

IPv6 Gateway: IPv6 gateway address for the port.

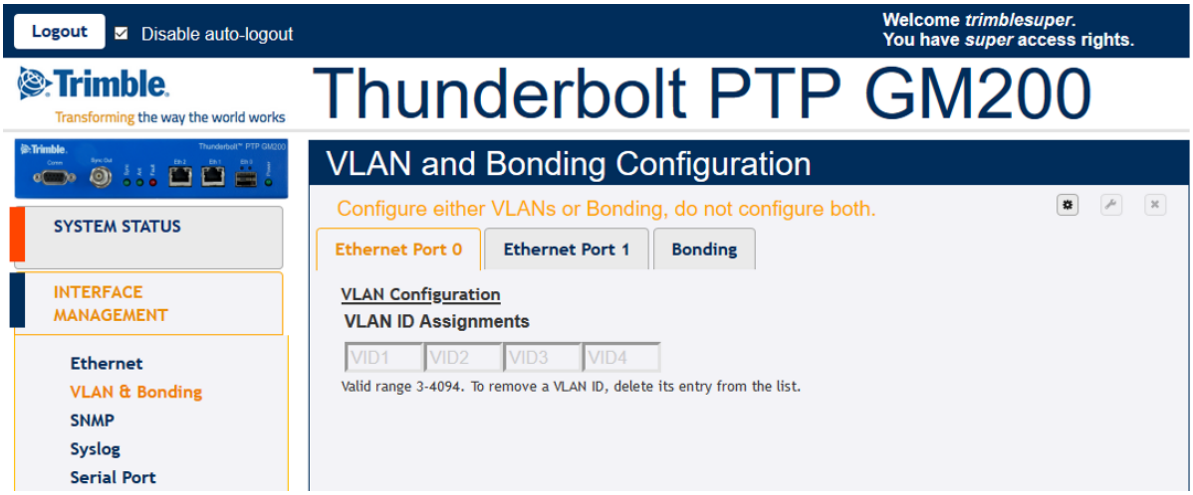
Ping IPv4: Enter IPv4 address to test ping.

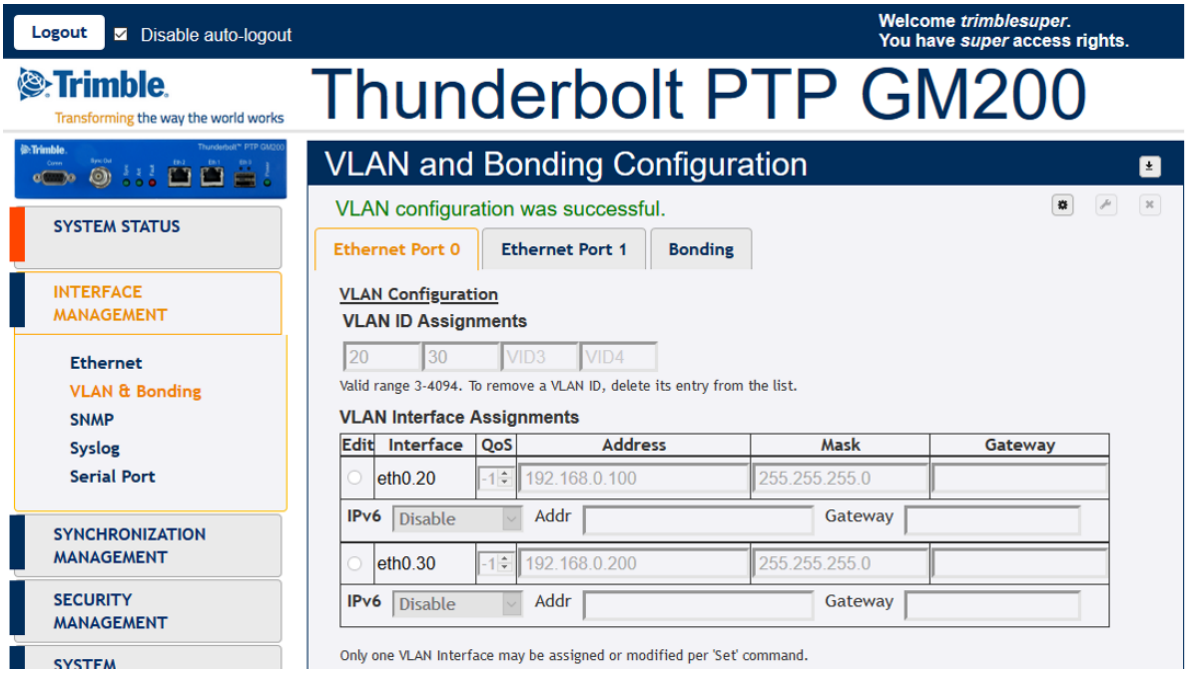
Ping IPv6: Enter IPv6 address to test ping.

6.5.2 VLAN & Bonding

6.5.2.1 Ethernet Port 0

To access this tab, select SYSTEM STATUS / VLAN & Bonding / Ethernet Port 0.





VLAN IDs: List of all VLAN IDs configured (3 to 4094).

Edit: Select a VLAN ID to change.

Interface: Ethernet interface with a VLAN ID.

QoS: Priority from 0 to 7, where 7 is the highest priority.

Address: IPv4 address of the selected VLAN ID.

Mask: Subnet mask of the selected VLAN ID.

Gateway: IPv4 gateway address of the selected VLAN ID.

IPv6: IPv6 address configuration. Disable, Static, DHCPv6, or SLAAC.

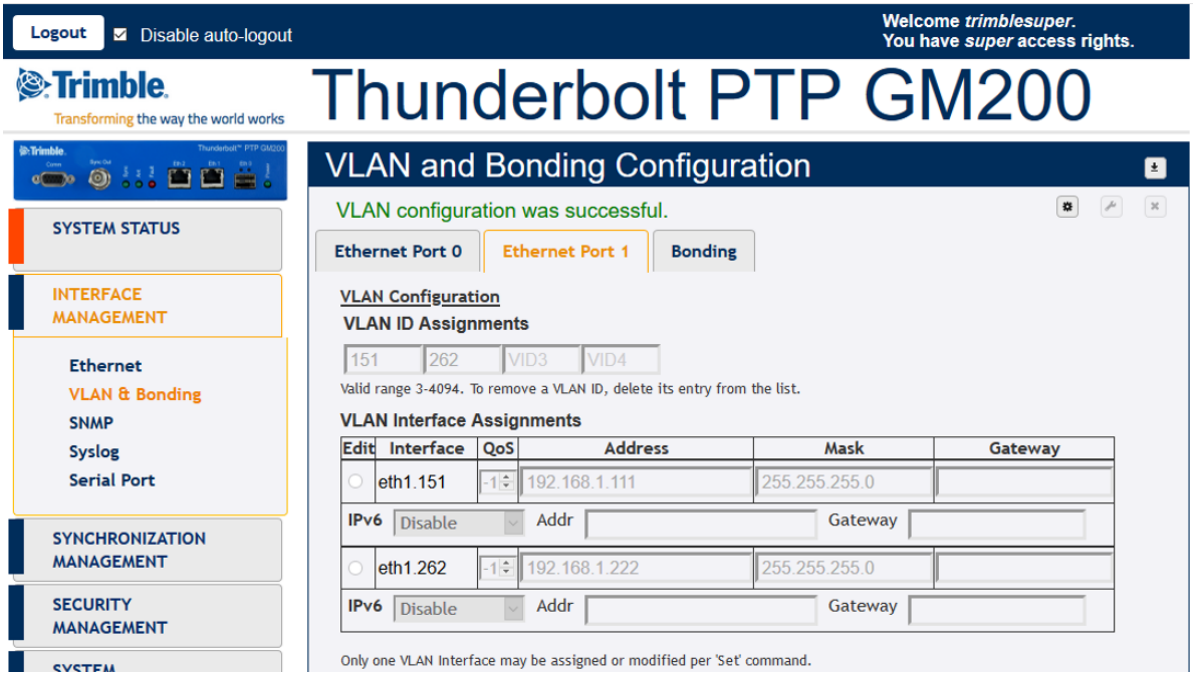
Addr: IPv6 address of the selected VLAN ID.

Gateway: IPv6 gateway address.

> NOTE – There is a limit of four VLANs per port.

6.5.2.2 Ethernet Port 1

To access this tab, select **SYSTEM STATUS** / **VLAN & Bonding** / **Ethernet Port 1**.



VLAN IDs: List of all VLAN IDs configured (3 to 4094).

Edit: Select a VLAN ID to change.

Interface: Ethernet interface with a VLAN ID.

QoS: Priority from 0 to 7, where 7 is the highest priority.

Address: IPv4 address of the selected VLAN ID.

Mask: Subnet mask of the selected VLAN ID.

Gateway: IPv4 gateway address of the selected VLAN ID.

IPv6: IPv6 address configuration. Disable, Static, DHCPv6, or SLAAC.

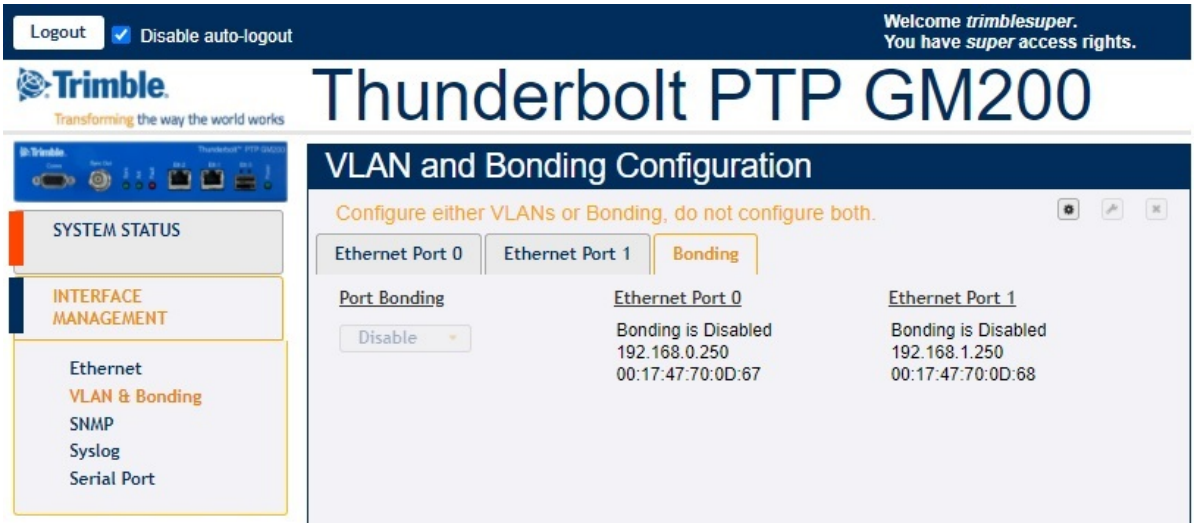
Addr: IPv6 address of the selected VLAN ID.

Gateway: IPv6 gateway address.

> NOTE – There is a limit of four VLANs per port.

6.5.2.3 Port Bonding configuration with NTP

To access this tab, select **SYSTEM STATUS** / **VLAN & Bonding** / **Bonding**.



Port Bonding: Either Enable, Disable, or Swap.

Ethernet Port 0: Port Bonding Status on Eth0. Either Disabled, Active, or Standby with IPv4 and Mac Address.

Ethernet Port 1: Port Bonding Status on Eth0. Either Disabled, Active, or Standby with IPv4 and Mac Address.

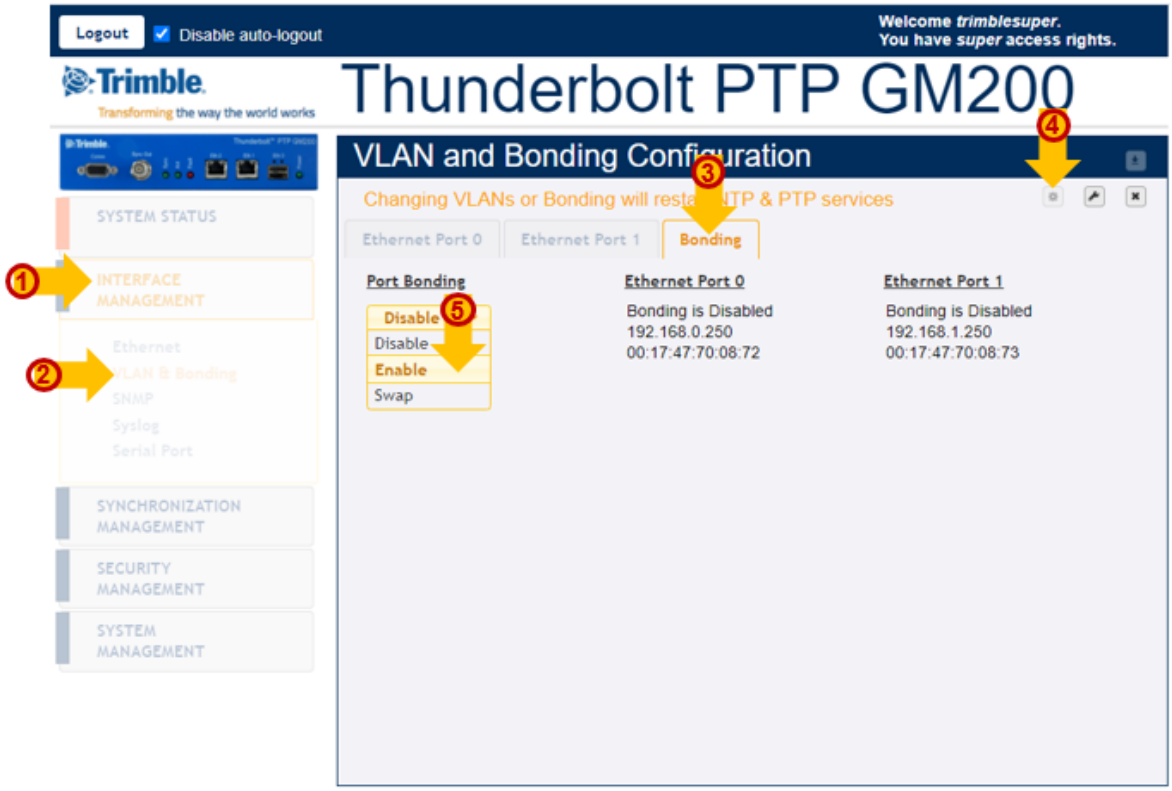
> NOTE – VLANs and Bonding cannot be configured simultaneously.

The main tasks to link the time server with NTP are:

1. Link on for both Eth0 and Eth1.
2. Configure the IP address to meet with the installed network.
3. Ping to an NTP Client and then confirm it works.
4. Enable NTP operation.
5. Enable Bonding function.
6. Ping to NTP Client and then confirm it works with the “Bonding” operation.
7. Check NTP clients, whether it synchronizes with the time server.

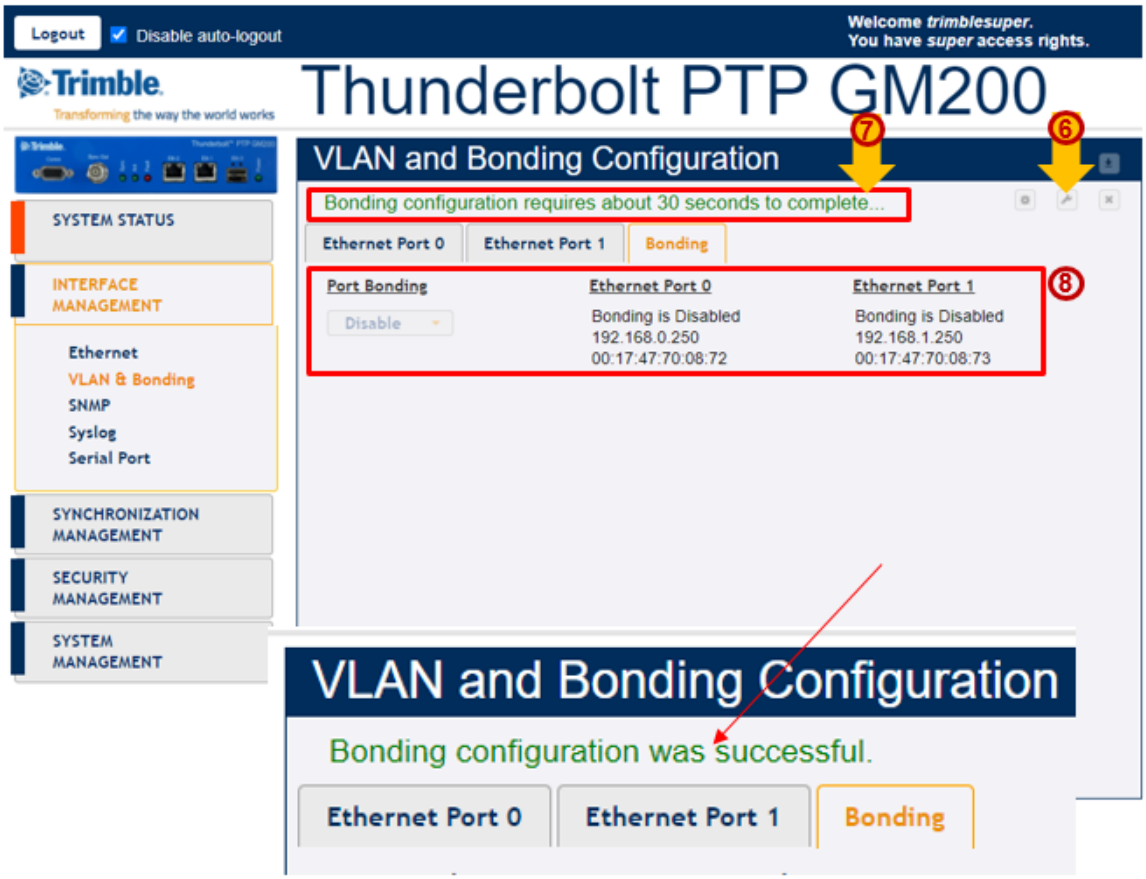
8. Remove or Swap the "Active" interface and then confirm that NTP clients are still synchronizing with the time server.

The basic operation of the port bonding in the time server is to bond two Ethernet interfaces with the same IP address and Mac address, as one port is active and the other port is standby, so that two physical interfaces act as one logical interface.



1. Select INTERFACE MANAGEMENT ❶ and then VLAN & Bonding ❷.
2. Click the **Bonding** tab ❸.
3. Click **Configure** ❹.
4. In the **Port Bonding** drop-down list, select **Enable** ❺.

5. Click **Set**  to apply the settings ❻.

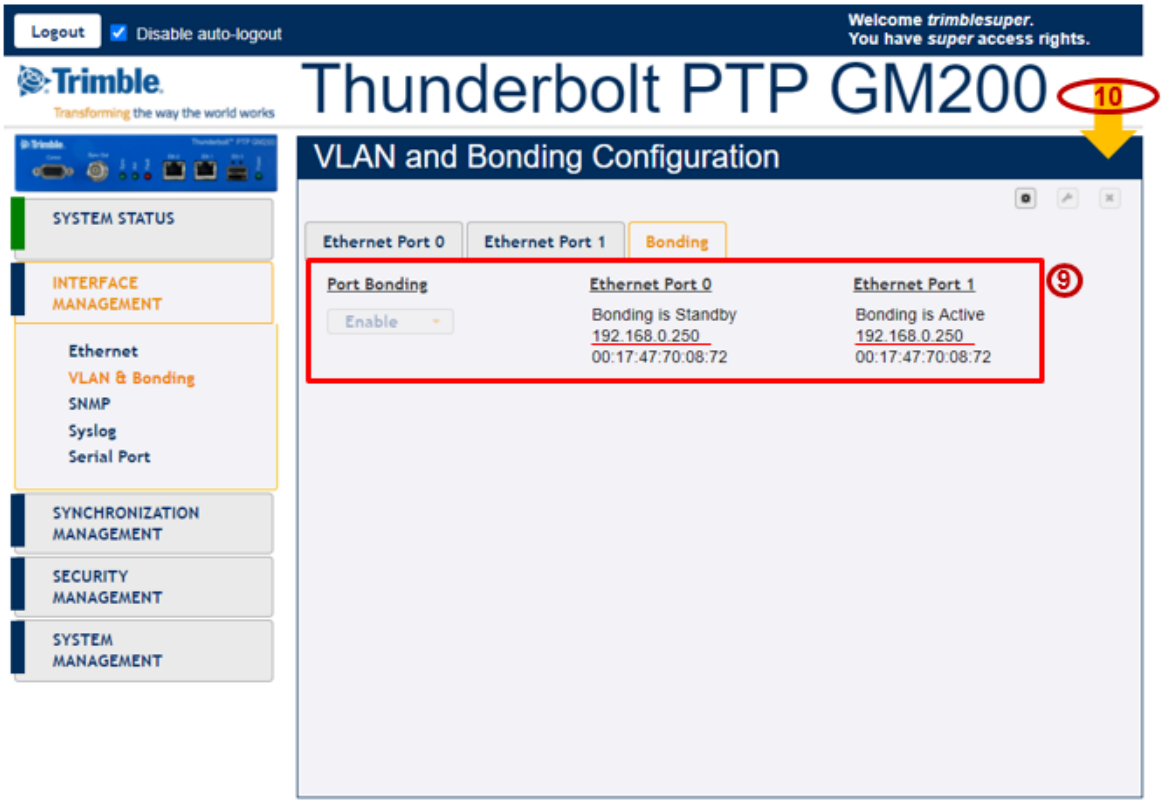


The time server shows a message with **Bonding configuration requires about 30 seconds to complete...** ❼.

After 30 seconds the **Bonding configuration was successful** message shows.

> NOTE – During these 30 seconds, the **Configure** and **Set** icons are deactivated so that you cannot set any other configuration while applying the bonding.
>
> NOTE – During the process of applying the bonding, the Eth0 and Eth1 still show **Bonding is Disabled**, with different IP address and Mac address ❽.

6. Within 30 seconds of seeing the completion message, the screen shows the same IP address and Mac address with **Bonding is Standby** in Eth0 and'**Bonding is Active** in Eth1 ❾:

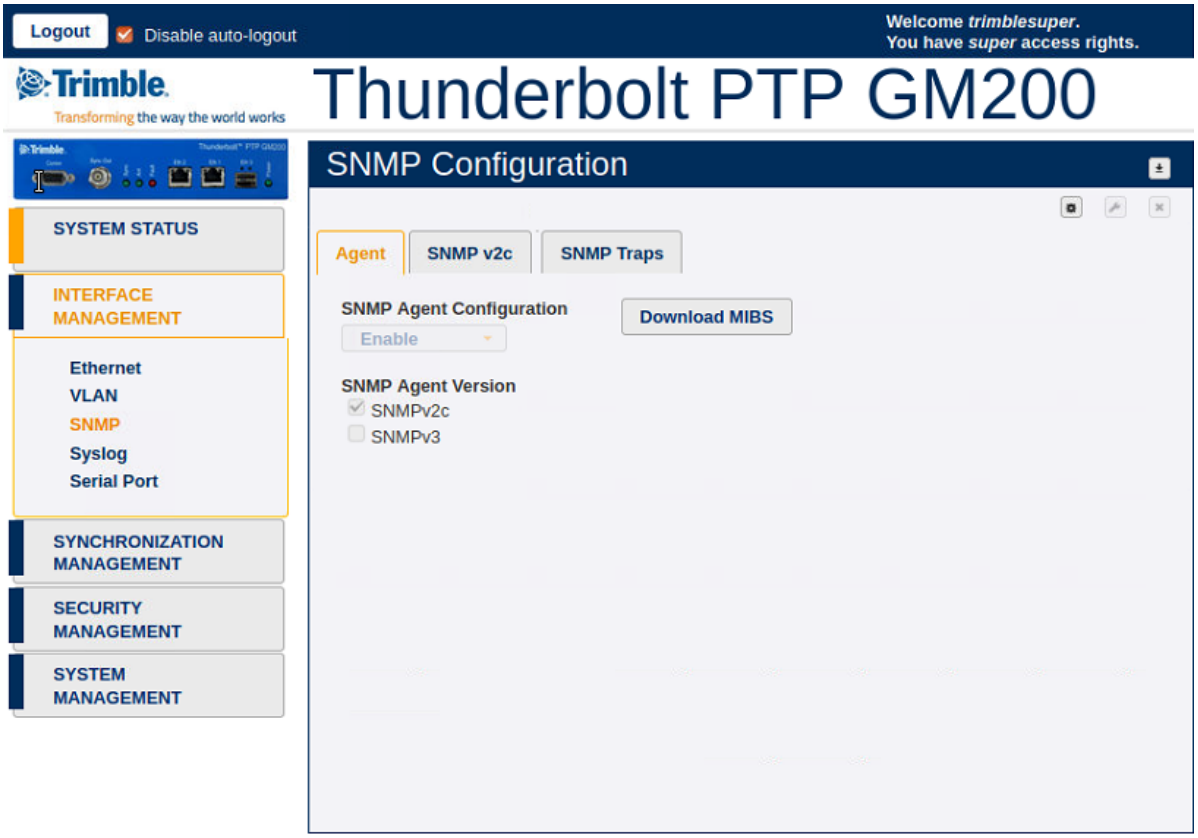


7. Click **Save configuration** to store and restore your configuration after power on reset ❿.

6.5.3 SNMP

6.5.3.1 Agent

To access this tab, select SYSTEM STATUS / SNMP / Agent.



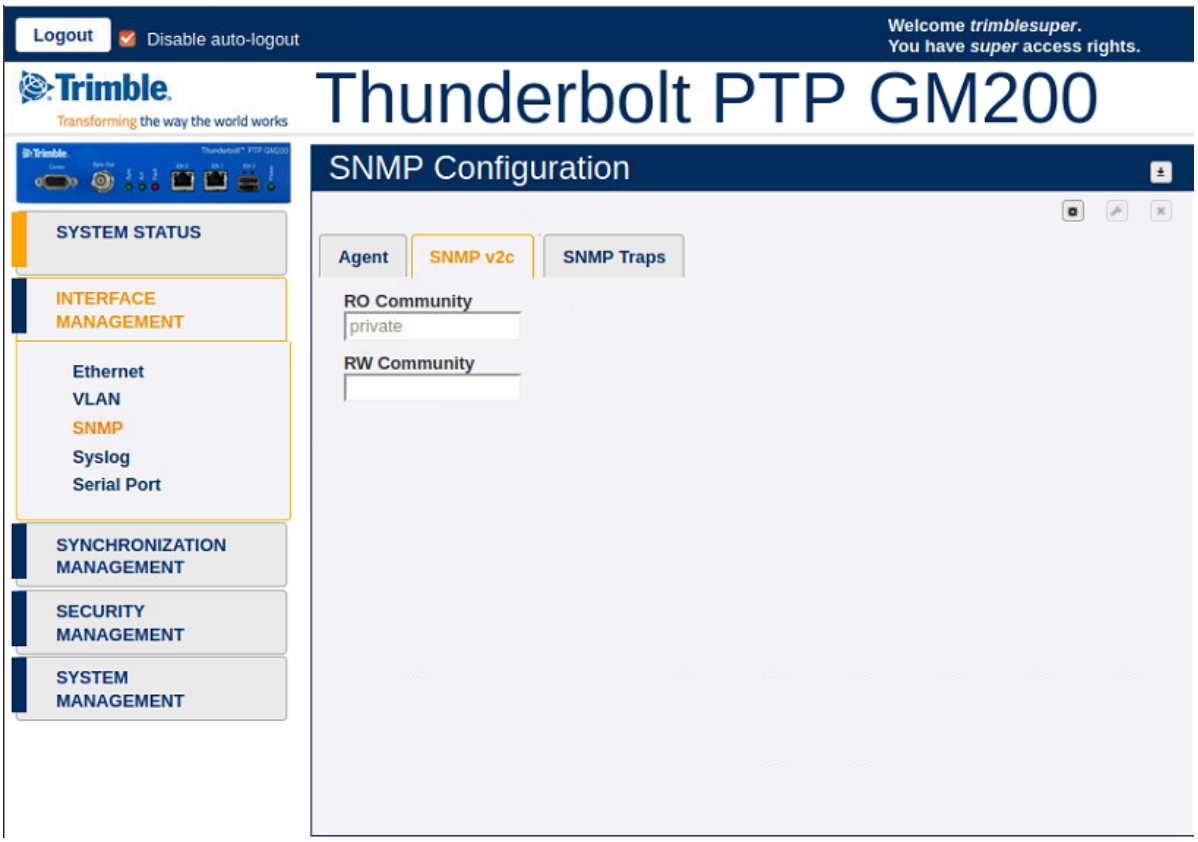
SNMP Configuration: Enable or Disable.

Download MIBS: Download SNMP MIB files.

SNMP Agent Version: Either SNMP v2c or SNMPv3.

6.5.3.2 SNMP v2c

This tab appears if you have configured SNMPv2c in the Agent tab. To access this tab, select SYSTEM STATUS / SNMP / SNMP v2c.

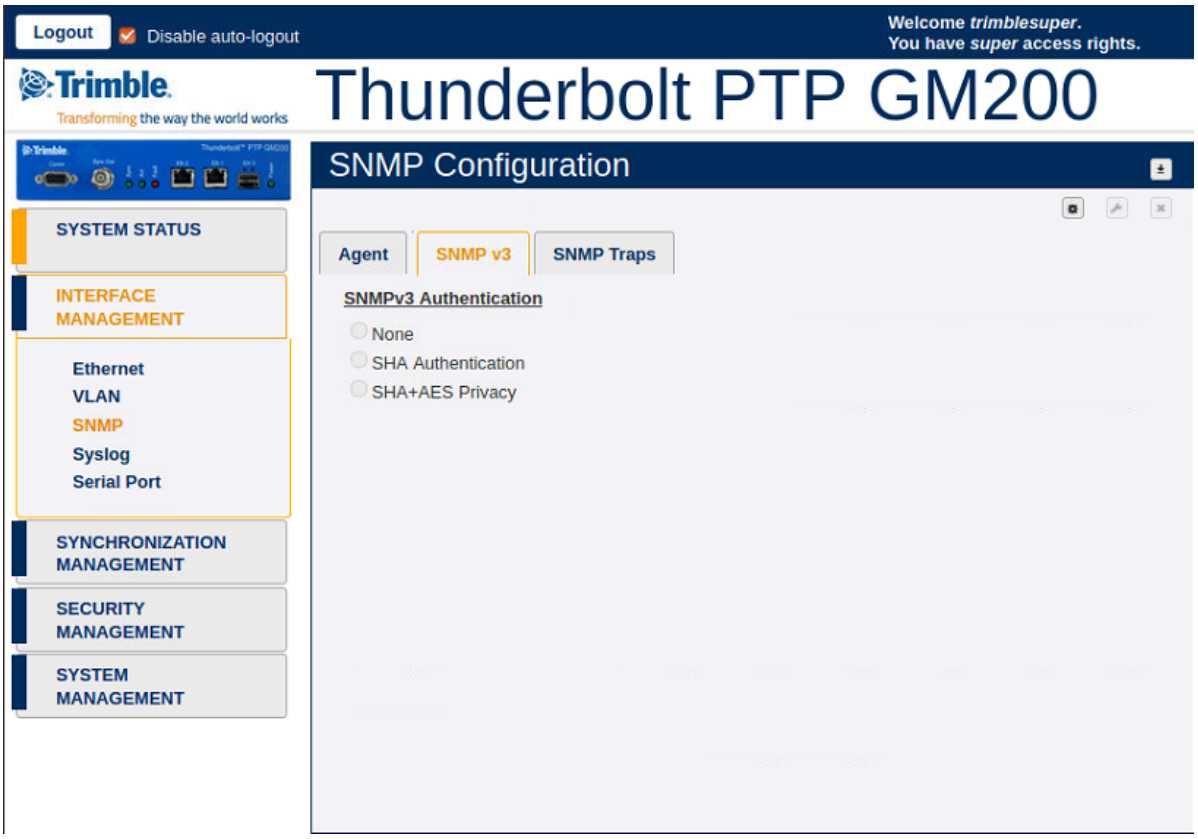


RO Community: Community string for read only.

RW Community: Community string for read and write.

6.5.3.3 SNMP v3

This tab appears if you have configured SNMPv3 in the Agent tab. To access this tab, select SYSTEM STATUS / SNMP / SNMP v3.

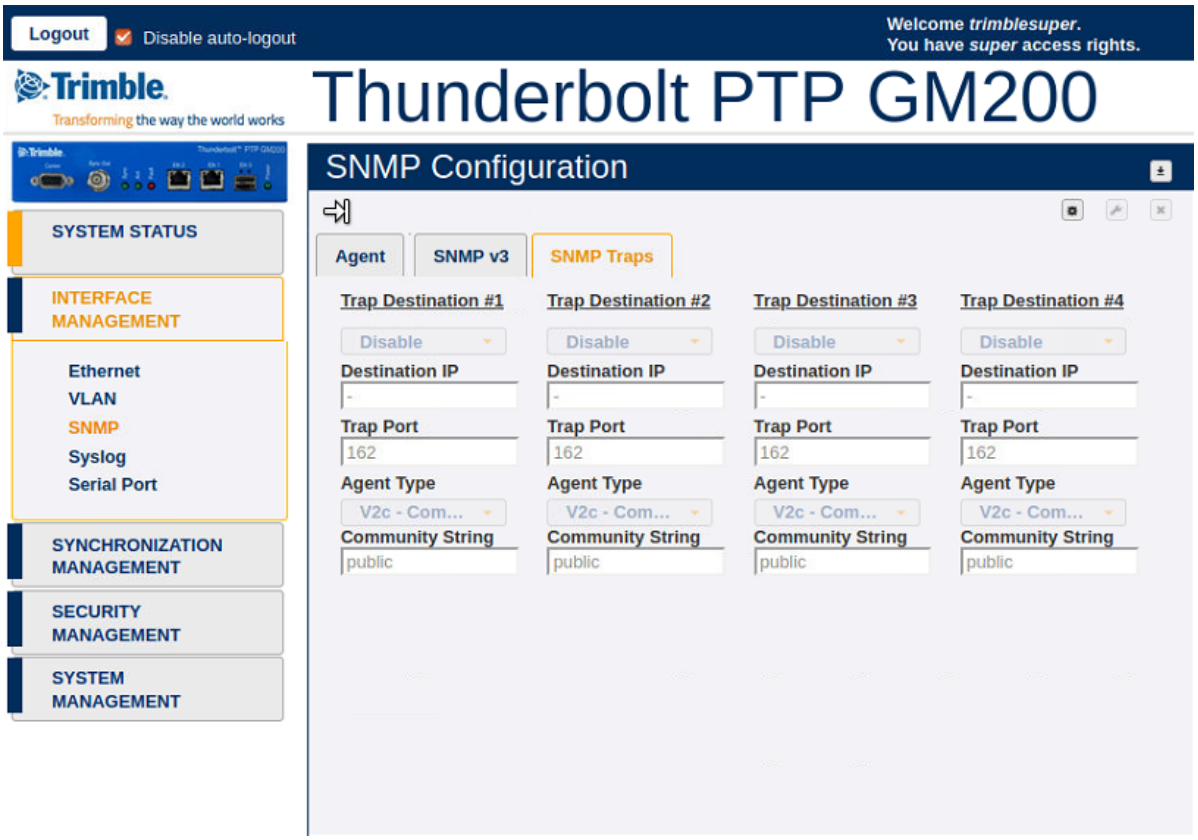


SNMP v3 agent authorization type

- <none>: no authentication (other than username) is required.
- <SHA auth>: SHA password authentication is required.
- <SHA+AES privacy>: SHA password is required and AES encryption is active.

6.5.3.4 SNMP Traps

To access this tab, select INTERFACE MANAGEMENT / SNMP / SNMP Traps.



Trap Destination #n: Enable, Disable, or Default.

SNMP Manager IP: IP address of the SNMP manager that receives the TRAP.

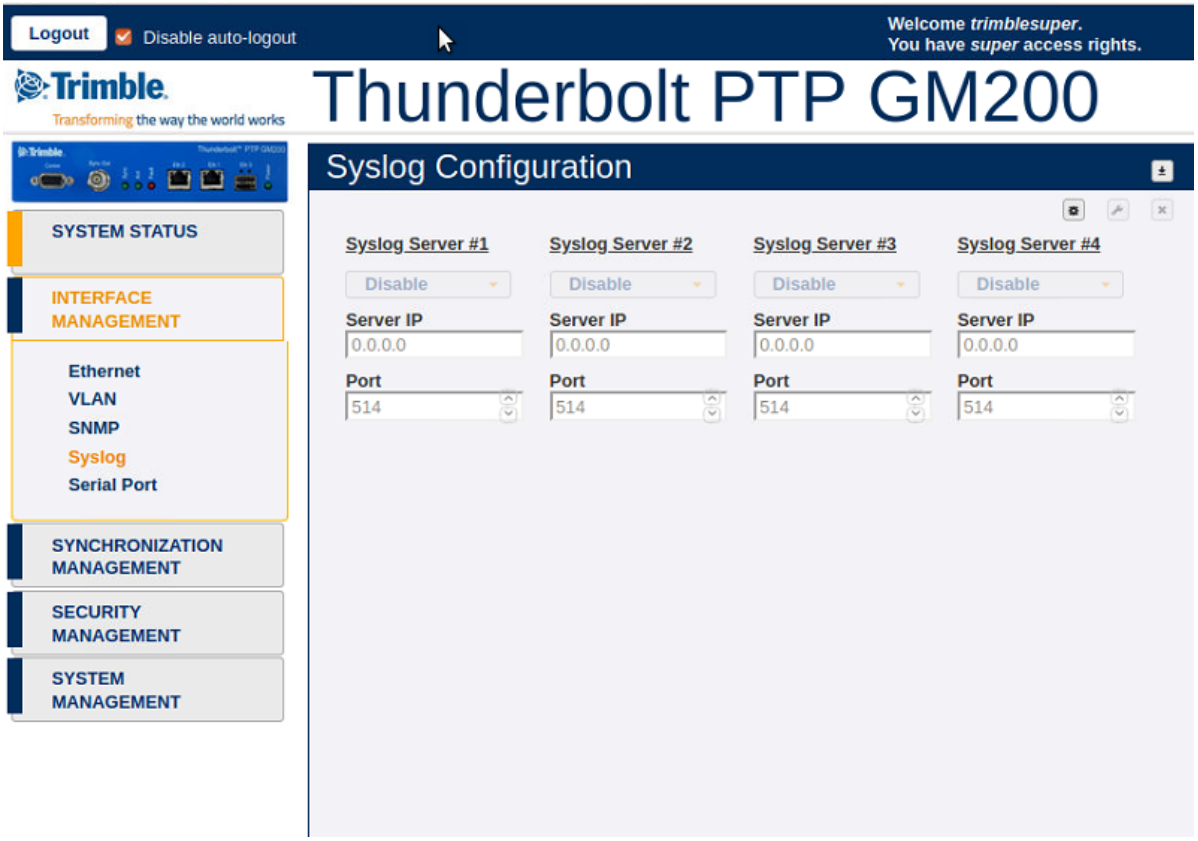
SNMP Manager Port: Port number of the SNMP manager.

Agent Type: V2c-Community, V3-Auth Name(None), V3-Password(SHA), or V3-Privacy(SHA+AES).

Trap Community String: Community string ID for SNMP.

6.5.4 Syslog

To access the **Syslog Configuration** page, select **SYSTEM STATUS** / **Syslog**.



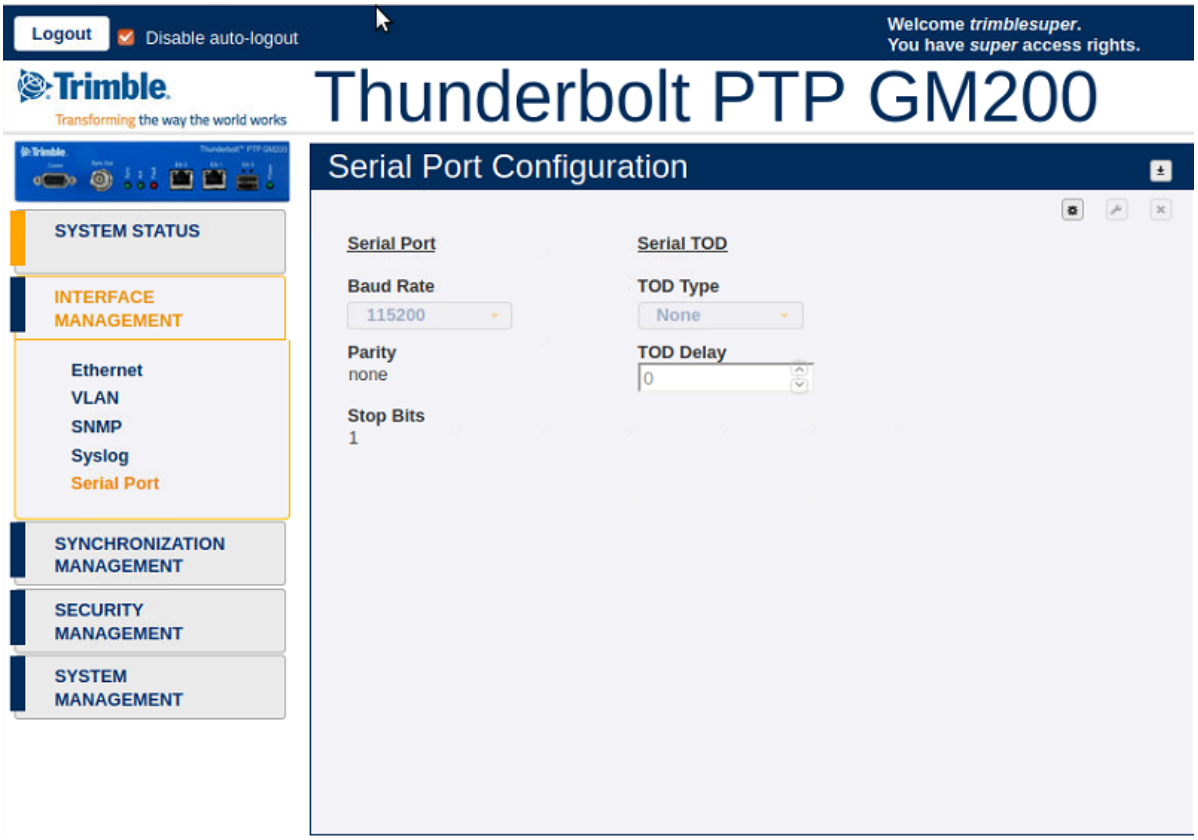
Syslog Protocol: Enable or Disable.

Syslog Server: The IP address of the Syslog server.

Syslog Port: Enter Syslog port.

6.5.5 Serial Port

To access the **Serial Port Configuration** page, select **SYSTEM STATUS** / **Serial Port**.



Baud Rate: Serial port speed – 9600, 19200, 38400, 57600, 115200. The default value is 115200.

Parity: Serial port parity setting – Even, None, or Odd.

Stop Bits: Serial port stop bit setting – 0 or 1.

TOD Type: Sets the serial port to output TOD on demand. This is used with the PPS output on the serial port (on the DCD pin). Option selects the output type and can be one of:

- None – Disable the TOD output (default)
- RMC – Set NMEA RMC output
- ZDA – Set NMEA ZDA output
- GPRMC – Set NMEA GPRMC output

TOD Delay: Set a delay for the TOD output in us (microseconds). This delays the TOD message for <d> us (microseconds) after the PPS.

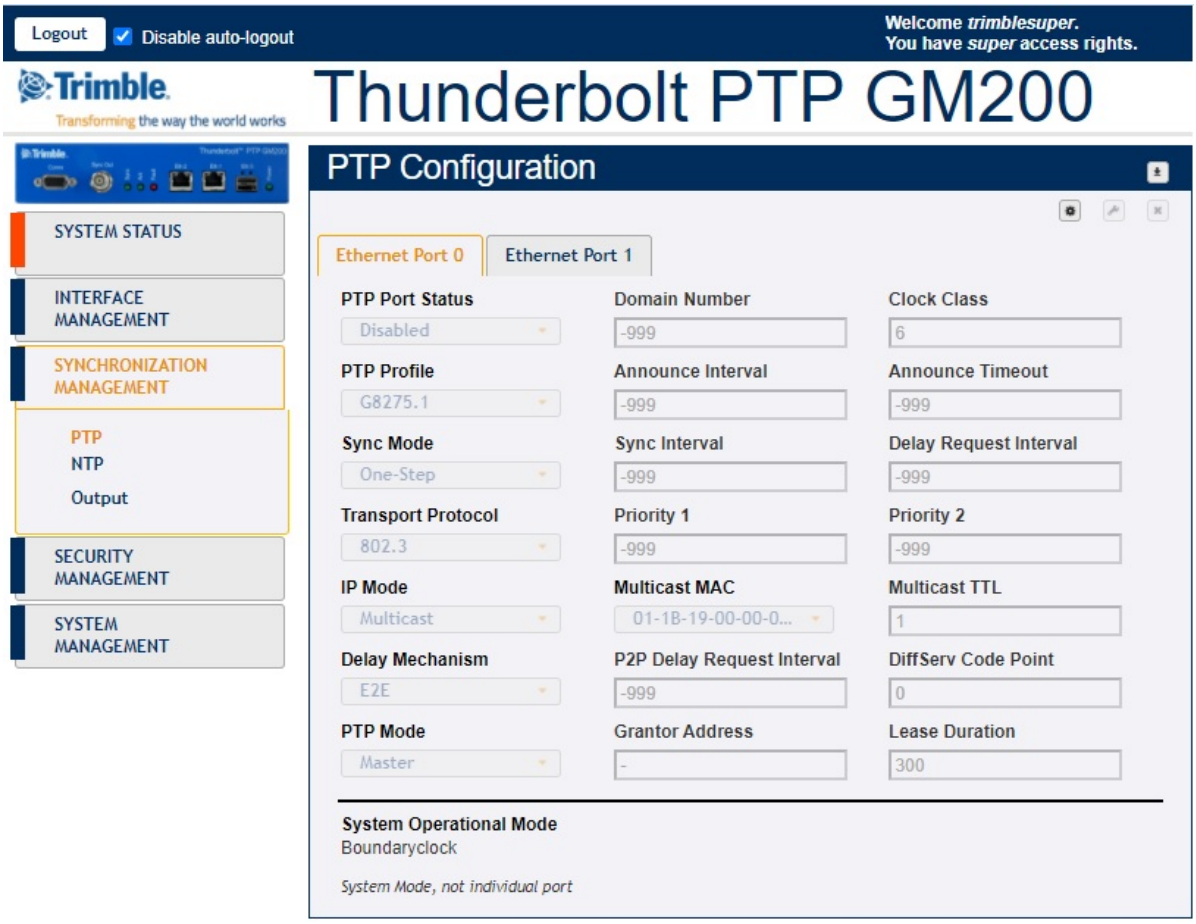
NOTE – The parity and stop bits are for reference only and cannot be configured.

6.6 SYNCHRONIZATION MANAGEMENT menu

6.6.1 PTP

6.6.1.1 Ethernet Port 0

To access this tab, select SYNCHRONIZATION MANAGEMENT / PTP / Ethernet Port 0.



PTP Port Status: PTP port status - Enabled or disabled.

PTP Profile: 1588, G8265-I, G8265–II, telecom, G8275.2, G8275.1, Power, SMPTE, Enterprise or 802.1AS.

Sync Mode: 1-step or 2-Step.

Transport Protocol: Transport mechanism – IPv4, IPv6 or 802.3 (Ethernet).

IP Mode: Multicast, Unicast, or Hybrid.

Delay Mechanism: E2E or P2P.

PTP Mode: Master or Slave clock. Only shows if the System mode is enabled to APTS or Boundary Clock (BC).

> NOTES –
>
> 1. When you configure the APTS or BC mode, you must first configure the PTP slave port and then configure the PTP master port.
> 2. You must reboot the system after the PTP slave mode is enabled. Before reboot the system, save user configuration to restore the current configuration from the system reboot.
> 3. Before the PTP grantor is assigned an IPv6 address, you must set the PTP Transport to IPv6.1.

Domain Number: The PTP domain number.

Announce Interval: Mean time interval between successive announce messages.

Announce Timeout: Mean timeout interval between successive announce messages.

Sync Interval: Mean time interval between successive sync messages.

Delay Request Interval: Mean time interval between delay requests.

P2P Delay Request Interval: Mean time interval between delay requests of peers.

Grantor Address: For PTP unicast input profiles only, IP address (es) of the unicast grandmasters to use as the 'grantor' for the requests.

Multicast MAC: Multicast MAC address selection either Routable (01-1B-19-00-00-00) or Non-Routable(01-80-C2-00-00-0E).

Priority 1: Priority 1 value between 0 and 255.

Priority 2: Priority 2 value between 0 and 255.

Clock Class: View the clock class.

Multicast TTL: Set the multicast ttl value for the transmission (from 1 to 6).

DiffServ Code Point: Diff Serv Code Point.

Lease Duration: For unicast grant messages, set the duration field.

System Operational Mode: GrandMaster, Freerun, or BoundaryClock. This feature is configured through the **System Management**, **System Configuration** tab.

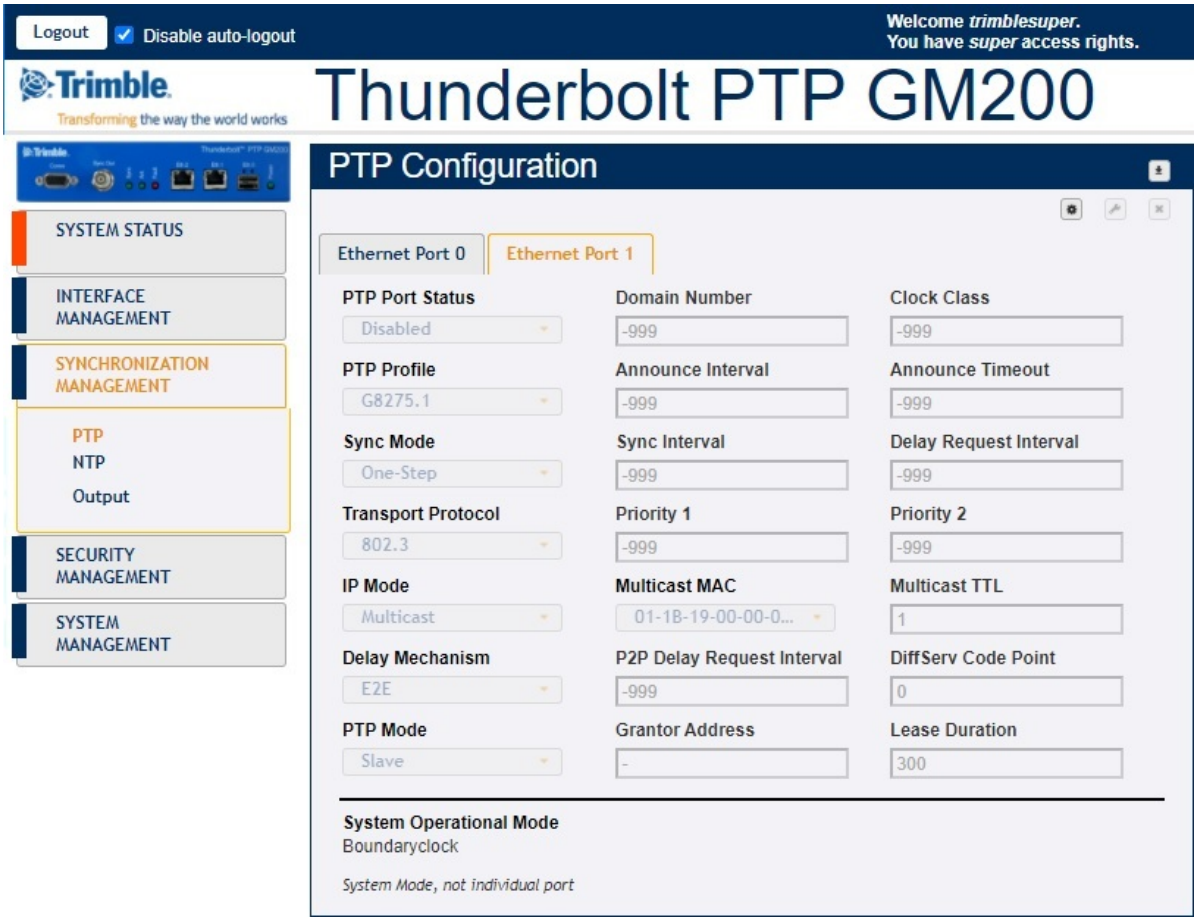
When the operational mode is configured for 'GrandMaster', the system will operate in a traditional GrandMaster manner, requiring a (GNSS) frequency and time reference to be established prior to starting PTP.

When the operational mode is configured for 'freerun', the system will start PTP as soon as the system is booted and interfaces are functional.

When the operational mode is configured for 'BoundaryClock', the system will operate in a Telecom boundary Clock(T-BC), requiring a PTP reference to be established prior to starting PTP.

6.6.1.2 Ethernet Port 1

To access this tab, select SYNCHRONIZATION MANAGEMENT / PTP / Ethernet Port 0.



PTP Port Status: PTP port status - enabled or disabled.

PTP Profile: 1588, G8265-I, G8265–II, telecom, G8275.2, G8275.1, Power, SMPTE, Enterprise or 802.1AS.

Sync Mode: 1-step or 2-Step.

Transport Protocol: Transport mechanism – IPv4, IPv6 or 802.3(Ethernet).

IP Mode: Multicast or Unicast or Hybrid.

Delay Mechanism: E2E or P2P.

PTP Mode: Master or Slave clock. Only showing if the System mode is enabled to APTS or Boundary Clock(BC).

NOTES –

1. When you configure the APTS or BC mode, you must first configure the PTP slave port and then configure the PTP master port.
2. You must reboot the system after the PTP slave mode is enabled. Before reboot the system, save user configuration to restore the current configuration from the system reboot.
3. Before the PTP grantor is assigned an IPv6 address, you must set the PTP Transport to IPv6.

Domain Number: The PTP domain number.

Announce Interval: Mean time interval between successive announce messages.

Announce Timeout: Mean timeout interval between successive announce messages.

Sync Interval: Mean time interval between successive sync messages.

Delay Request Interval: Mean time interval between delay requests.

P2P Delay Request Interval: Mean time interval between delay requests of peers.

Grantor Address: For PTP unicast input profiles only, IP address (es) of the unicast GrandMasters to use as the 'grantor' for the requests.

Multicast MAC: Multicast MAC address selection either Routable (01-1B-19-00-00-00) or Non-Routable(01-80-C2-00-00-0E).

Priority 1: Priority 1 value between 0 and 255.

Priority 2: Priority 2 value between 0 and 255.

Clock Class: View the clock class.

Multicast TTL: Set the multicast ttl value for the transmission (from 1 to 6).

DiffServ Code Point: Diff Serv Code Point.

Lease Duration: For unicast grant messages, set the duration field.

System Operational Mode: GrandMaster, Freerun or BoundaryClock. To configure this feature, select SYSTEM MANAGEMENT / System / System Configuration.

When the operational mode is configured for 'GrandMaster', the system will operate in a traditional GrandMaster manner, requiring a (GNSS) frequency and time reference to be established prior to starting PTP.

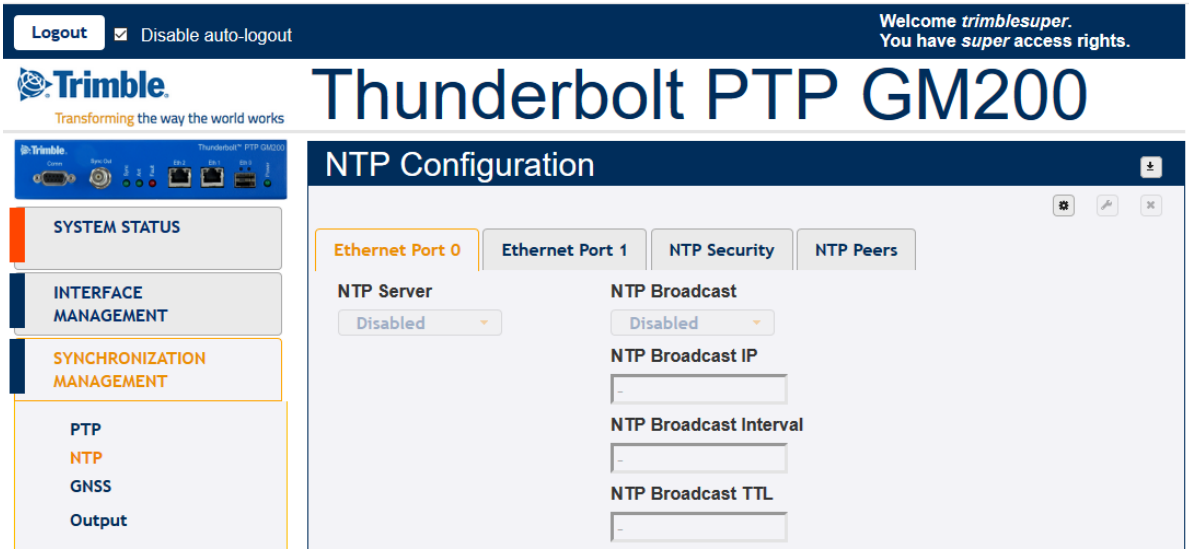
When the operational mode is configured for 'freerun', the system will start PTP as soon as the system is booted and interfaces are functional.

When the operational mode is configured for 'BoundaryClock', the system will operate in a Telecom boundary Clock(T-BC), requiring a PTP reference to be established prior to starting PTP.

6.6.2 NTP

6.6.2.1 Ethernet Port 0

To access this tab, select SYNCHRONIZATION MANAGEMENT / NTP / Ethernet Port 0.



NTP Server: Enabled, Disabled, or Default.

NTP Broadcast: Enabled or Disabled.

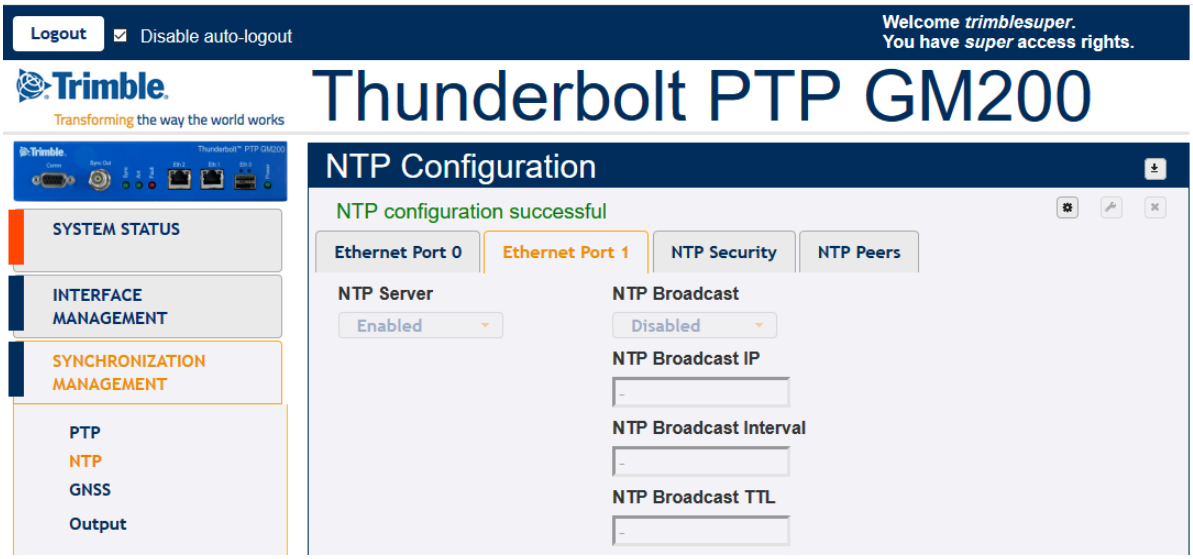
NTP Broadcast IP: Broadcast IP for NTP (must be in the same domain as that of the port).

NTP Broadcast Interval: Values between 4 and 17 representing $2^{\wedge}4$(16 secs) and $2^{\wedge}17$(36.4 hours).

NTP Broadcast TTL: Values between 1 to 7 hops.

6.6.2.2 Ethernet Port 1

To access this tab, select SYNCHRONIZATION MANAGEMENT / NTP / Ethernet Port 1.



NTP Server: Enabled, Disabled, or Default.

NTP Broadcast: Enabled or Disabled.

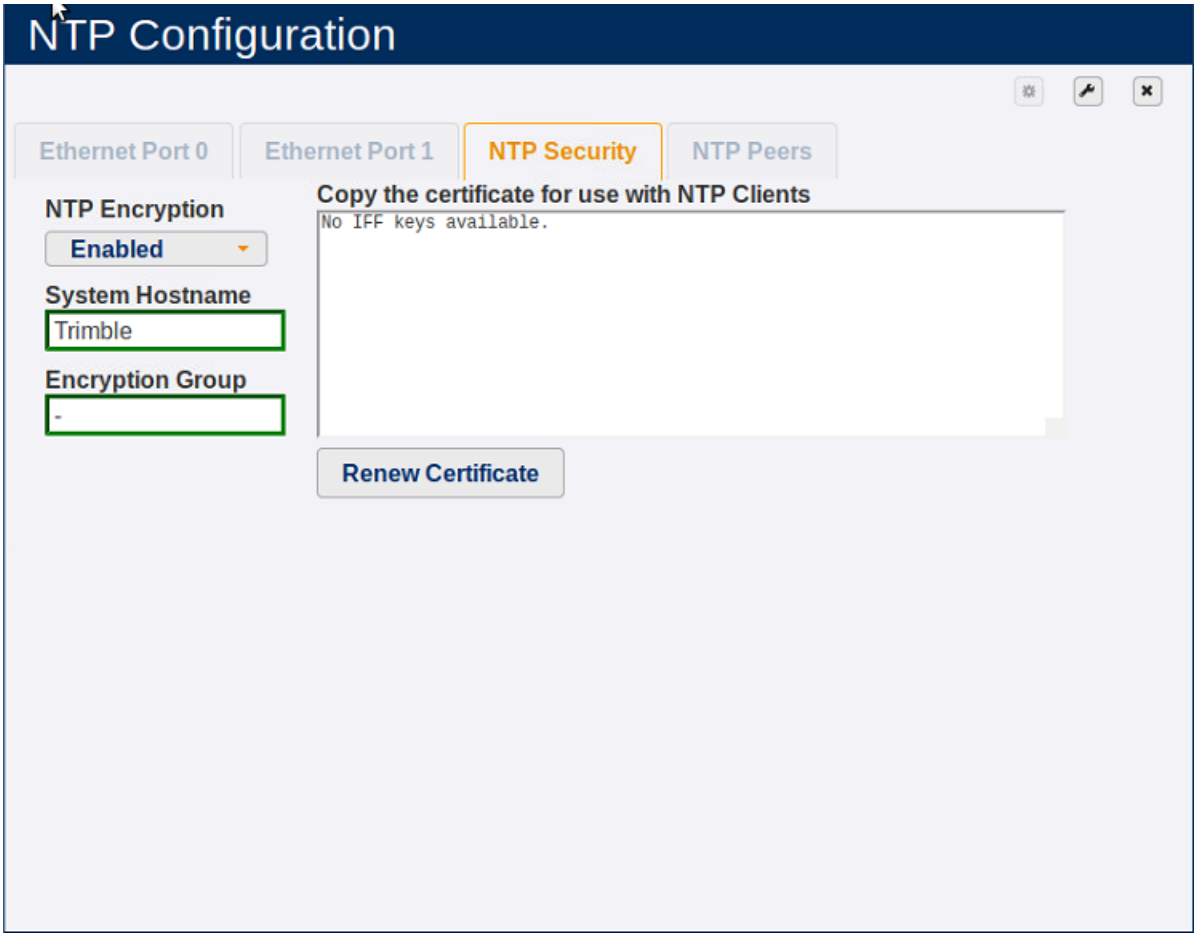
NTP Broadcast IP: Broadcast IP for NTP (must be in the same domain as that of the port).

NTP Broadcast Interval: Values between 4 and 17 representing $2^{\wedge}4$(16 secs) and $2^{\wedge}17$(36.4 hours).

NTP Broadcast TTL: Values between 1 to 7 hops.

6.6.2.3 NTP Security

To access this tab, select SYNCHRONIZATION MANAGEMENT / NTP / NTP Security.



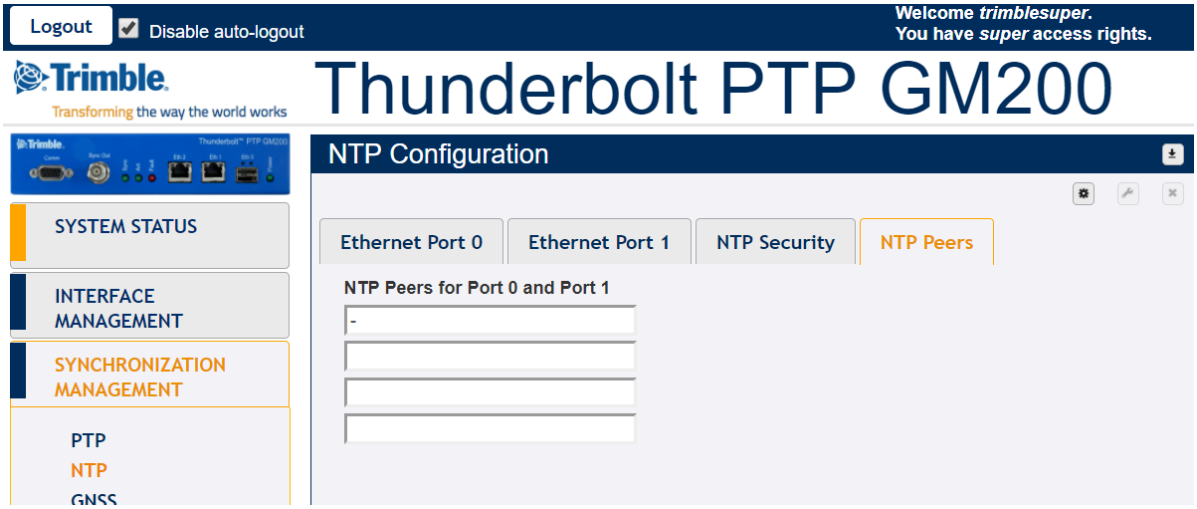
NTP Encryption: Enabled or Disabled. NTP encryption is the public key authentication (autokey).

System Hostname: Host name of the encryption certificate.

Encryption Group: Group name for the encryption certificate.

6.6.2.4 NTP Peers

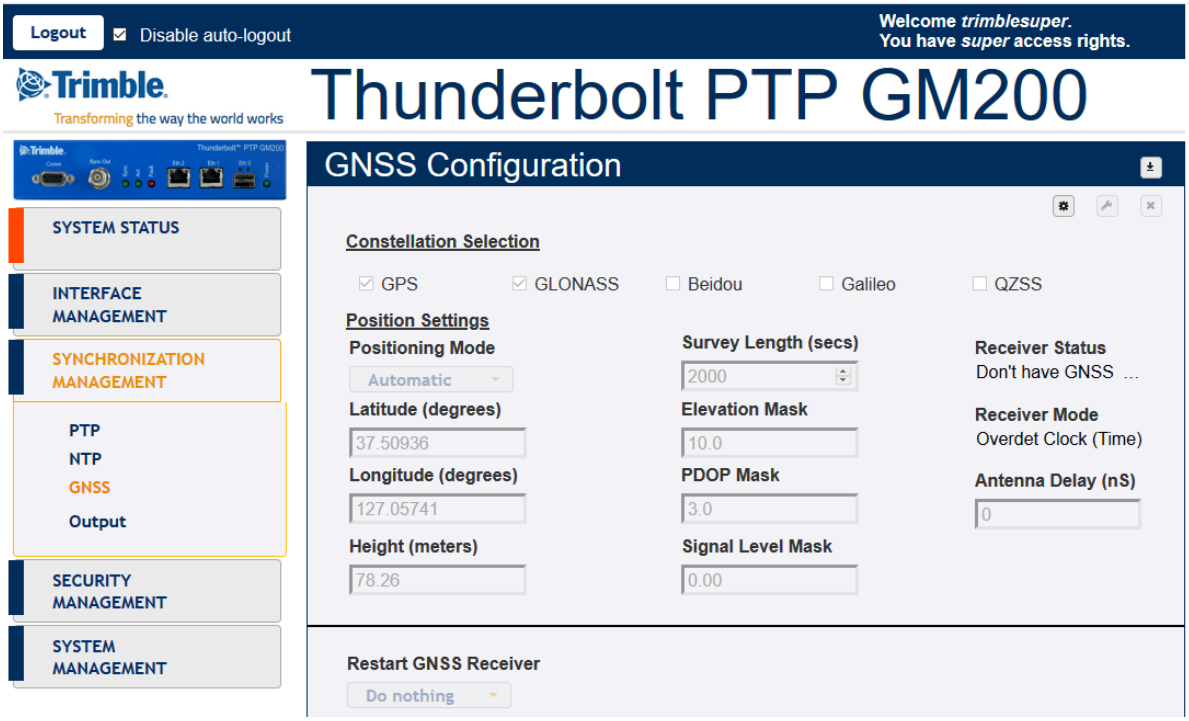
To access this tab, select SYNCHRONIZATION MANAGEMENT / NTP / NTP Peers.



NTP Peers: IP or domain addresses for up to four NTP Peers, valid for Port0 and Port1.

6.6.3 GNSS

To access the **GNSS Configuration** page, select **SYNCHRONIZATION MANAGEMENT** / **GNSS**.



GNSS Constellations: Combination of GPS, GLONASS, Beidou, Galileo, and/or QZSS.

Positioning Mode: Automatic, Survey, Dynamic, or Manual.

Latitude: Latitude in degrees.

Longitude: Longitude in degrees.

Height: Height in meters.

Survey Length: In seconds.

Elevation Mask: Satellite elevation mask level.

PDOP Mask: Satellite PDOP mask level.

Signal Level Mask: Set the signal level mask.

Antenna Delay (ns): The antenna delay setting affects the system time base of the time server. Negative numbers advance the internal time reference, positive numbers retard (delay) the time reference. So, to compensate for an antenna delay of 500 ns you would enter -500 as the antenna delay setting.

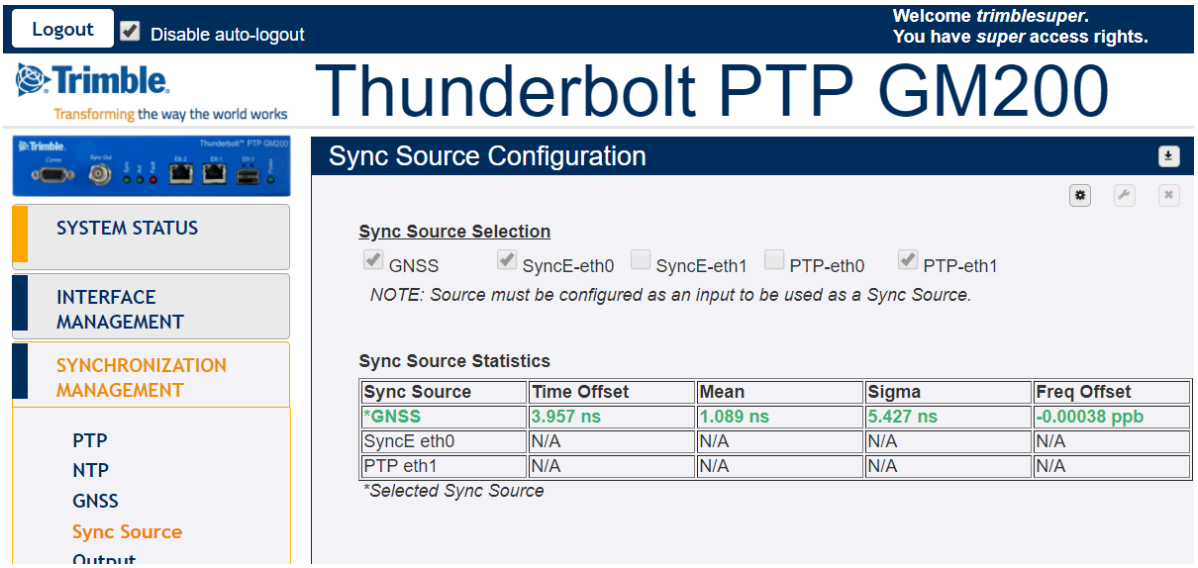
All PTP and NTP timestamps are derived from the system time base, which means that you want to make sure that the antenna delay is correctly compensated because that value affects the PTP and NTP clock accuracy in the LAN network.

Note that, since this setting affects the disciplined oscillator of the time server, the effect of changing the antenna delay value is not seen immediately on the system output. The antenna delay value will advance (or retard) the internal GNSS time measurements, which go into the oscillator's PLL control loop, which will then gradually steer the disciplined oscillator toward that new value. If the value is jumped too far after the time server has achieved lock (remember, this is normally an installation setting), then the unit may issue a "PPS-Sync-Bad" and/or a "Freq-Loop-Unlock" alarm. After a while, when the time base has moved to the new value, these alarms will be cleared.

Restart GNSS Engine: Warm, Cold, or Do Nothing.

6.4.4 Sync Source

To access the **Sync Source Configuration** page, select **SYNCHRONIZATION MANAGEMENT** / **Sync Source**.



Sync Source Selection: You can select or deselect the available Inputs of the system:

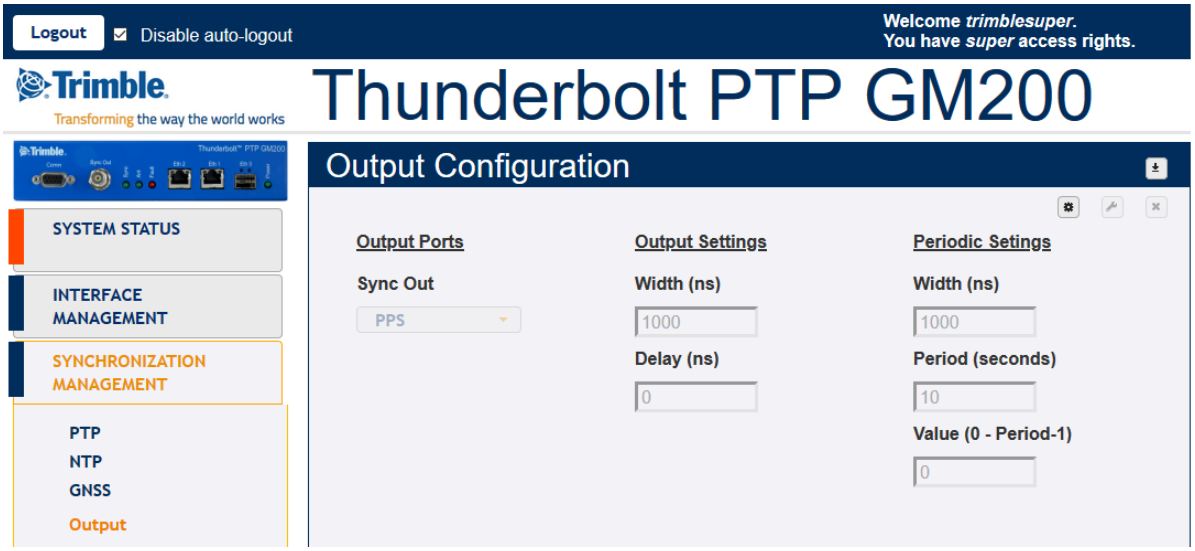
- GNSS
- SyncE-eth0
- SyncE-eth1

- PTP-eth0
- PTP-eth1

Sync Source Statistics: Shows the selected Sync Source actually used by the time server.

6.6.5 Output

To access the Output Configuration page, select SYNCHRONIZATION MANAGEMENT / Output.



BNC Output: The type of output signal – PPS, PP2S, Periodic, or 10 MHz.

Output Width: Width of Output in nS.

Output Delay: Delay of Output in nS. The output delay setting, only affects the PPS pulse on the BNC connector. That value does NOT affect the system time base and has no effect on the PTP and NTP timestamps. Negative numbers advance the PPS pulse, positive numbers retard (delay) the PPS pulse. The output delay can be used for application-specific adjustments of the PPS timing, for example the length of cable that is attached to the BNC output for conducting the PPS pulse signal. It has only a local impact, though. Clients in the LAN network will not see any effect from this value.

The output delay setting has an immediate effect on the PPS pulse.

The output delay setting should NOT be used for compensating the antenna delay!

Periodic Width: Periodic width in ns.

Period: Period in seconds.

Periodic Value: Periodic value.

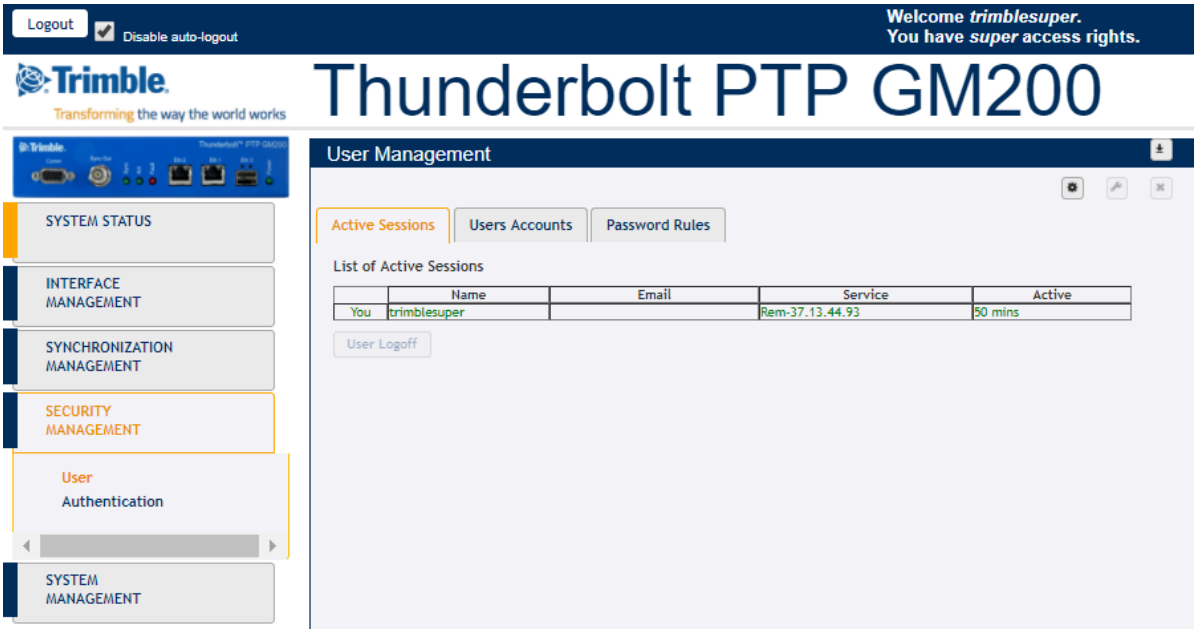
6.7 SECURITY MANAGEMENT menu

6.7.1 User

Use this option to manage users.

6.7.1.1 Active Sessions

To access this tab, select SECURITY MANAGEMENT / User / Active Sessions.



Name: Existing username.

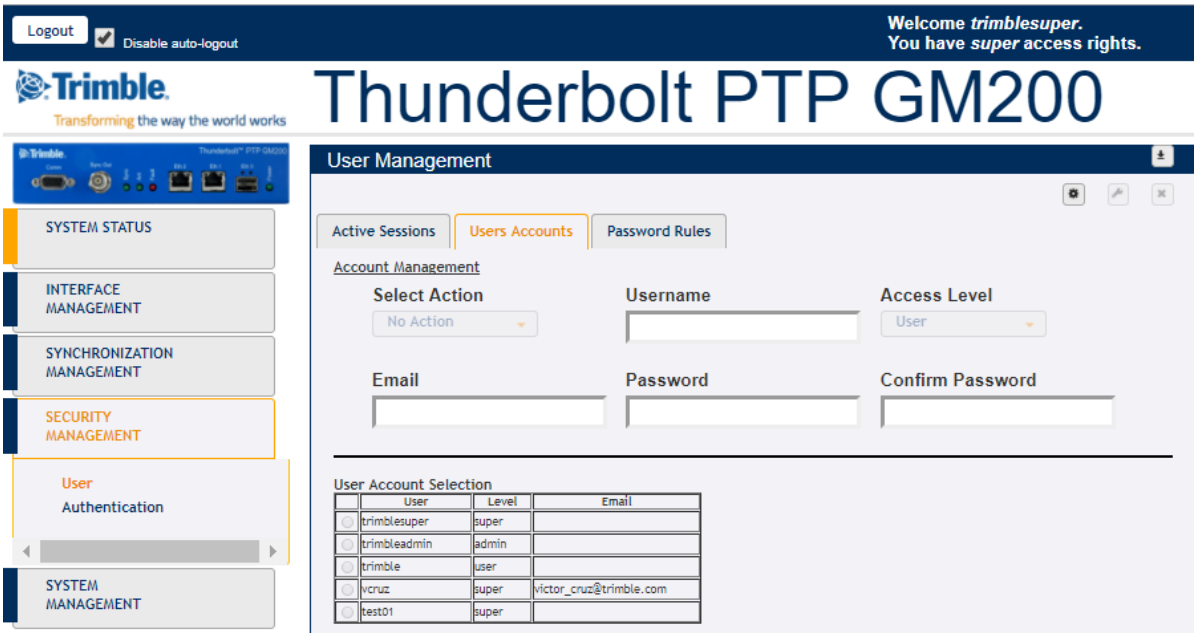
Email: Updated email address.

Service: The IP address used to connect to.

Active: The time that the session has been active.

6.7.1.2 Users Accounts

To access this tab, select SECURITY MANAGEMENT / User / Users Accounts.



Select Action: No Action, Add, Modify, Delete.

Username: New username to be added.

Password: New password to be chosen.

Confirm Password: Confirm password. Should be same as password.

Access Level: User, Admin or Super(visor).

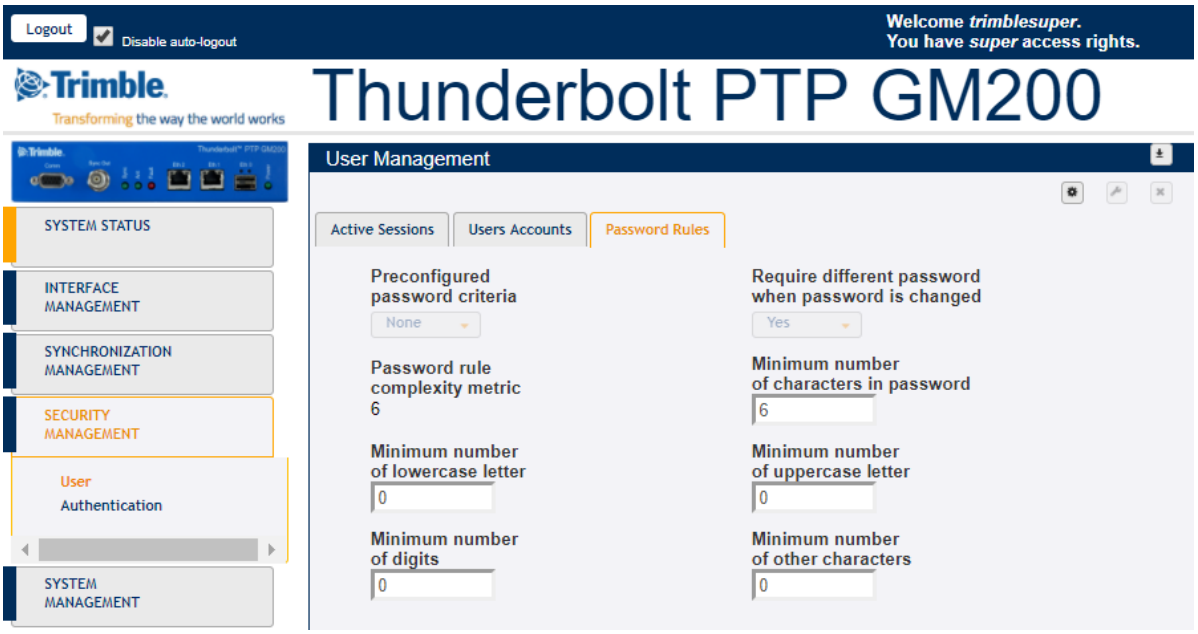
- User – This level can only view status and configuration, cannot make changes to configuration.
- Admin – All functions of 'user' with added ability to change most configuration settings.
- Super – All functions of 'admin' with added ability to edit the user table.

Email: New email.

User Account Selection: This is a list of all users created in the time server.

6.7.1.3 Password Rules

To access this tab, select SECURITY MANAGEMENT / User / Password Rules.



Preconfigured password criteria: Five criteria of password already configured:

- None: The password does not require any rule to be accepted by the time server
- p0: 6 characters as minimum (complexity = 6).
- p1: 7 characters as minimum, one uppercase letter as minimum (complexity 8).
- p2: 9 characters as minimum, one uppercase letter as minimum, two lowercase letters as minimum (complexity 12).
- p3: 10 characters as minimum, one uppercase letter as minimum, two lowercase letters as minimum, one digit as minimum (complexity 14).
- p4: 11 characters as minimum, one uppercase letter as minimum, two lowercase letters as minimum, one digit as minimum, one other character as minimum (complexity 16).

Require different password when password is changed: Yes or No. It sets if the user is required to enter a different password when changing their password.

Password rule complexity metric: The sum of all conditions configured.

Minimum number of characters in password: Password requires <n> characters as minimum.

Minimum number of lowercase letter: password requires <n> lowercase letters as minimum.

Minimum number of uppercase letter: password requires <n> uppercase letters as minimum.

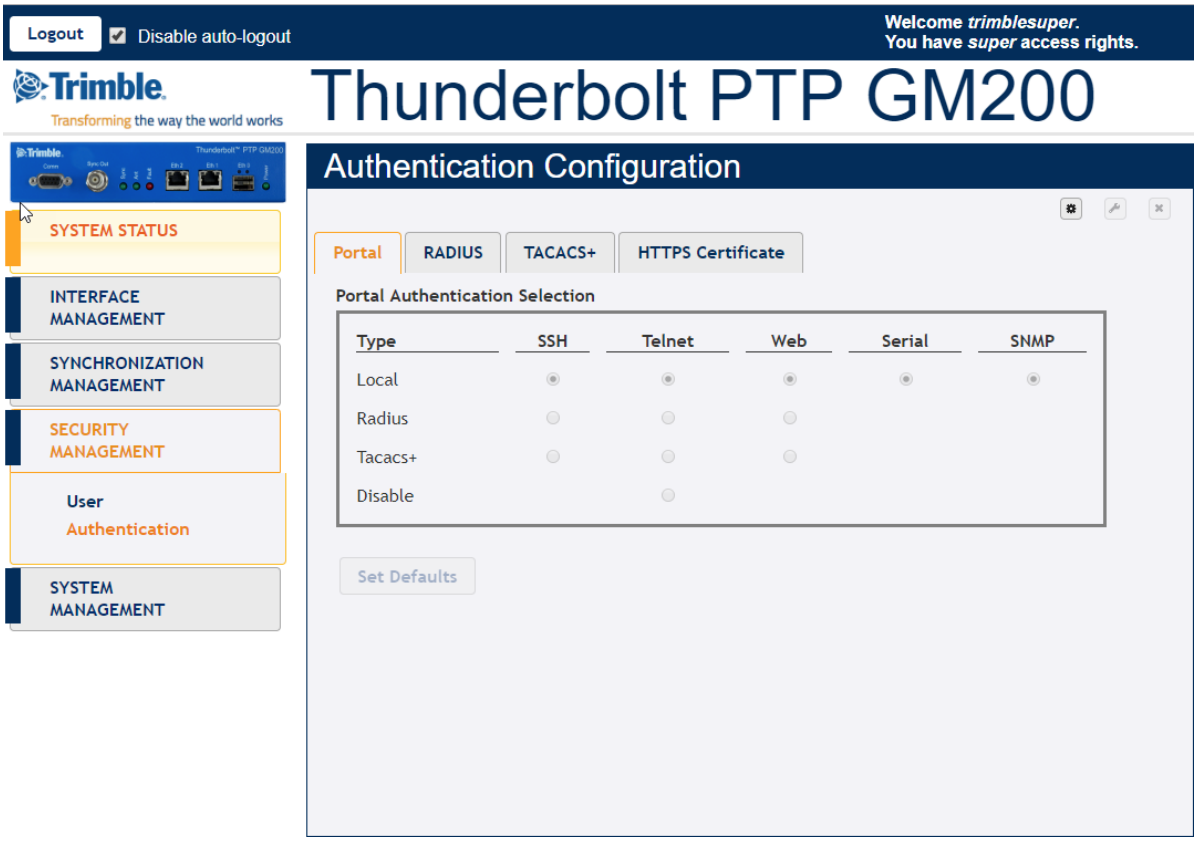
Minimum number of digits: password requires <n> digits as minimum.

Minimum number of other characters: password requires <n> other characters as minimum. These other characters can be any printable character, except for space.

6.7.2 Authentication

6.7.2.1 Portal

To access this tab, select SECURITY MANAGEMENT / Authentication / Portal.



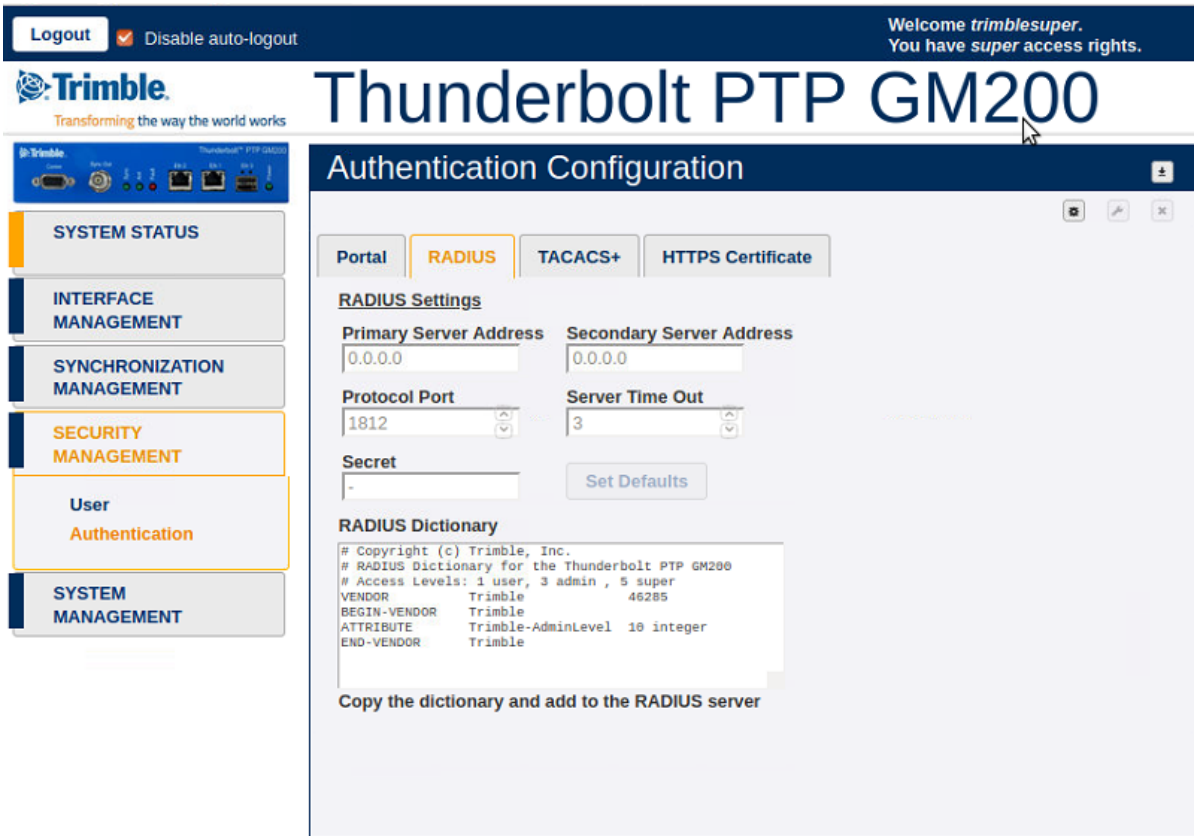
This page shows the authentication type Local, Radius, or TACACS+ with the three different portal types: SSH, Telnet, or Web.

Set Defaults button sets the authentication to the default values.

Disable option allow to disable telnet access to the time server.

6.7.2.2 RADIUS

To access this tab, select SECURITY MANAGEMENT / Authentication / RADIUS.



Primary Address: Displays or allows to enter the primary server address for the RADIUS server.

Secondary Address: Displays or allows to enter the secondary server address for the RADIUS server.

Protocol Port: Displays or allows to set the IP port for the RADIUS server.

(same for primary and secondary).

Server Time Out: Sets the RADIUS server timeout value. 1 to 60 seconds.

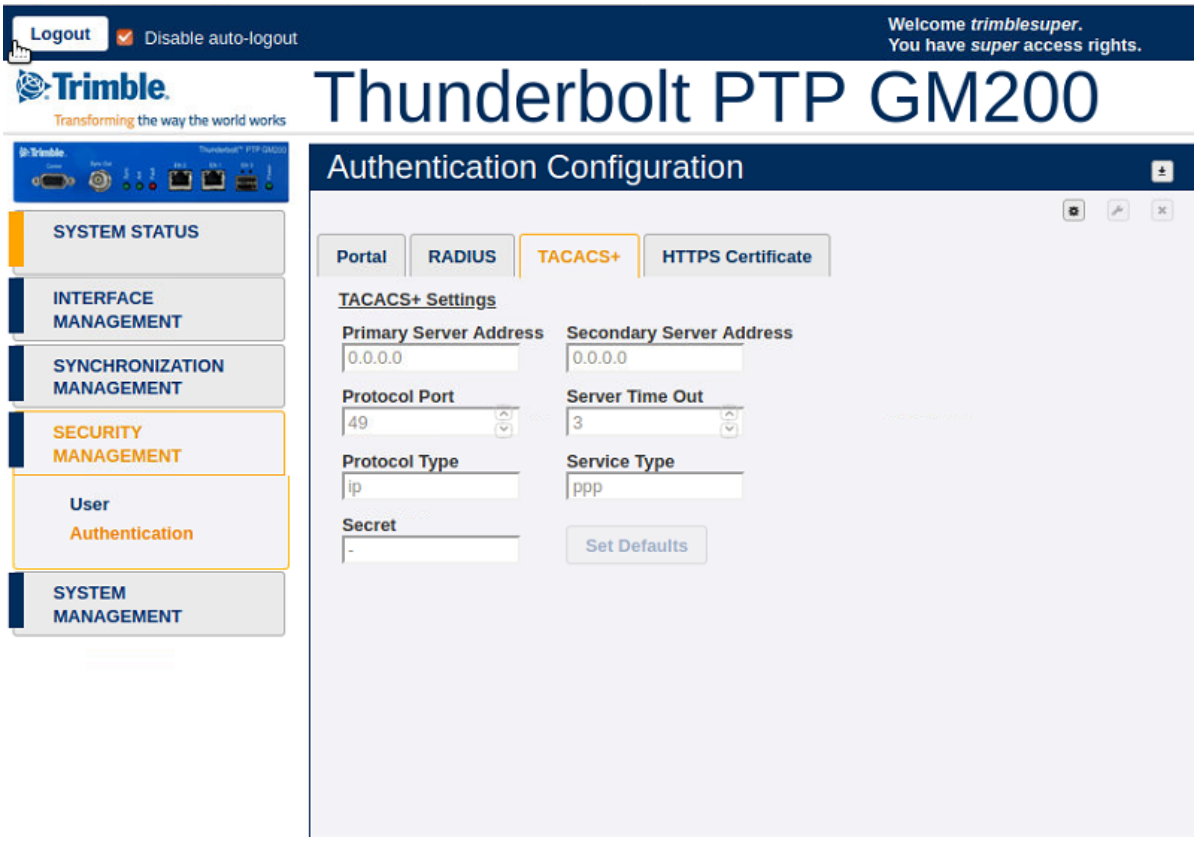
Secret: Sets the shared secret value for the RADIUS server.

RADIUS Dictionary

Set Defaults button: Sets the RADIUS server information to defaults.

6.7.2.3 TACACS+

To access this tab, select SECURITY MANAGEMENT / Authentication / TACAS+.



Primary Address: Displays or allows to enter the primary server address for the TACACS+ server

Secondary Address: Displays or allows to enter the secondary server address for the TACACS+ server

Protocol Port: Displays or allows to set the IP port for the TACACS+ server (same for primary and secondary)

Server Time Out: Sets the TACACS+ server timeout value. 1 to 60 seconds.

Protocol Type: Sets the TACACS+ server protocol string

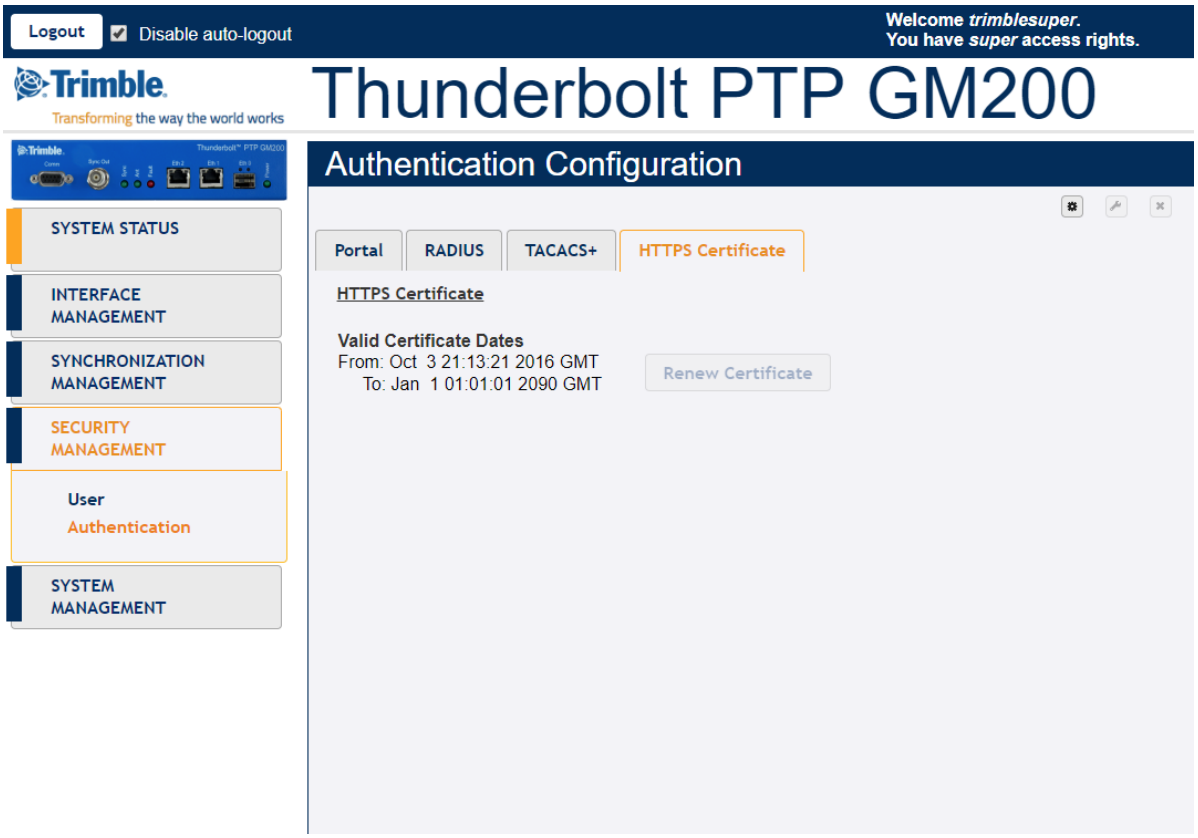
Service Type: Sets the TACACS+ server service string

Secret: Sets the shared secret value for the TACACS+ server

Set Defaults Button: Sets the TACACS+ server information to defaults.

6.7.2.4 HTTPS Certificate

To access this tab, select SECURITY MANAGEMENT / Authentication / HTTPS Certificate.



Renew Certificate: Displays or allows to enter the primary server address for the TACACS+ server.

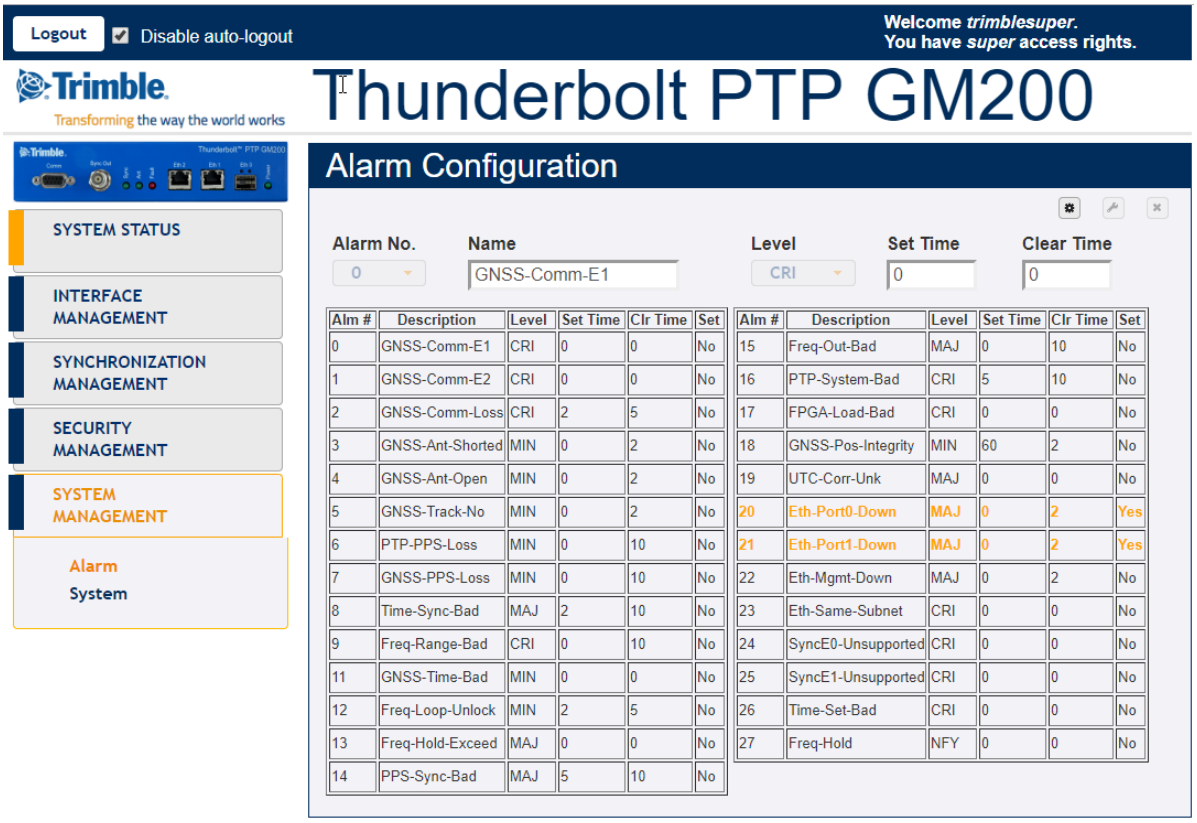
Regenerate the HTTPS certificate. This will force web users to re-establish web access with the new certificate. The previous Trimble certificate must be removed from the browser, then the user will need to reconnect to the system with their browser. The certificate's valid 'From' and 'To' date range is displayed.

6.8 SYSTEM MANAGEMENT menu

6.8.1 Alarm

The table on this page shows the list of available alarms along with their current level, and the set and clear time. You can also change the severity level, and the set and clear time.

To access the Alarm Configuration page, select SYSTEM MANAGEMENT / Alarm.



Alm #	Description	Level	Set Time	Clr Time	Set
0	GNSS-Comm-E1	CRI	0	0	No
1	GNSS-Comm-E2	CRI	0	0	No
2	GNSS-Comm-Loss	CRI	2	5	No
3	GNSS-Ant-Shorted	MIN	0	2	No
4	GNSS-Ant-Open	MIN	0	2	No
5	GNSS-Track-No	MIN	0	2	No
6	PTP-PPS-Loss	MIN	0	10	No
7	GNSS-PPS-Loss	MIN	0	10	No
8	Time-Sync-Bad	MAJ	2	10	No
9	Freq-Range-Bad	CRI	0	10	No
11	GNSS-Time-Bad	MIN	0	0	No
12	Freq-Loop-Unlock	MIN	2	5	No
13	Freq-Hold-Exceed	MAJ	0	0	No
14	PPS-Sync-Bad	MAJ	5	10	No

Alm #	Description	Level	Set Time	Clr Time	Set
15	Freq-Out-Bad	MAJ	0	10	No
16	PTP-System-Bad	CRI	5	10	No
17	FPGA-Load-Bad	CRI	0	0	No
18	GNSS-Pos-Integrity	MIN	60	2	No
19	UTC-Corr-Unk	MAJ	0	0	No
20	Eth-Port0-Down	MAJ	0	2	Yes
21	Eth-Port1-Down	MAJ	0	2	Yes
22	Eth-Mgmt-Down	MAJ	0	2	No
23	Eth-Same-Subnet	CRI	0	0	No
24	SyncE0-Unsupported	CRI	0	0	No
25	SyncE1-Unsupported	CRI	0	0	No
26	Time-Set-Bad	CRI	0	0	No
27	Freq-Hold	NFY	0	0	No

Alarm No.: Select the alarm number to be configured.

Level: IGN(ignored), NFY(notification), MIN(minor), MAJ(major), or CRI(critical).

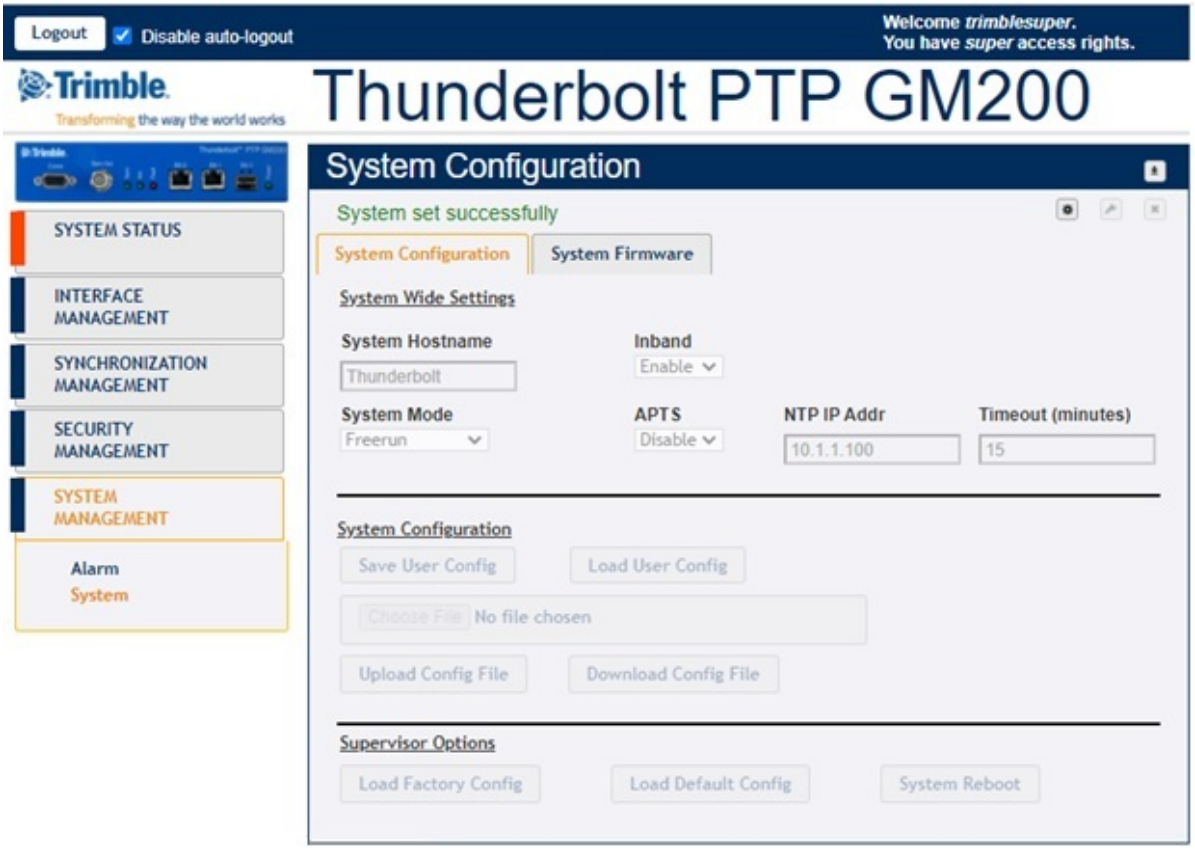
setTime: Time for which the alarm condition must be active before it is set.

clrTime: Time for which the alarm condition is inactive before it is cleared.

6.8.2 System

6.8.2.1 System Configuration

To access this tab, select SYSTEM MANAGEMENT / System / System Configuration.



Use this tab to configure the system with following options:

System Hostname: Enter the hostname.

System Mode: Change the system operating mode for Freerun, GrandMaster or BoundaryClock. See the description in the section.

Inband: To set the Inband management configuration. This sets the Inband management on Eth0 and Eth1.

APTS: To set the APTS (Assisted Partial Timing Support) mode. See the description in the PTP Slave operation section.

Save User Configuration: Store the current user settings to be the defaults used on a system restart.

Load User Config: Restore the previously saved user configuration.

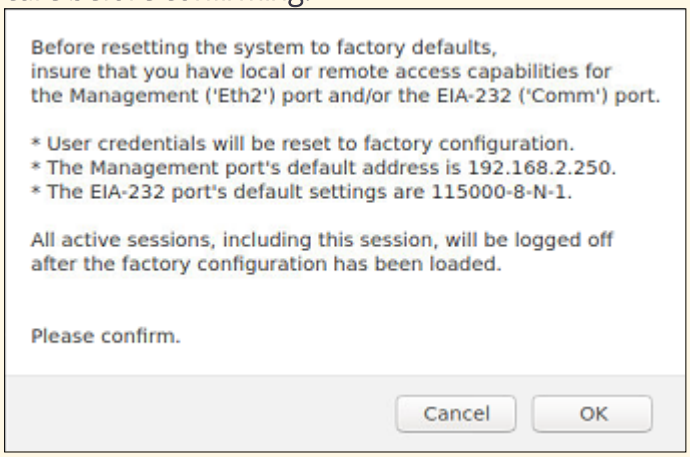
Upload Config File: Load the file selected after clicking Browse.

Download Conf File: Download a user configuration file that can later be uploaded through **Upload Config File**.

Load Default Config: To set factory configuration, ***except network config***. This restores settings to those configured during Trimble production, ***except the network config***.

Load Factory Config: To set factory configuration. This restores settings to those configured during Trimble production.

CAUTION – The pop-up window shows the changes that will occur. Take care before confirming.

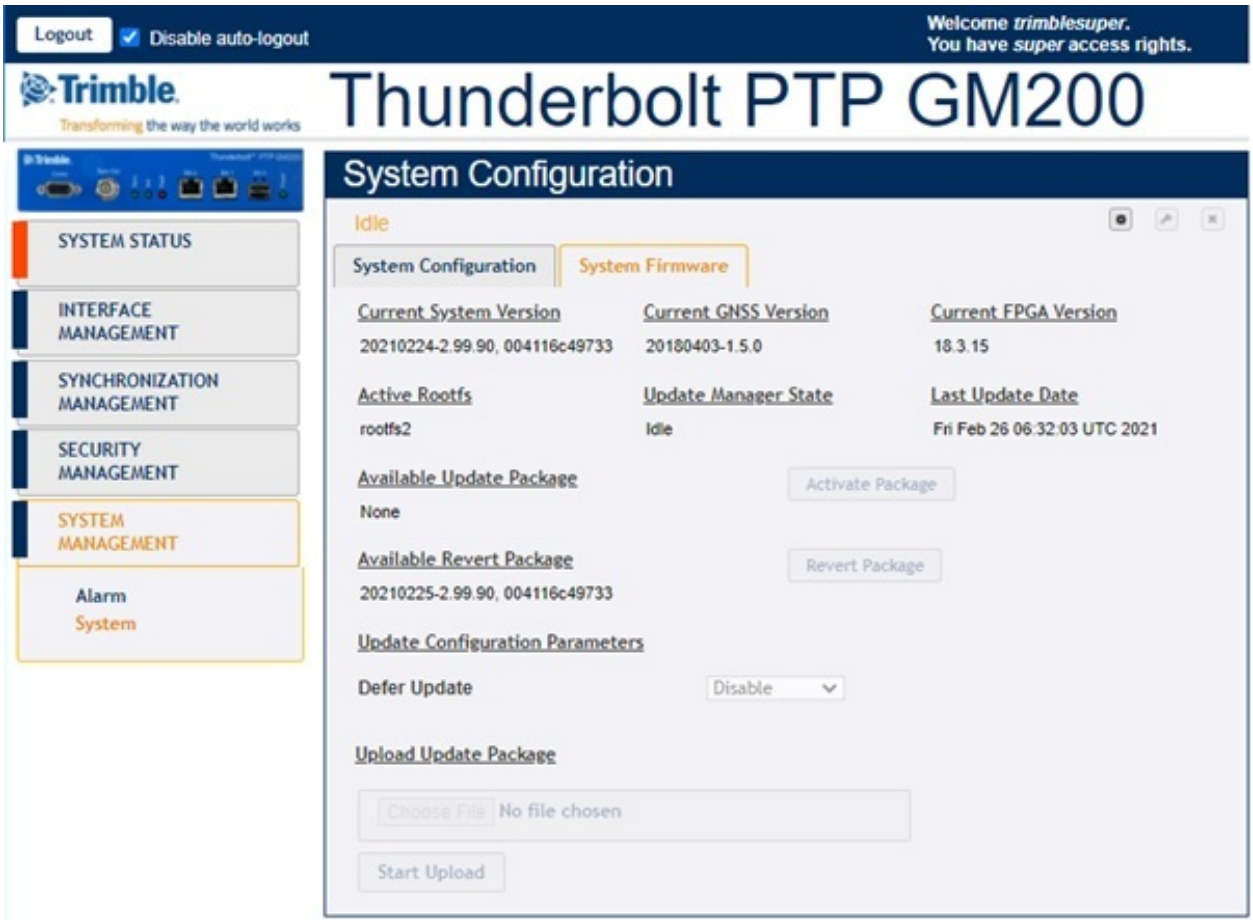


System Reboot: Reboot the system.

6.8.2.2 System Firmware

This tab displays the **Current System Version**, the **Current GNSS Version**, and **Current FPGA Version**. From this tab, you can also upload firmware patches to the system.

To access this tab, select **SYSTEM MANAGEMENT** / **System** / **System Firmware**.



Active Rootfs: Display the activated partition where the current activated firmware is placed. 'rootfs1' or 'rootfs2'.

Update Manager State: Display the current firmware upgrade status.

Activate Package: Activate the uploaded package that is shown in the **Available Update Package** field.

Revert Package: Activate the package that is shown at the **Available Revert Package** field.

Defer Update: If this option is set to Disable, then patches are automatically uploaded and activated. If you select the Enable option, patches are not automatically uploaded and activated; you need to manually activate the patches after the firmware is updated.

Choose File: Choose a firmware image to be upgraded.

Start Upload: Start updating the firmware.

NOTE – The **System Firmware** tab is available when logged in with supervisor user-level access.

NOTE – The firmware update restarts the system, which will cause a loss of network timing output.

7. SNMP Support

This chapter describes the SNMP and SNMP notification setting procedure.

7.1 SNMP overview

Simple Network Management Protocol (SNMP) is an Internet-standard application-layer protocol for managing and monitoring network elements. It has been defined by the Internet Engineering Task Force (IETF) under RFC 1157 for exchanging management information between network devices.

An SNMP-managed network consists of three key components:

- Managed device
- Agent – software that runs on managed devices
- Network management station (NMS) – software that runs on the manager

SNMP agents expose management data on the managed systems as variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The time server supports SNMP v2c.

7.2 SNMP traps

SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

The time server provides a command line interface to enable the traps. (See Command Line Interface Reference, page 69).

Following is a list of available alarms through an SNMP trap.

7.2.1 Description: Set alarm 0, GNSS-Comm-E1 (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.2 Description: Clear alarm 0, GNSS-Comm-E1 (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.3 Description: Set alarm 1, GNSS-Comm-E2 (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.4 Description: Clear alarm 1, GNSS-Comm-E2 (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.5 Description: Set alarm 2, GNSS-Comm-Loss (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.6 Description: Clear alarm 2, GNSS-Comm-Loss (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.7 Description: Set alarm 3, GNSS-Ant-Shorted (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.8 Description: Clear alarm 3, GNSS-Ant-Shorted (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.9 Description: Set alarm 4, GNSS-Ant-Open (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.10 Description: Clear alarm 4, GNSS-Ant-Open (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.11 Description: Set alarm 5, GNSS-Track-No (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.12 Description: Clear alarm 5, GNSS-Track-No (MIN)

iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.13 Description: Set alarm 6, PTP-PPS-Loss (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.14 Description: Clear alarm 6, PTP-PPS-Loss (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.15 Description: Set alarm 7, GNSS-PPS-Loss (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.16 Description: Clear alarm 7, GNSS-PPS-Loss (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.17 Description: Set alarm 8, Time-Sync-Bad (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.18 Description: Clear alarm 8, Time-Sync-Bad (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.19 Description: Set alarm 9, Freq-Range-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.20 Description: Clear alarm 9, Freq-Range-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.21 Description: Set alarm 11, GNSS-Time-Bad (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.22 Description: Clear alarm 11, GNSS-Time-Bad (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.23 Description: Set alarm 12, Freq-Loop-Unlock (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.24 Description: Clear alarm 12, Freq-Loop-Unlock (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.25 Description: Set alarm 13, Freq-Hold-Exceed (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.26 Description: Clear alarm 13, Freq-Hold-Exceed (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.27 Description: Set alarm 14, PPS-Sync-Bad (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.28 Description: Clear alarm 14, PPS-Sync-Bad (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.29 Description: Set alarm 15, Freq-Out-Bad (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.30 Description: Clear alarm 15, Freq-Out-Bad (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.31 Description: Set alarm 16, PTP-System-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.32 Description: Clear alarm 16, PTP-System-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.33 Description: Set alarm 17, FPGA-Load-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.34 Description: Clear alarm 17, FPGA-Load-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.35 Description: Set alarm 18, GNSS-Pos-Integrity (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.36 Description: Clear alarm 18, GNSS-Pos-Integrity (MIN)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.37 Description: Set alarm 19, UTC-Corr-Unk (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.38 Description: Clear alarm 19, UTC-Corr-Unk (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.39 Description: Set alarm 20, Eth-Port0-Down (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.40 Description: Clear alarm 20, Eth-Port0-Down (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.41 Description: Set alarm 21, Eth-Port1-Down (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.42 Description: Clear alarm 21, Eth-Port1-Down (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.43 Description: Set alarm 22, Eth-Mgmt-Down (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.44 Description: Clear alarm 22, Eth-Mgmt-Down (MAJ)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.45 Description: Set alarm 23, Eth-Same-Subnet (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.46 Description: Clear alarm 23, Eth-Same-Subnet (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.47 Description: Set alarm 24, SyncE0-Unsupported (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.48 Description: Clear alarm 24, SyncE0-Unsupported (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.49 Description: Set alarm 25, SyncE1-Unsupported (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.50 Description: Clear alarm 25, SyncE1-Unsupported (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.51 Description: Set alarm 26, Time-Set-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.2.52 Description: Clear alarm 26, Time-Set-Bad (CRI)

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

Trap OID:

.iso.iso-3.iso-3-6.iso-3-6-1.iso-3-6-1-4.iso-3-6-1-4-1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

7.3 Accessing the SNMP MIB files

Private MIB files can be downloaded through the web interface.

The MIB download option is available from the INTERFACE MANAGEMENT menu. See SNMP, page 164.

The SNMP MIB consist of two files:

- TRIMBLE-MIB.mib
- TRIMBLE-TBOLT2-MIB.mib

8

8. Upgrading the firmware

There are two ways to upgrade the firmware. You can use the CLI command or the web interface.

If you use the CLI command, you need to have a server such as FTP, TFTP, SCP, HTTP, and HTTPS, which automatically includes the time server firmware files.

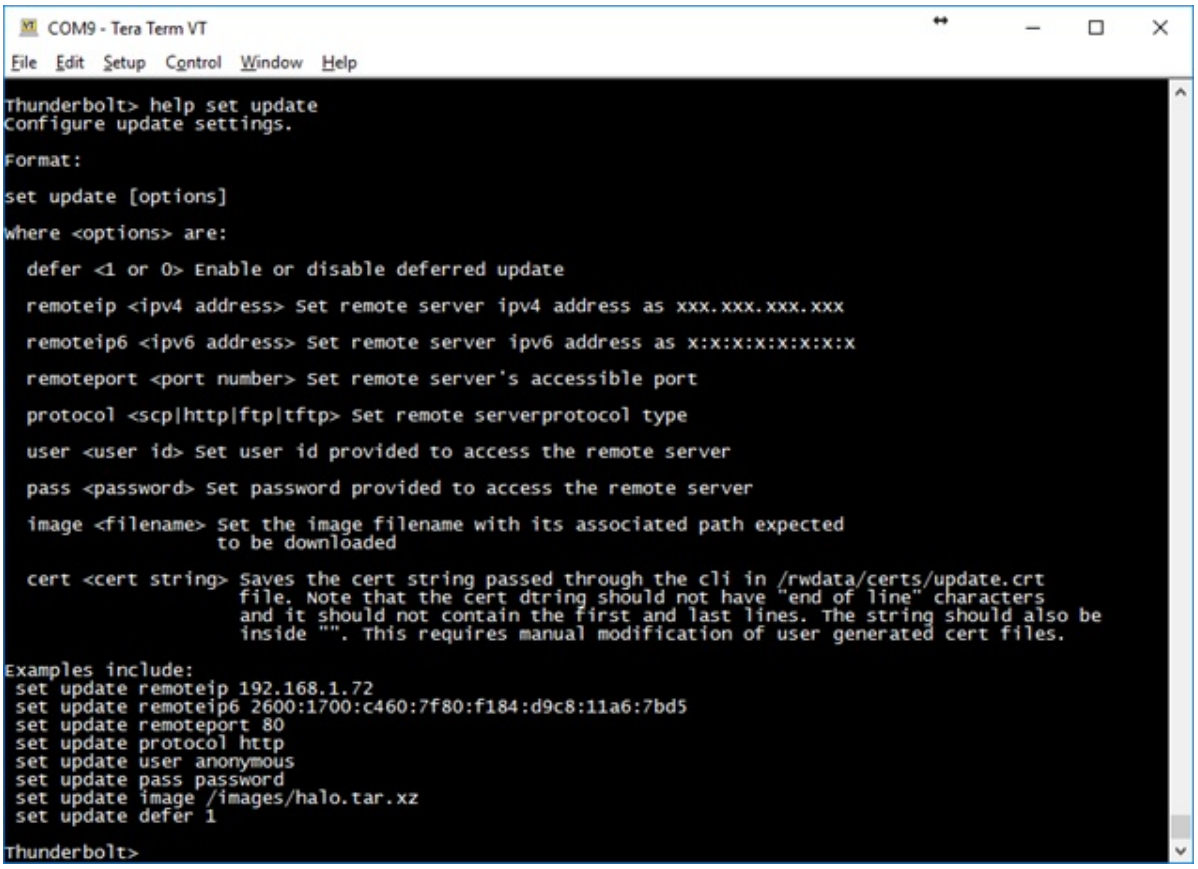
If you use the web interface, you can choose a firmware file from the list in your PC and you can upload and activate it without additional servers.

The time server supports a one-step or two-step upgrade method depending on how you have configured the **Defer Update** option. The one-step method is to upload and automatically activate the firmware. The two-step method is to upload the firmware first and then activate it by user command.

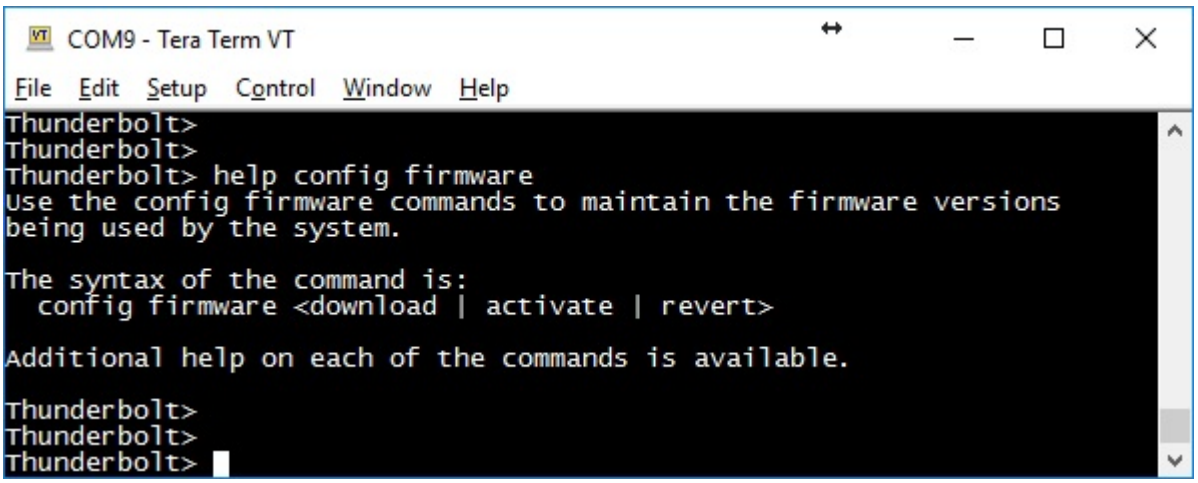
8.1 Upgrading the firmware using the CLI command

To upgrade the firmware using the CLI command:

Use the *help set system* command to get some help information.

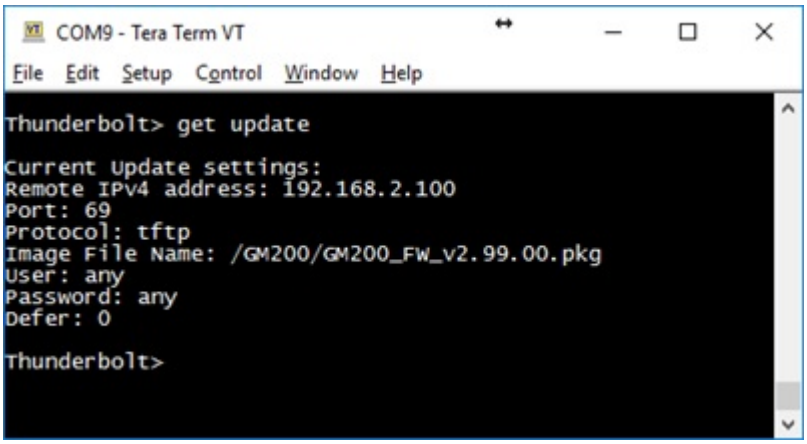


Also, you can get more information with the *help config firmware <download | activate | revert>* command.

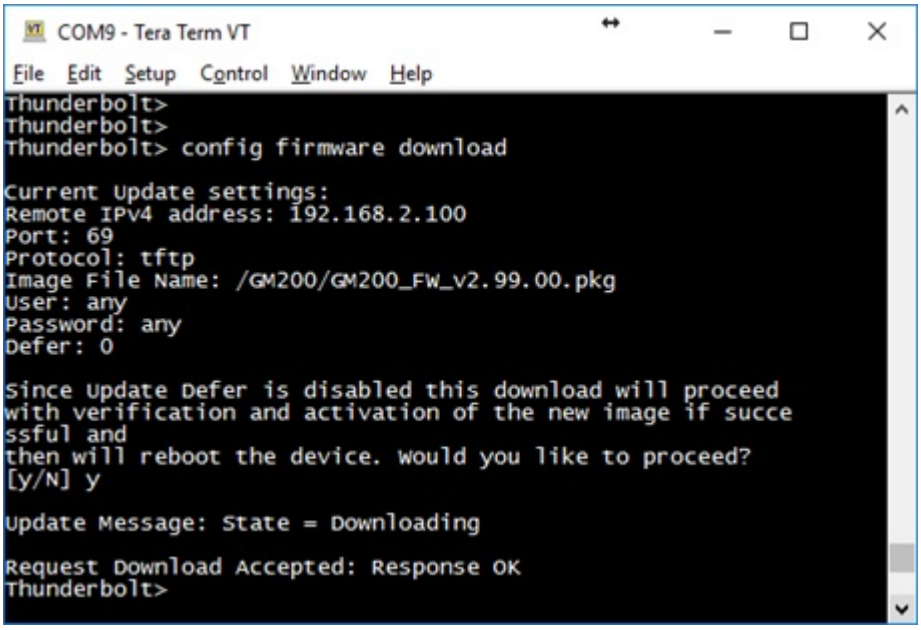


To configure the settings, you should configure the server IP address, port number, protocol, firmware image name, ID, PW, Defer, and so on.

In this example, the file transport **Protocol** is tftp. The **Defer** value is set to 0, which means "Disabled" and the firmware is automatically uploaded and activated.



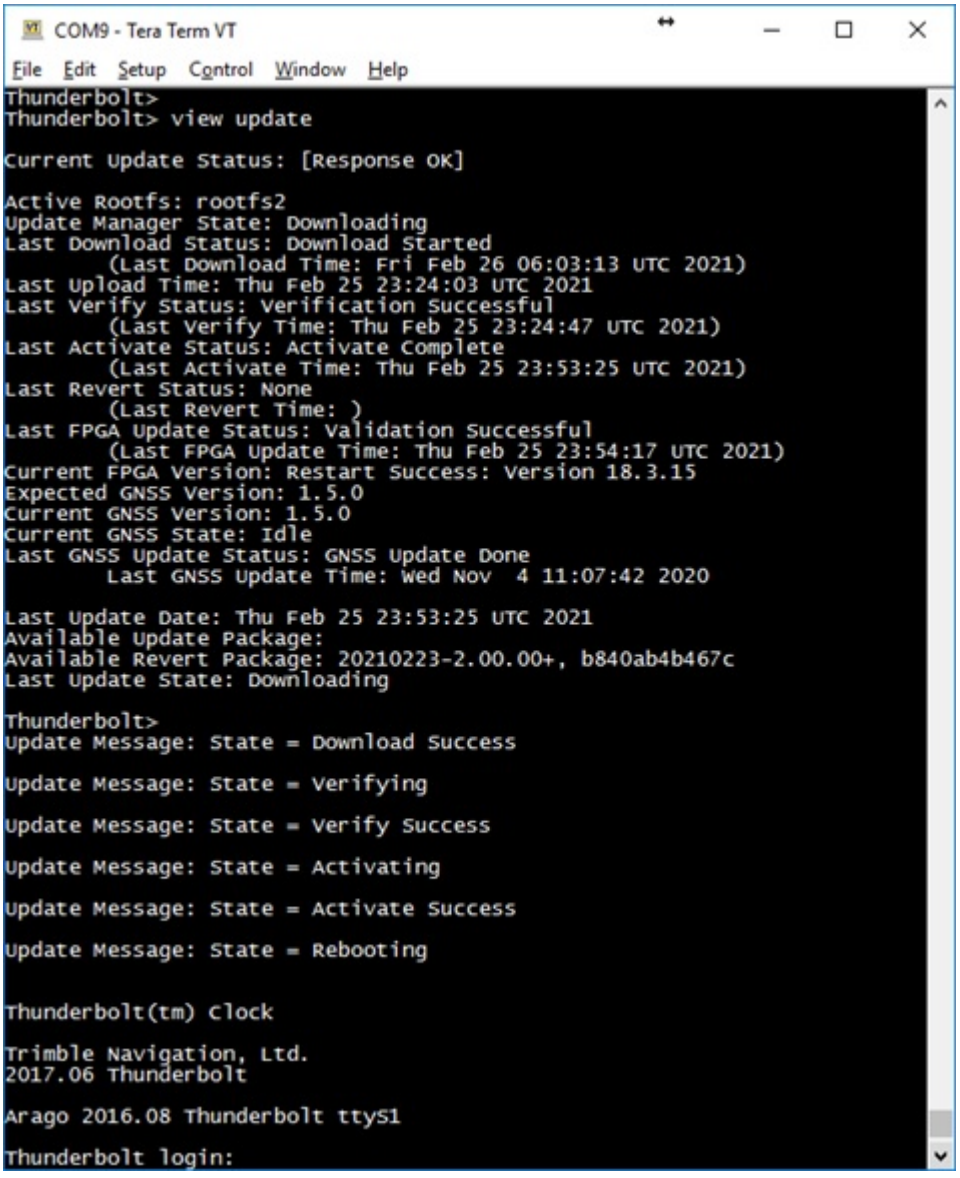
If you complete your configuration, you can use the command shown below to start the firmware upgrade.



Now, the command is working and the firmware is downloading from the TFTP server to the time server if you use the *view update* command.

In the time server, it can store two firmware images in two different partitions: 'rootfs1' and 'rootfs2'. One of the partitions is chosen for automatically upgrading firmware when the *config firmware download* command (see page 90) is executed.

Update Manager State shows the current firmware upgrade status.

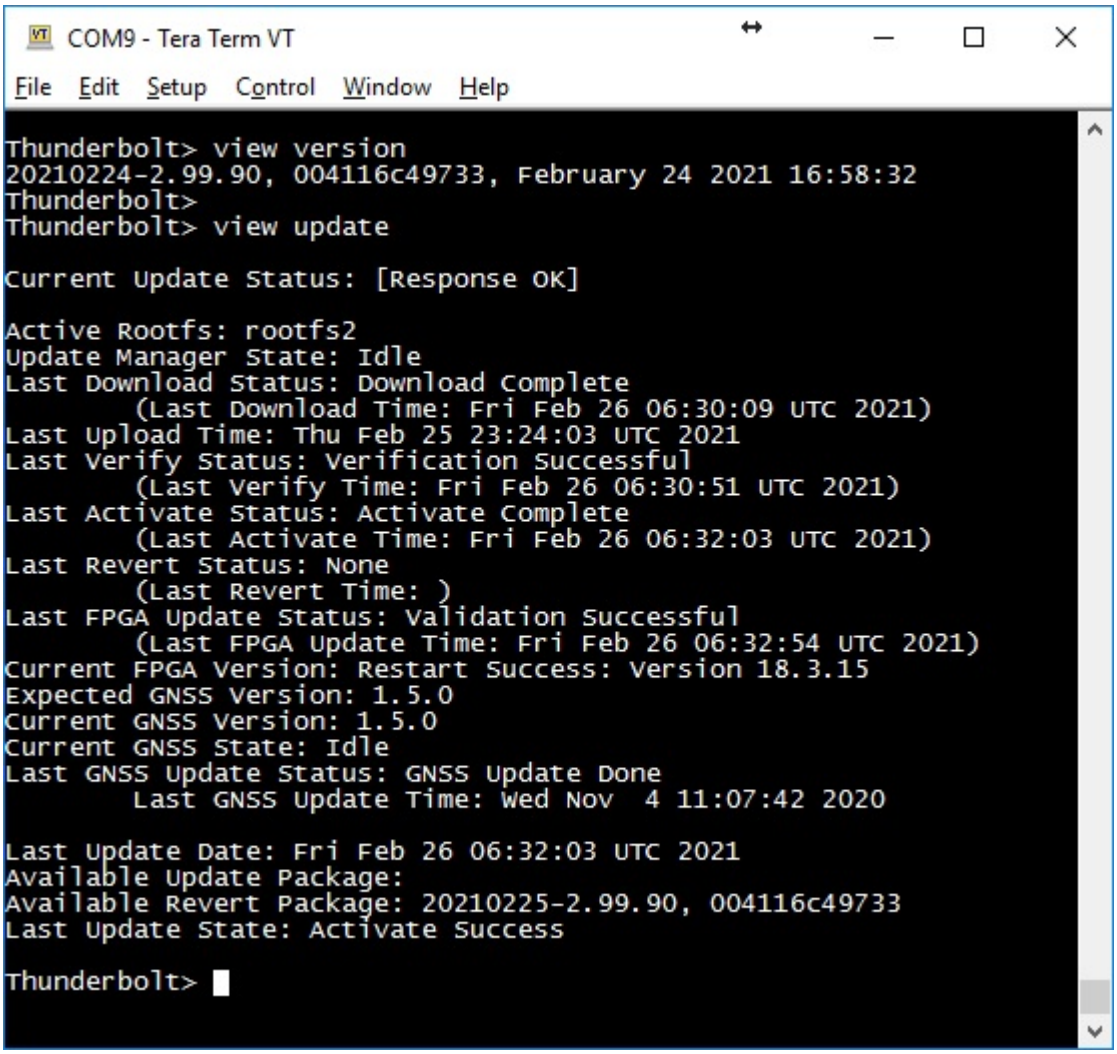


From the system output, firmware download, verify and activate should be done successfully.

After completing the firmware upgrade, the time server restarts.

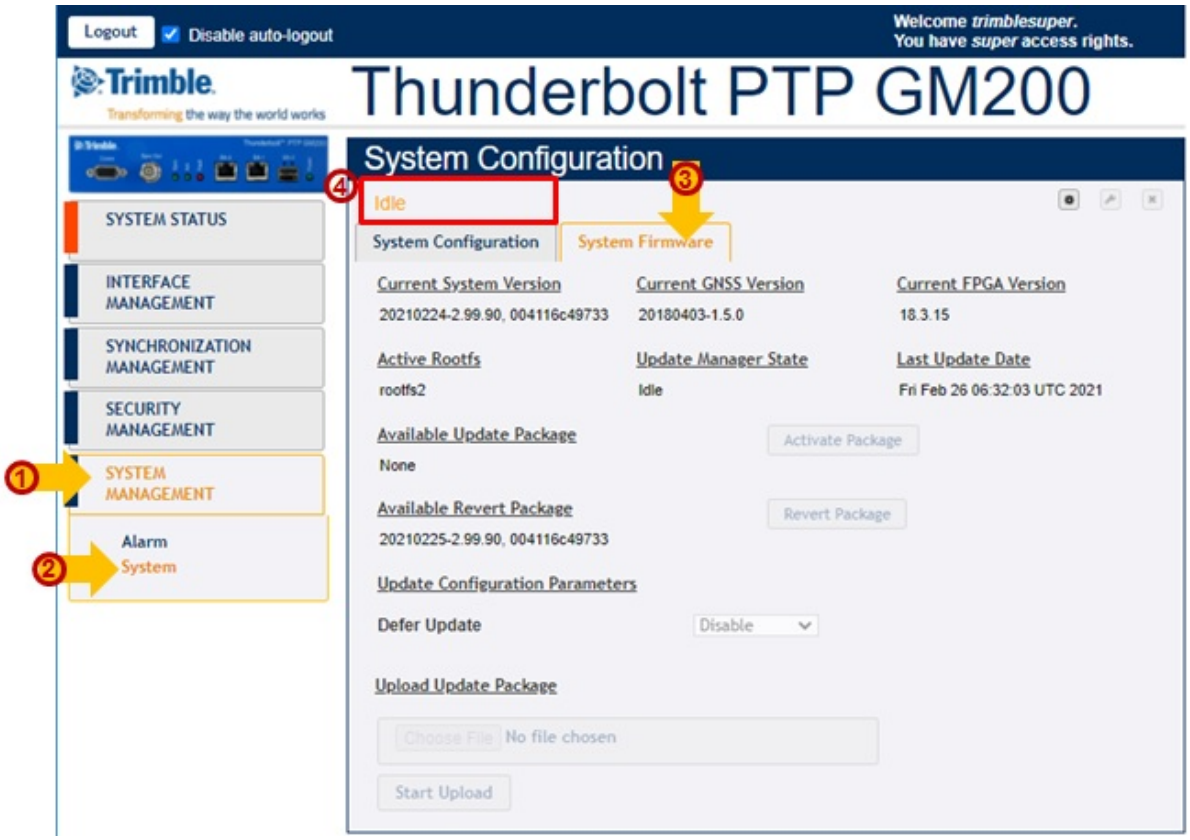
> NOTE – The firmware update restarts the system, which will cause a loss of network timing output.

After restarting from the firmware upgrade, you can check current firmware status with the *view version* (page 105) and *view update* commands.

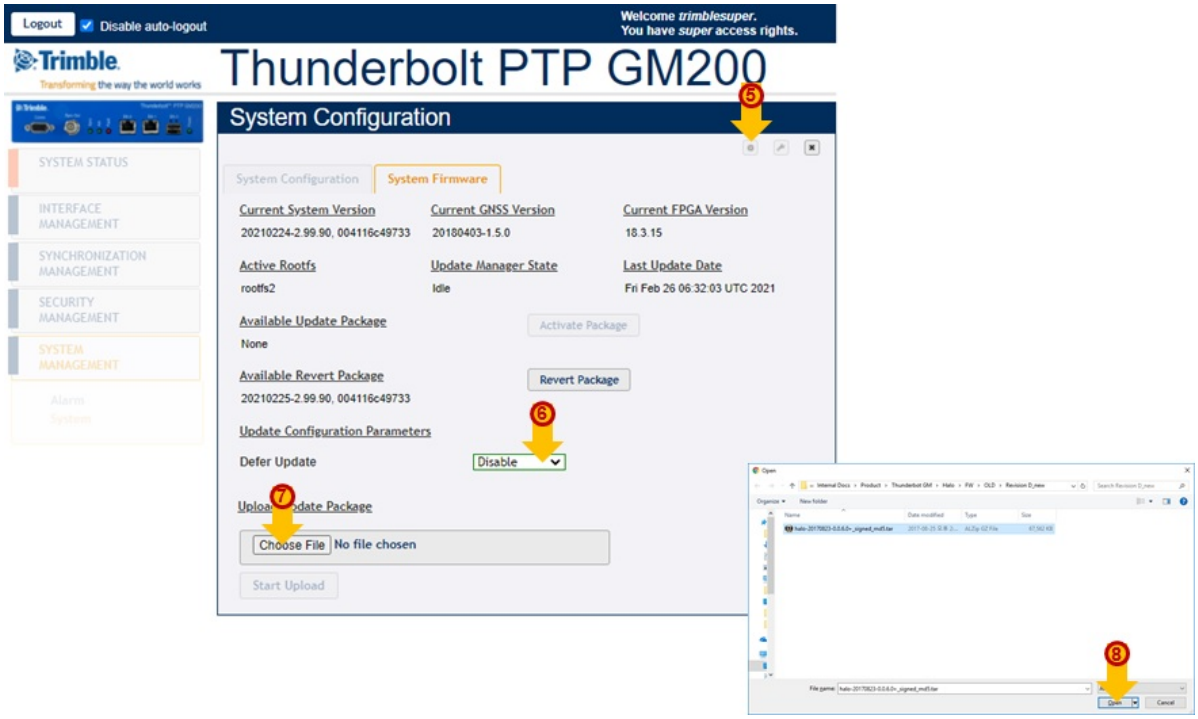


8.2 Upgrading the firmware using the web interface

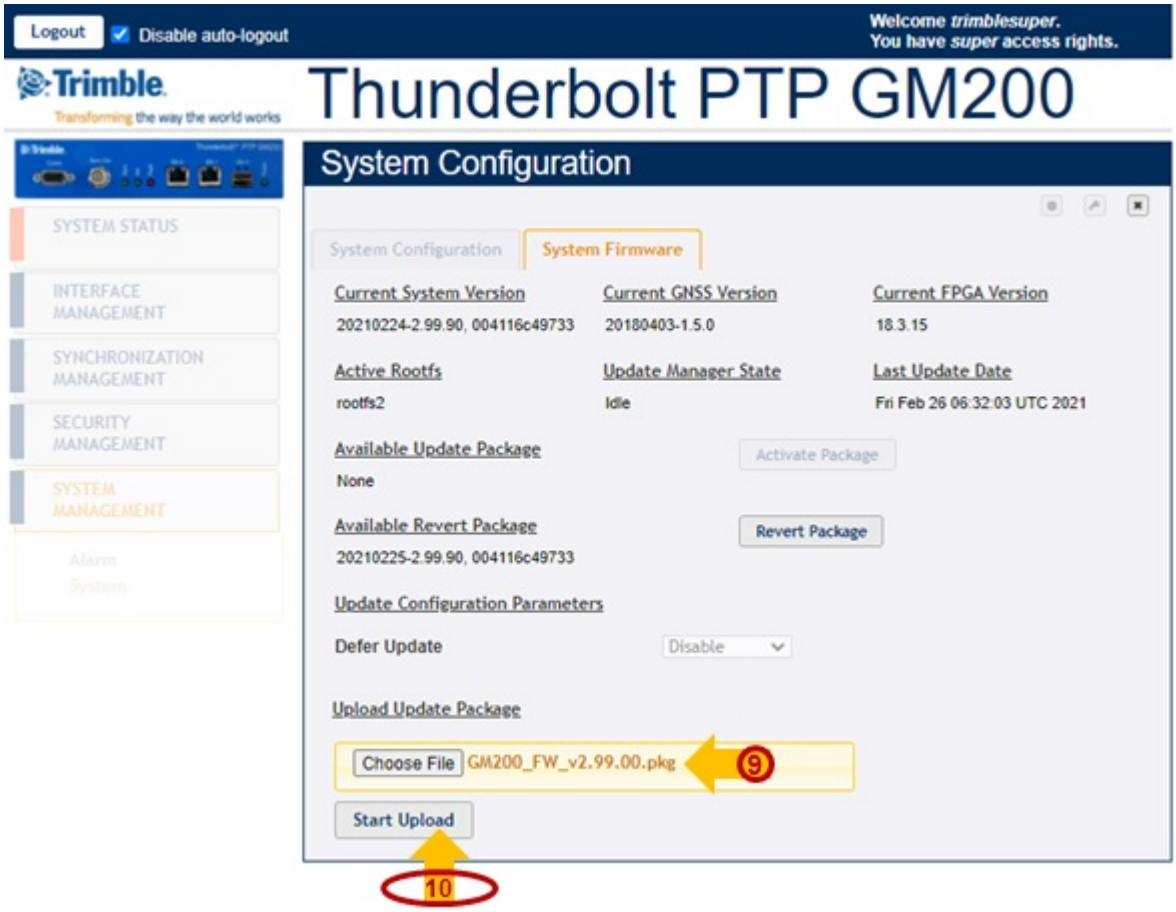
To upgrade the firmware using the web interface:



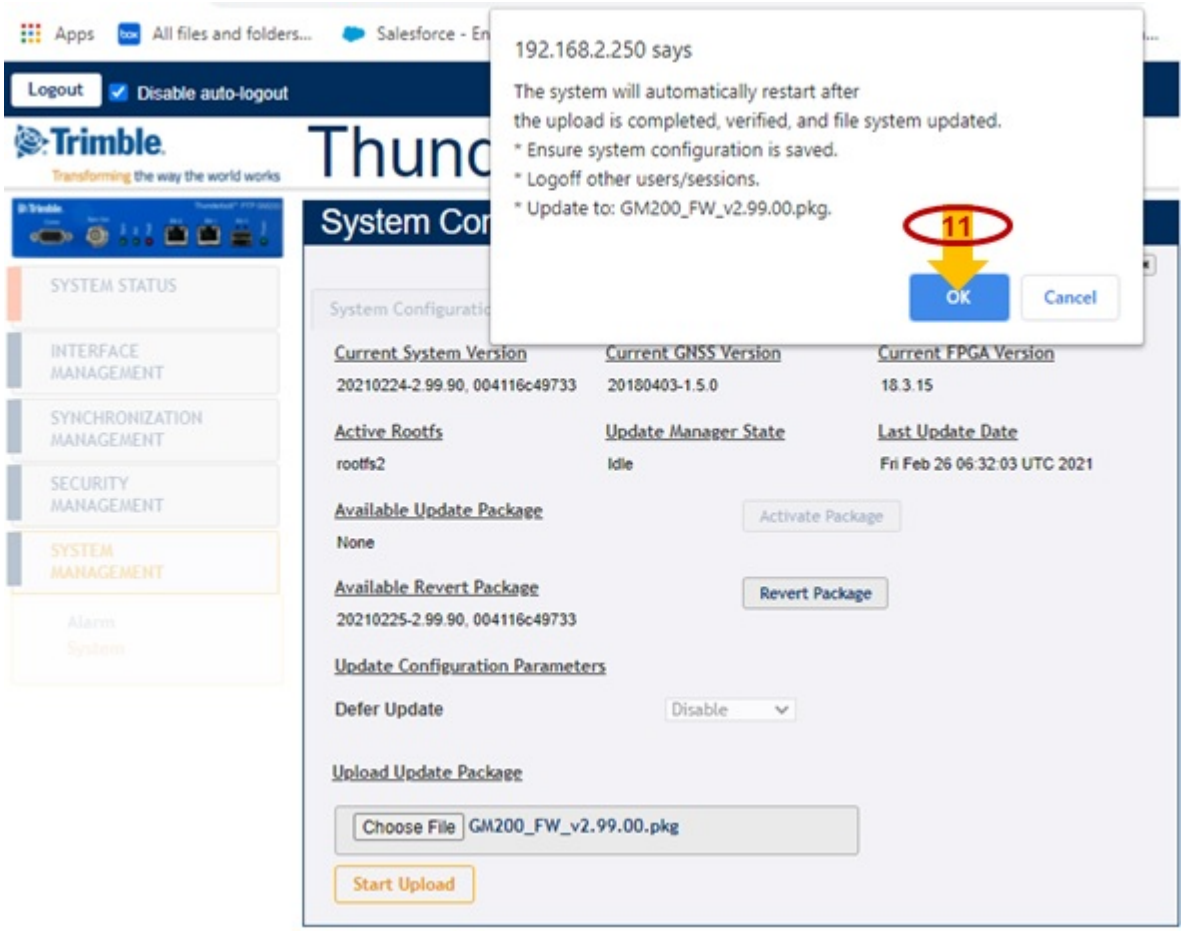
1. Click SYSTEM MANAGEMENT.
2. Click System.
3. Click System Firmware.
4. Always check the current status. The above example shows the status is Idle.



5. Click the CONFIGURE icon to start the firmware upgrade.
6. Set the **Defer Update** field to Disable to upgrade the firmware immediately.
7. Click **Choose File** to select the firmware upgrade file. After selecting the file, click **Open**.

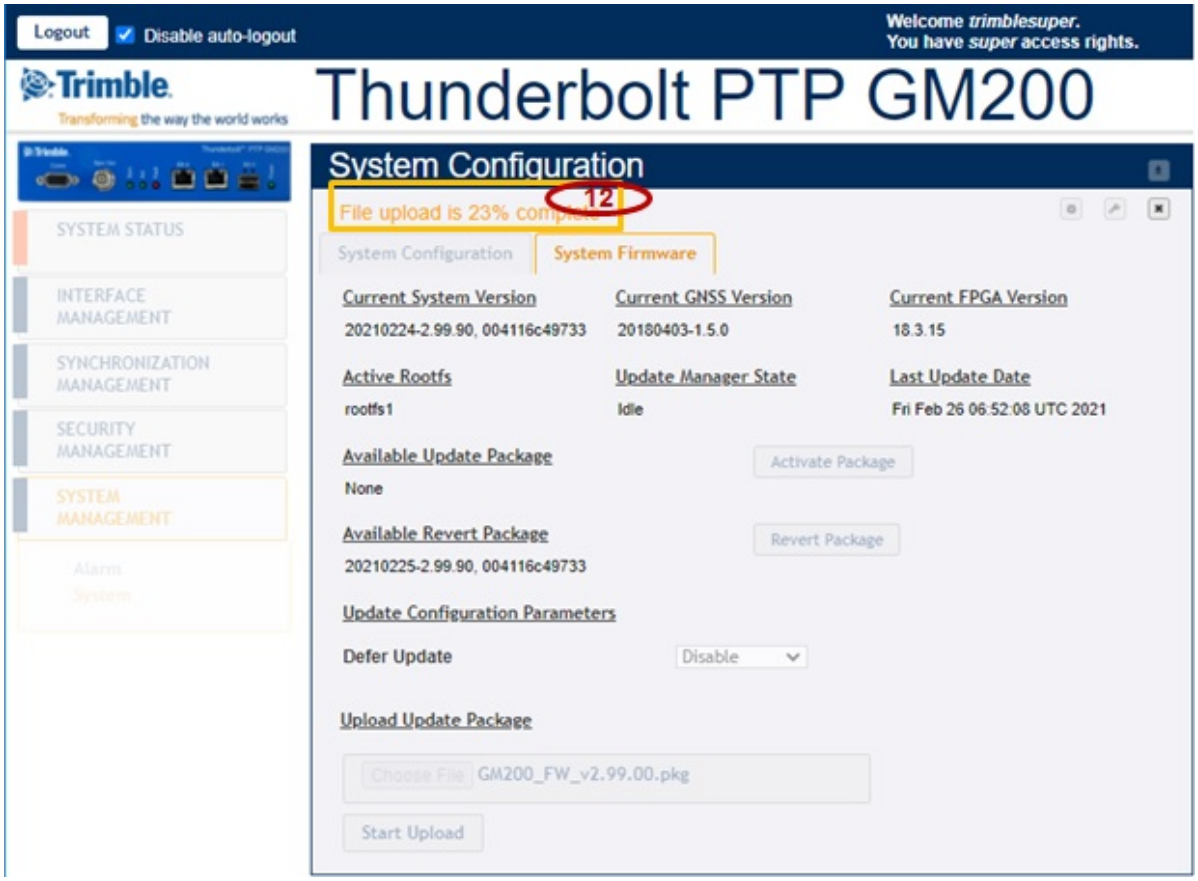


8. The selected file name is shown.
9. Click **Start Upload**.

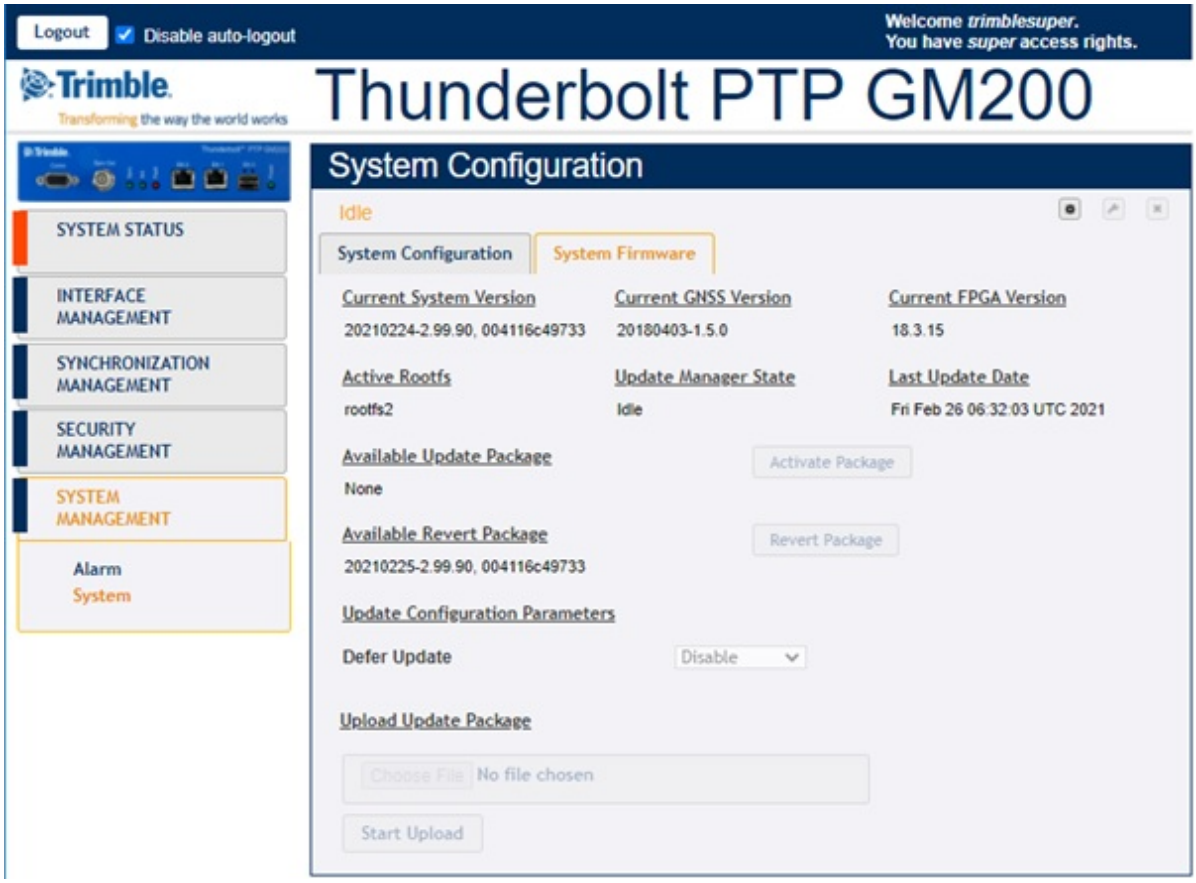


10. Click **OK** in the pop-up window that appears to start the firmware upgrade.

> NOTE – The firmware update restarts the system, which will cause a loss of network timing output.



11. A processing message shows: **Total file progress is 1% =>100% => Verifying => Activating => Rebooting**.



12. Now, you can check the revised firmware version.

9

9. Applications

This chapter describes how to configure the PTP slave operation and the VLAN operation.

9

9.1 PTP Slave operation

Trimble GNSS receivers deliver timing references accurate to ±15 ns. This provides timing-critical applications with the world's most precise and stable source of timing information.

However, when GNSS tracking is unavailable there must be a backup reference besides holdover. PTP Input is the answer to this call with PTP Slave operation, and GNSS is complemented by network-based timing distribution to maintain the time base during GNSS reference failure.

9.1.1. PTP Input overview

Deployment of PTP grandmasters having GNSS receiver references is very simple and quick, however these devices have a point of failure: the antenna. To have the best line-of-sight to multiple satellites, it is always exposed outside the building. The consequence is that it is always subject to lighting strikes, interference due to weather conditions, reflections, jamming, and so on.

The time server has the best holdover in the market, however, to provide even more protection and trying to keep longer time accuracy, the time server also has a feature called PTP Input that is a network-based timing distribution backup reference.

The time server will continue using GNSS as the primary time reference. PTP Input complements GNSS and will help and maintain the time when a GNSS reference is not available.

PTP Input feature is a secondary reference and will be active if GNSS tracking is lost. The time server will never work as a Boundary Clock because the time server has superior holdover specifications to a network device due to excellent oscillator specifications.

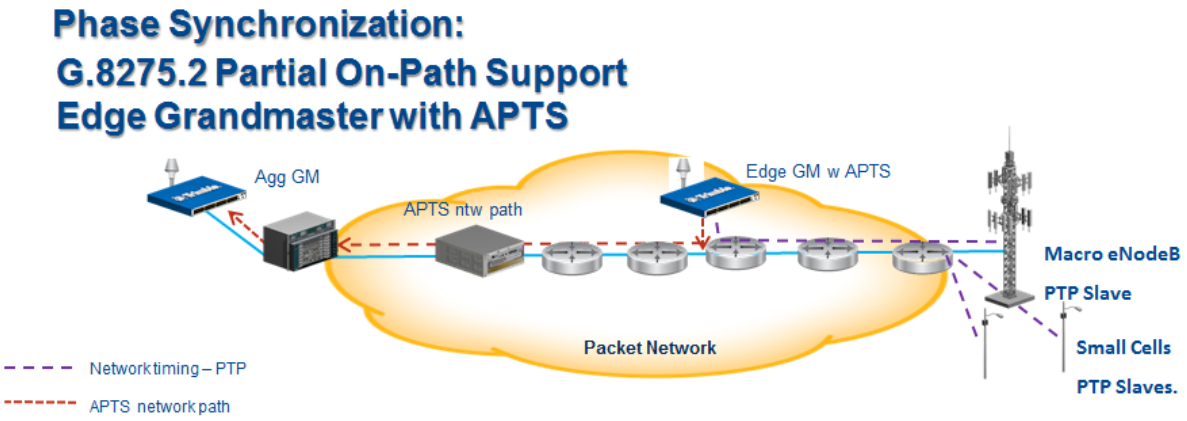
9.1.2 How PTP Input works in APTS mode

PTP Input is designed as a secondary (backup) reference of GNSS reference of the time server.

It can be configured in Ethernet port 0 or 1. It will be an additional input for the time server. The Ethernet port will be configured as a PTP slave for the time server.

Since the Ethernet port will be configured as PTP slave, it will require a grandmaster reference or 'grantor'. The time server PTP Input supports up to three grantors to be configured.

PTP Input can be used with all unicast PTP profiles supported by *GM200: G.8265.1 Profile Option I or II* and *IEEE-1588 Telecom Profile v2* (unicast). All previous grandmasters deployed by telecom operators are working right now with those PTP profiles.



9.1.3 Configuring PTP Input using CLI commands

PTP Input is related to the following CLI commands. Remember that to use any Ethernet port, you must first configure the network interface (IP addresses and/or VLAN IDs):

To do any PTP configuration change, you must disable the PTP service in the Ethernet port.

To disable/enable the PTP service:

```
set ptp eth0/1 enable/disable
```

Use the *set ptp* command to do changes in PTP configuration. In this case, the command changes the profile required, the mode from grandmaster to slave, and adds at least one grantor:

```
set ptp eth0/1 profile <yyyyyyy> mode slave grantor
<x.x.x.x>
```

Where:

<x.x.x.x>	is an IP address
<yyyyyyy>	is one of the following options: • g8265-II – Profile G.8265.1 Option II (clock class 80) • g8265-I – Profile G.8265.1 Option I (clock class 84) • telecom – Profile IEEE-1588 Telecom Profile v2 (unicast)

To configure port Ethernet 0 or 1 into PTP input, set the system mode first:

```
set system apts enable
```

or

```
set system opermode bc
```

To see all inputs/references or a specific one: GNSS or PTP input in Ethernet 0 (ptp0) or PTP input in Ethernet 1 (ptp1):

```
view input (gnss or ptp1 or ptp0)
```

To see PTP configuration in Ethernet ports (for verification purposes):

```
get ptp eth0/1
```

NOTE – If you need to use this command after doing any change in PTP configuration, allow at least 15 seconds before seeing the changes done.

9.1.4 Configuring PTP input examples

Below are examples of PTP input configuration steps.

9.1.4.1 Example of an APTS slave mode configuration

In APTS slave operation, eth0 will be used as PTP Input and eth1 will be used as PTP grandmaster. There will be two grantors used (two grandmasters already used in Aggregation or Core network that will serve as a reference of the time server), with IP addresses 10.173.230.225 and 10.75.134.224. It will use the *IEEE-1588 Telecom Profile v2* (unicast) profile. The sequence of commands is:

```
set system apts enable

set ptp eth0 disable

set ptp eth0 profile telecom mode slave grantor
10.173.230.255,10.75.134.224

set ptp eth0 enable

get ptp eth0

view input
```

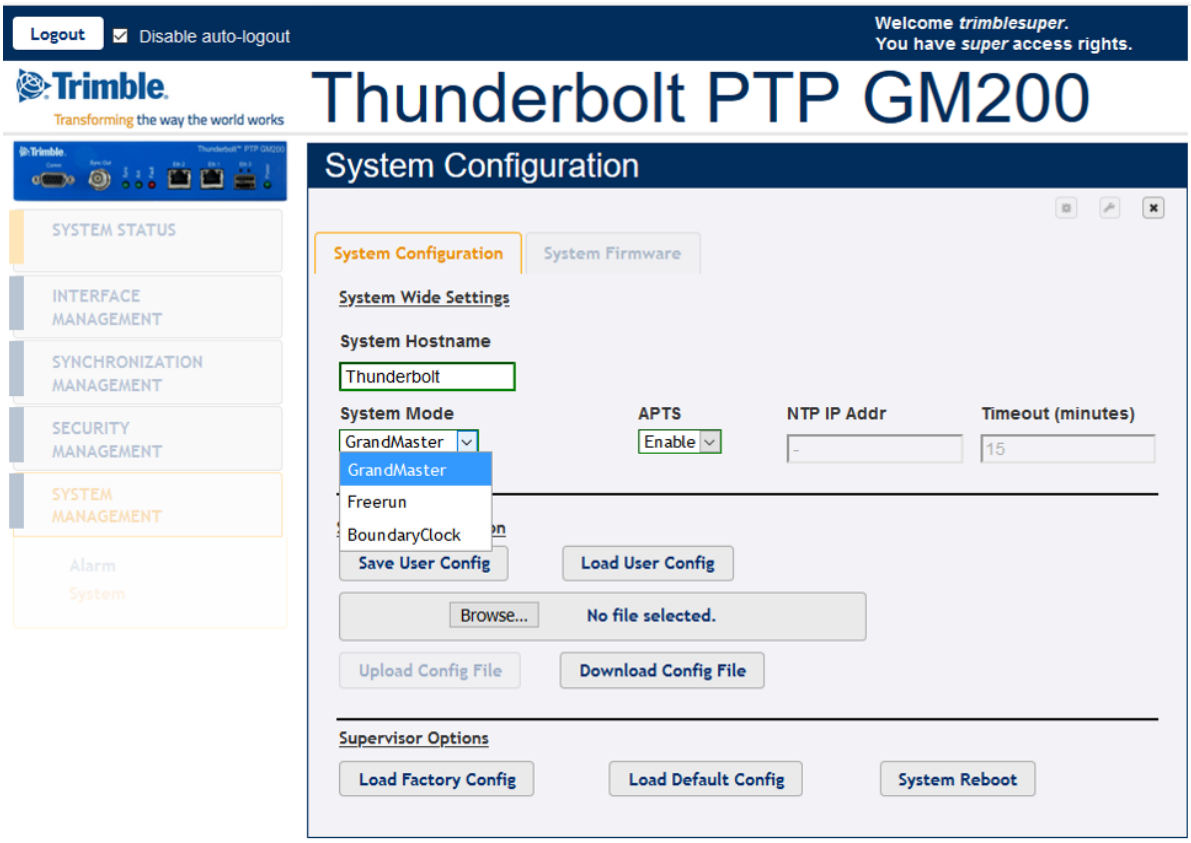
9.1.4.2 Example of an BC Slave mode configuration

In the BC slave operation, eth1 will be used as PTP Input and eth0 will be used as PTP grandmaster. There will be one grantor used (one grandmaster already used in Aggregation or Core network that will serve as reference of the time server) with IP addresses 10.73.130.251. It will use the *G.8275.2* profile. The sequence of commands is:

```
set system opermode bc

set ptp eth1 profile g8275.2 mode slave grantor
10.73.130.251

set ptp eth1 enable

get ptp eth1

view input
```

9.1.5 Configuring PTP Input using the web interface

9.1.5.1 Configure the System Mode



In the **System Configuration** screen, select the **System Mode** from the drop-down options:

- **GrandMaster**: GM mode
- **Freerun**: Freerun mode
- **BoundaryClock**: BC mode

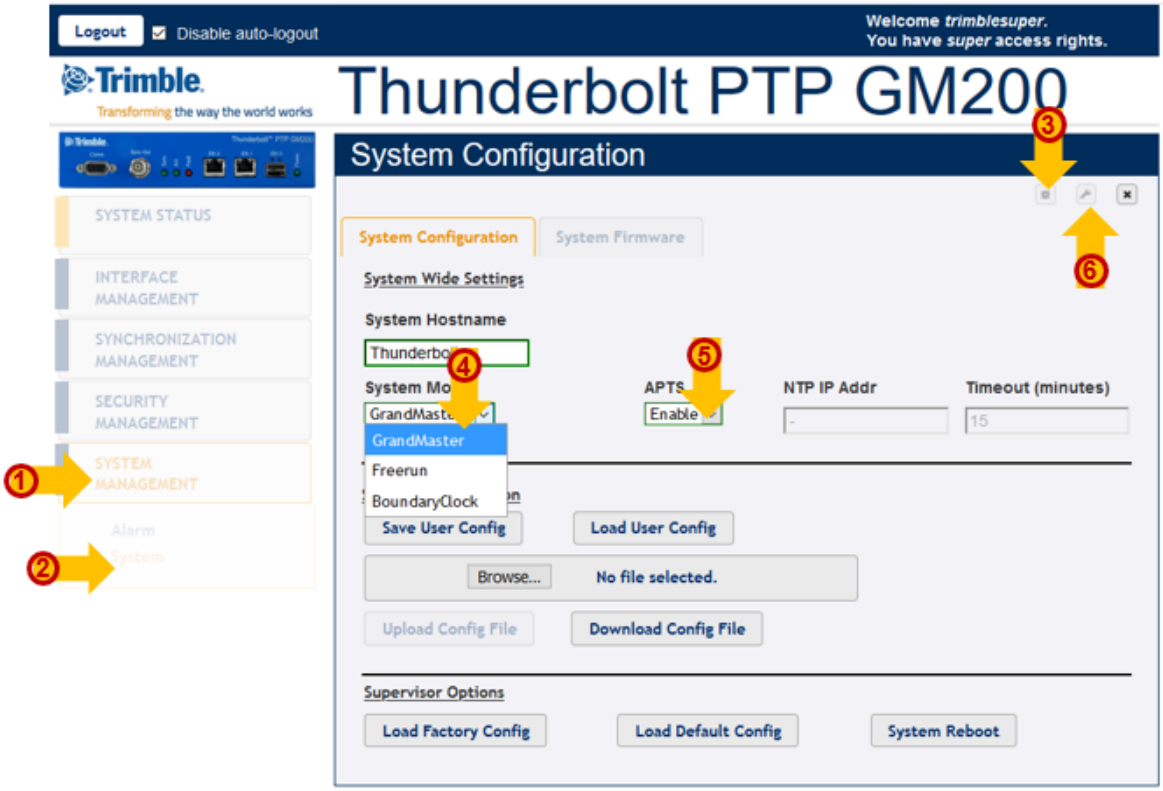
In the **APTS** field (APTS mode for GM), select **Enable** or select BoundaryClock.

> NOTE – If you change the system mode, first save your configuration and then reboot the system to apply the changed mode.

9.1.5.2 System mode change to start the APTS PTP Slave configuration

Before starting the configuration, make sure that the time server is connected with GNSS (or GPS) antenna FIRST to be set as APTS slave mode.

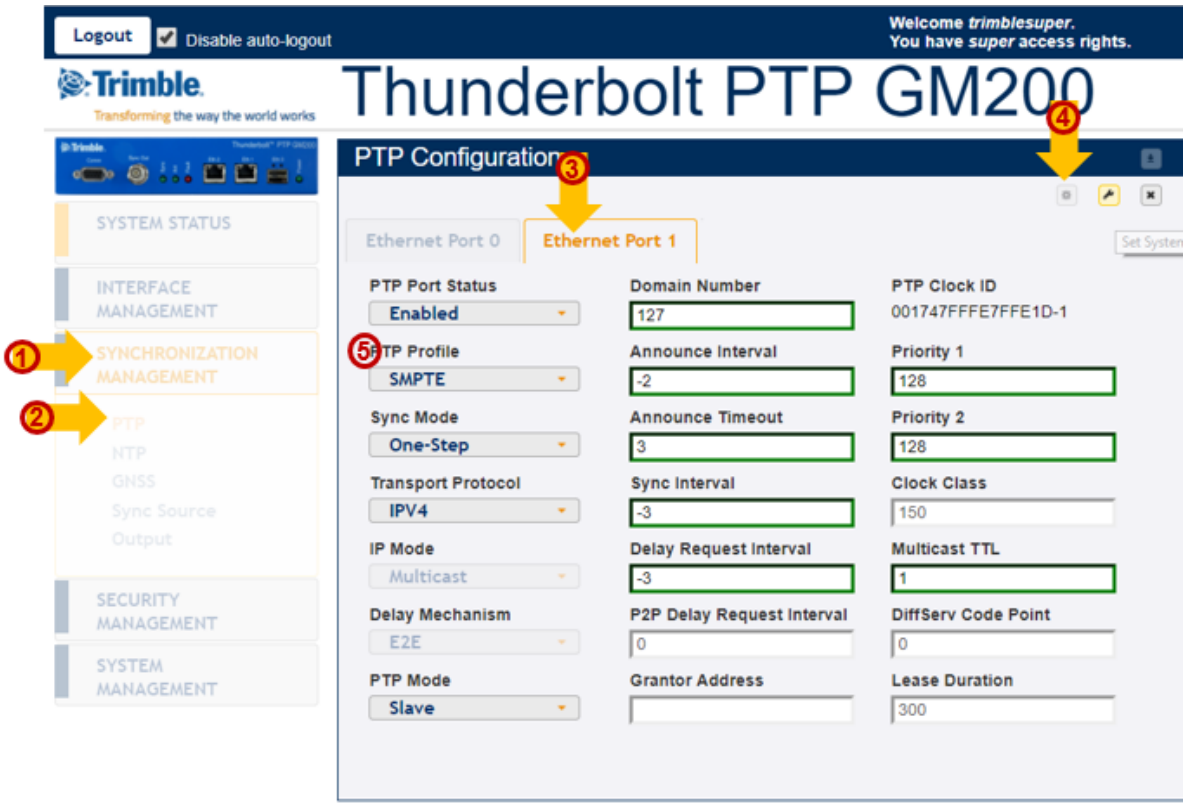
Connect the GNSS antenna if it is not already connected.



1. Select SYSTEM MANAGEMENT ❶ and then select System ❷.
2. To make changes, click Configure ❸.
3. From the System Mode list, select the GrandMaster option ❹.
4. From the APTS list, select the Enable option ❺.
5. Click Set to apply the settings ❻.

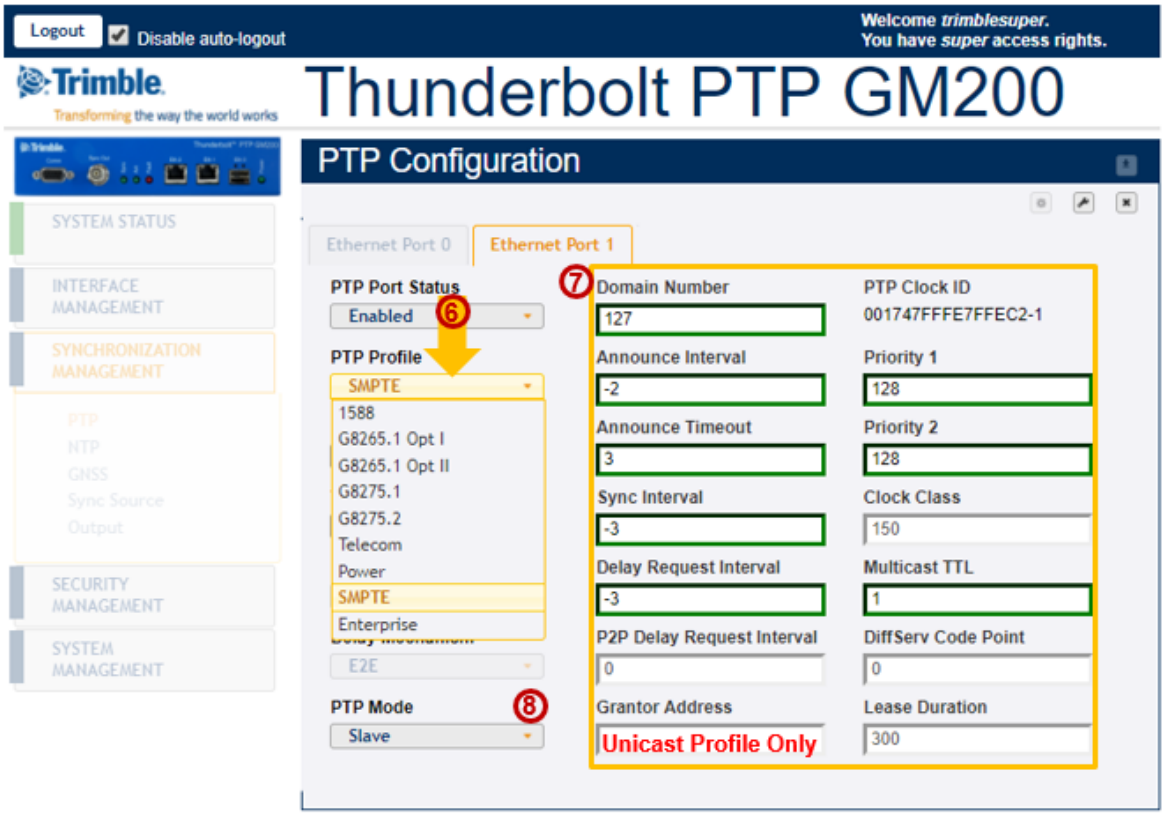
9.1.5.3 APTS PTP slave configuration

After configuring the system mode:



1. Select SYNCHRONIZATION MANAGEMENT ❶.
2. Then, click PTP ❷.
3. Select Ethernet Port 1 tab ❸ or Ethernet Port 0 if using ETH0.
4. Click Configure ❹. The parameters are activated.

5. Click the **PTP Profile** list ❺.



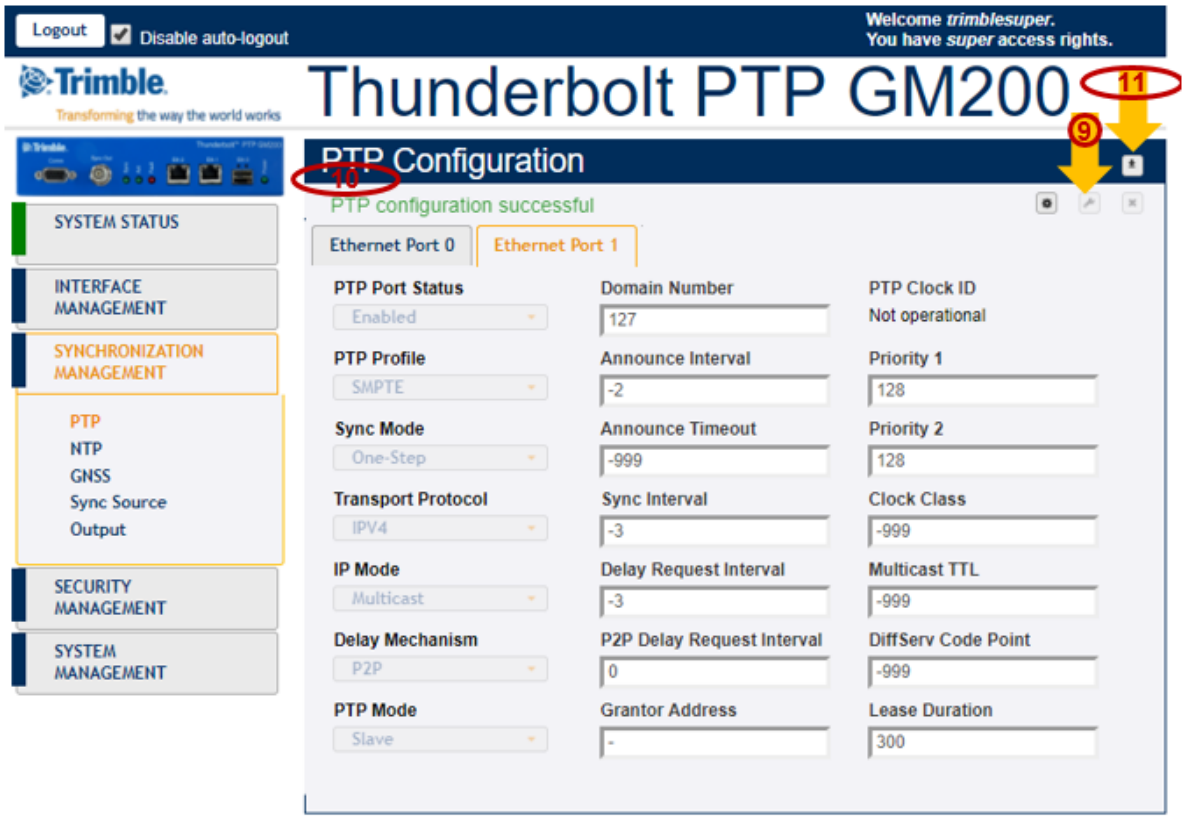
6. Select a profile from the **PTP Profile** list ❻ .
7. Most settings are changed automatically based on the selected profile, so if you don't have any specific settings for the profile you chose, just use default values for the profile ❼.
8. From the PTP Mode list, select **Slave** ❽.

> NOTE – If you are using the Unicast profile, set the **Grantor Address** field. This is the Master GM IP address. If you are using the Multicast profile, you don't need to set the **Grantor Address**.

> NOTE – Configure the PTP slave port first and enable it (it is still disabled at this point). Then, go to the PTP master port and enable it. Now both Master and Slave ports are enabled at once.

9. Click **Set**  to apply the settings ❾ .

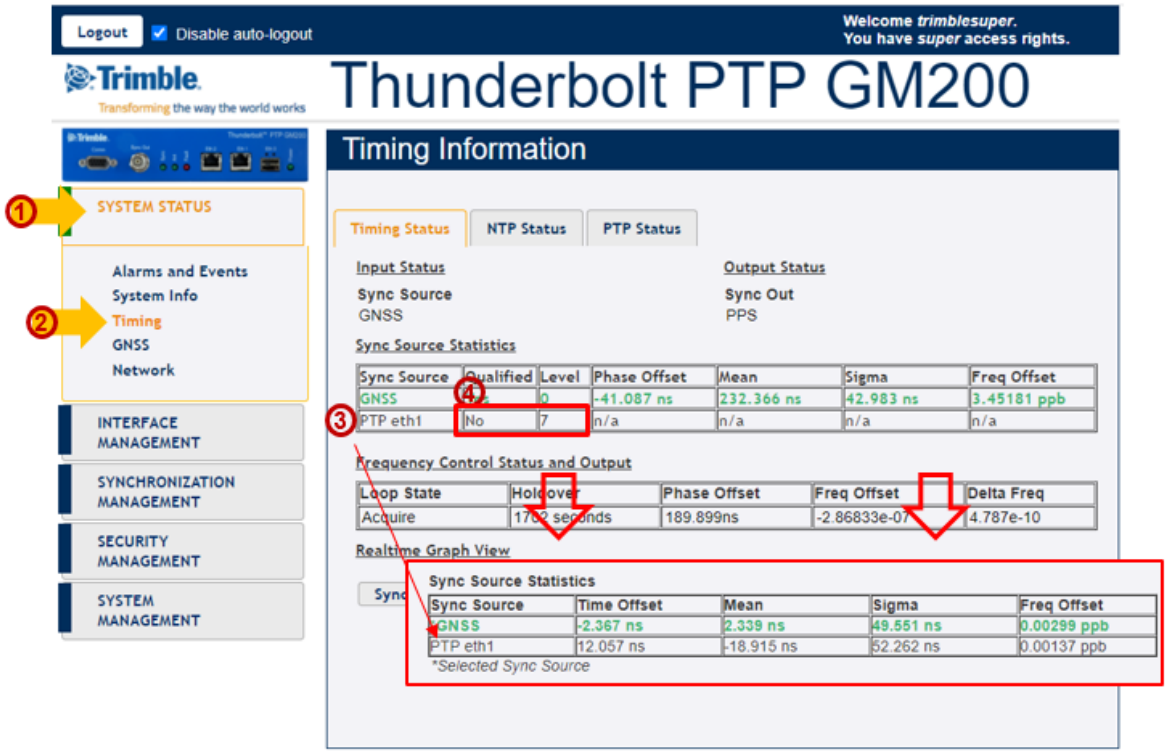
10. A confirmation message **PTP configuration successful** appears ⑩.



11. Click the **Save System Configuration** icon to save the current settings ⑪.

9.1.5.4 Status of an APTS PTP Slave operation

After completing the PTP slave configuration, you can confirm the status of the time server.



1. Select SYSTEM STATUS ❶ and then Timing ❷.

   After about five minutes, you will see time offset values as in the example above on PTP eth1 ❸.

   Note that the GNSS Sync Source line is colored in green.

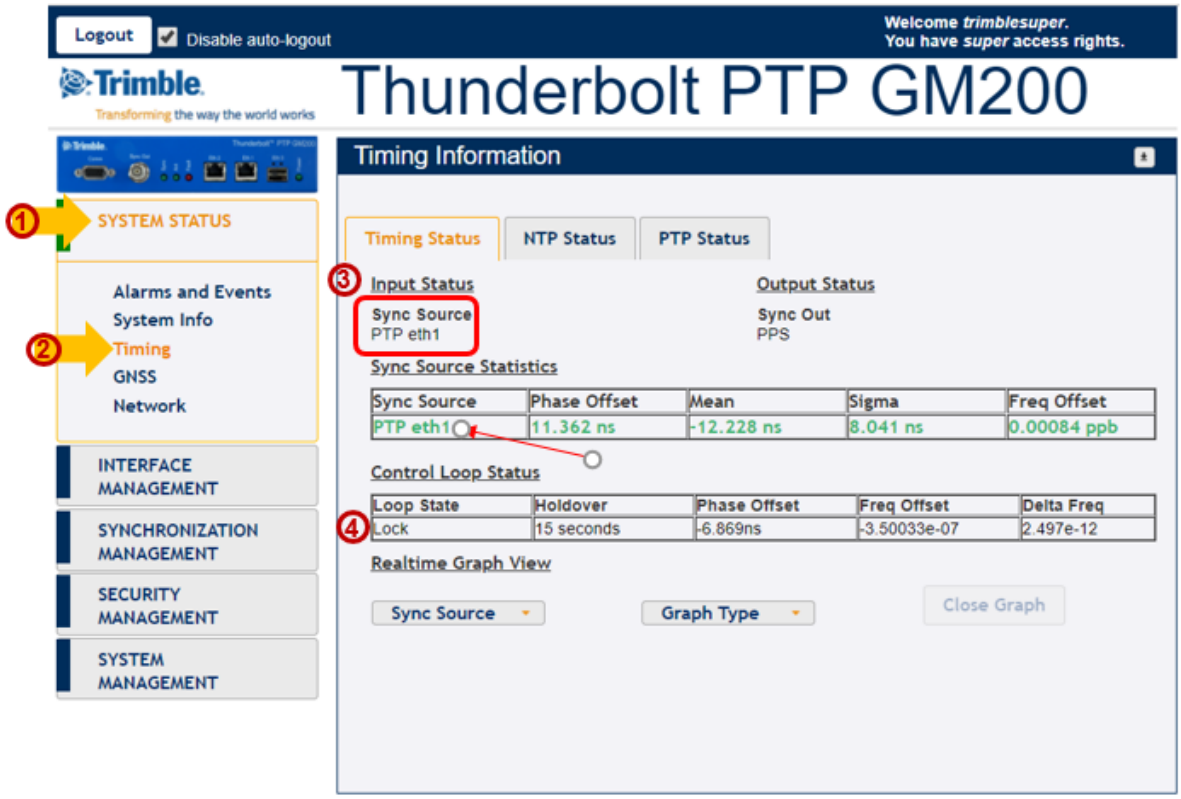
2. Check the Qualified and Level values.

   To start the APTS slave mode operation, it should be Yes and 1 ❹. If you see "Yes" and "1", the time server is ready to operate the ATPS Slave mode.

   Alternatively, you can remove the GNSS antenna for an APTS test case.

9.1.5.5 Removing the GNSS reference to start the APTS PTP Slave operation

If you remove the GNSS reference:



1. Select SYSTEM STATUS ❶ and then Timing ❷.

   You will see that the Sync Source has been changed from GNSS to PTP eth1 ❸.

   Also you will see the PTP Eth1 (or Eth0) shown in green color (it is a time reference source now).

2. Check that the Loop State field status is Lock ❹.

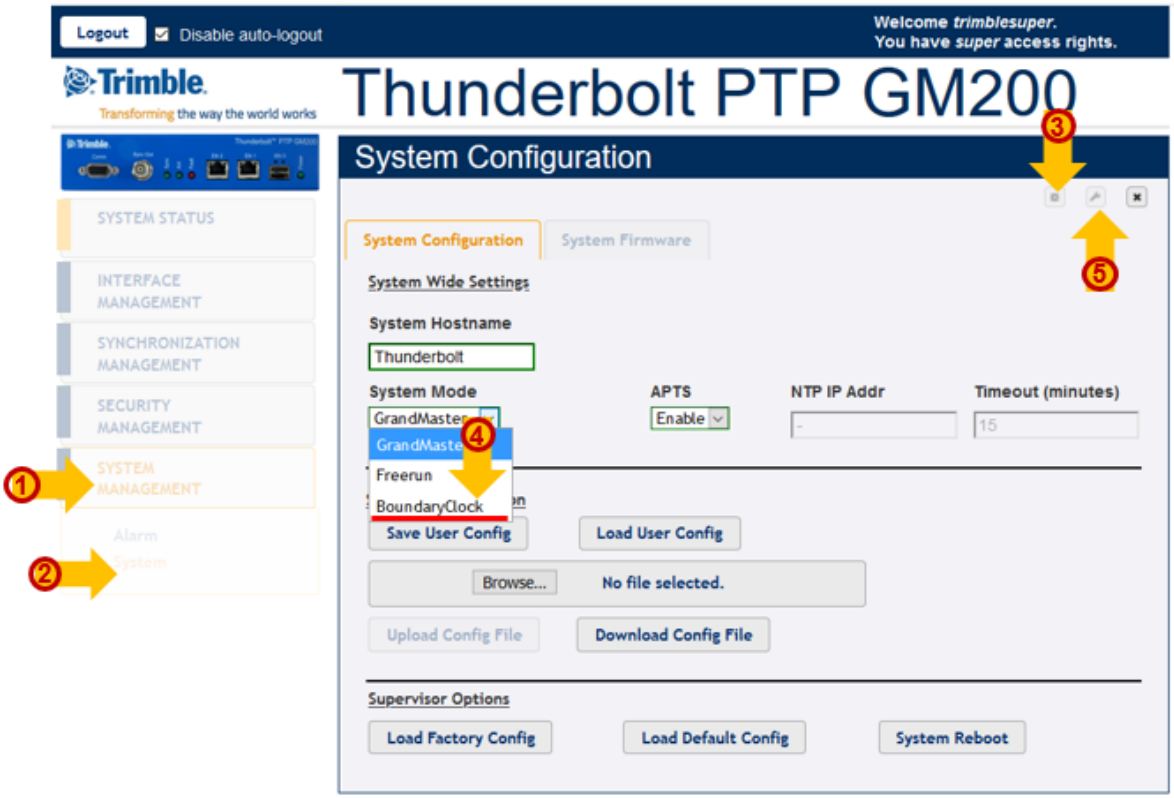
   Now the time server is locked to external PTP input.

3. If you want to see **Real-time Graph View** for phase offset of incoming PTP reference:
   a. Click **Realtime Graph View** to expand the information. The following screen appears:

   b. Click **PTP eth1** ❺.
   c. Click **Phase Offset** ❻.

      You will see a real-time graph for a selected reference source.

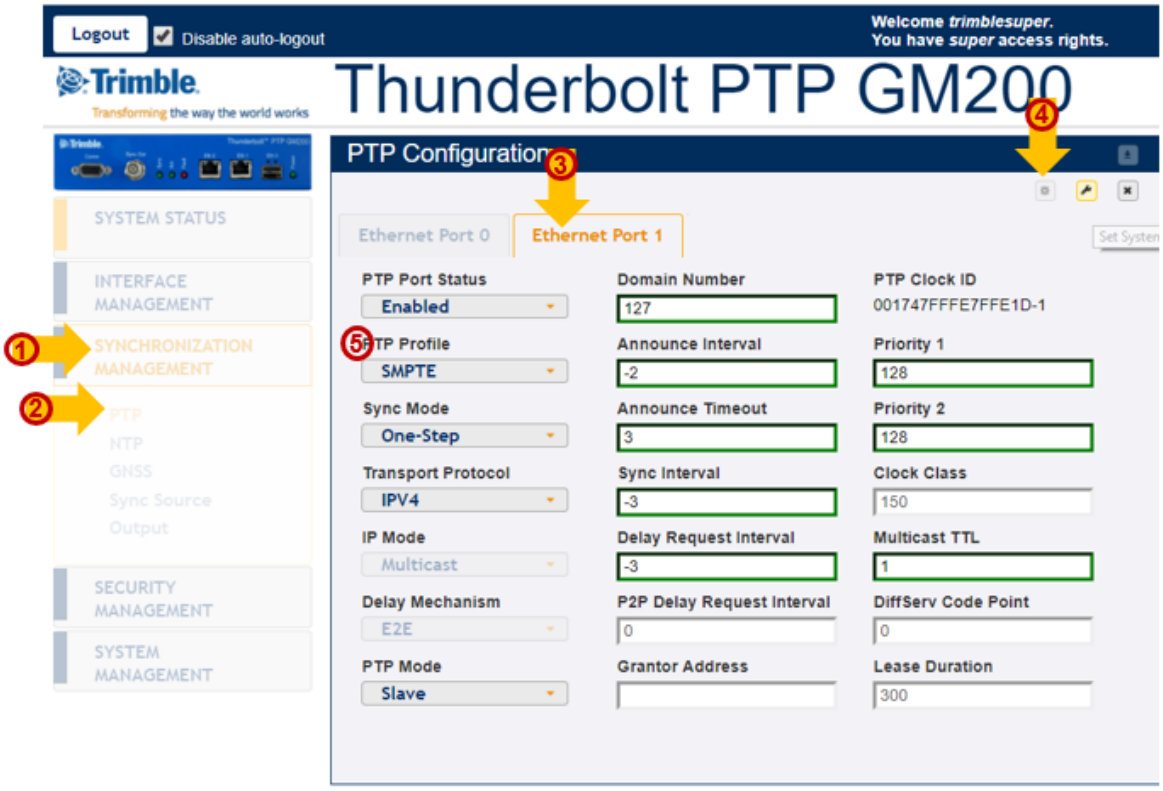
9.1.5.6 System mode change to start the BC PTP Slave configuration



1. Select SYSTEM MANAGEMENT ❶.
2. Then, click System ❷.
3. Click Configure  ❸.
4. From the System Mode list, select the BoundaryClock option ❹.
5. Click Set  to apply the settings ❺.

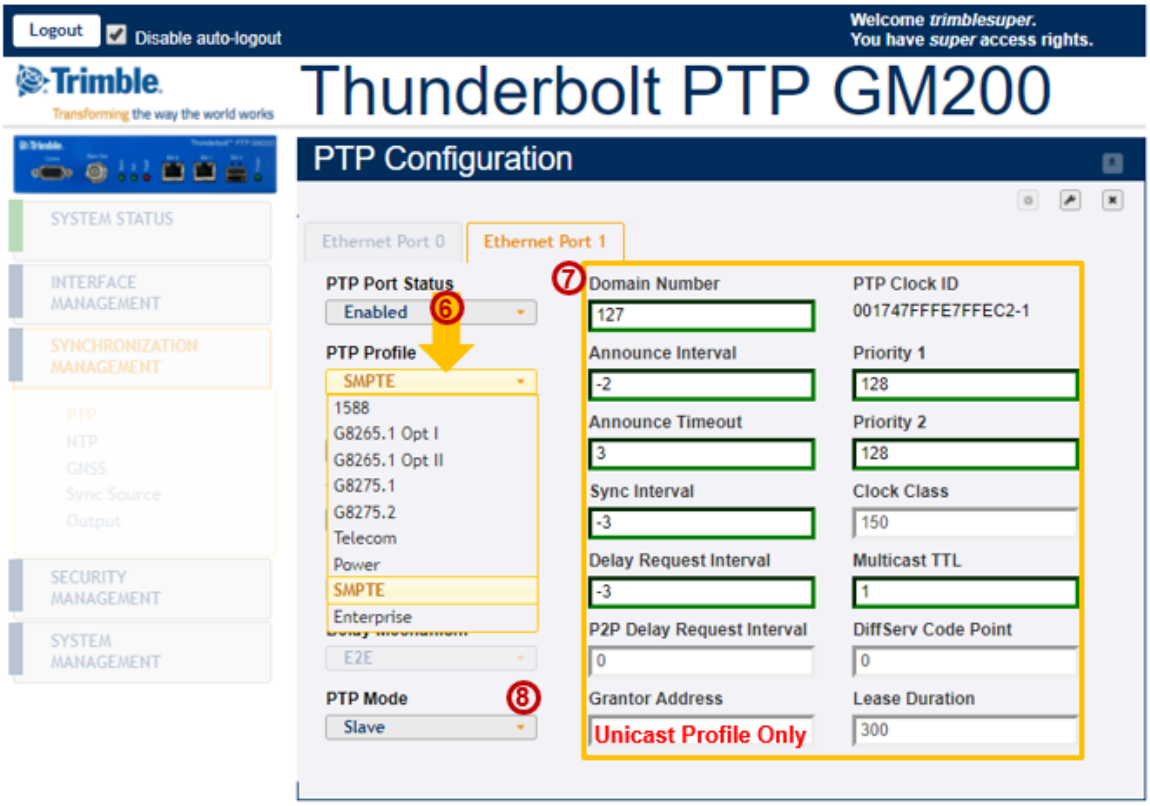
9.1.5.7 BC PTP slave configuration

After configuring the system mode:



1. Select SYNCHRONIZATION MANAGEMENT ❶.
2. Then, Click PTP ❷.
3. Select Ethernet Port 1 tab ❸ or Ethernet Port 0 if using ETH0.
4. Click Configure ❹. The parameters are activated.

5. Click the **PTP Profile** list ❺.



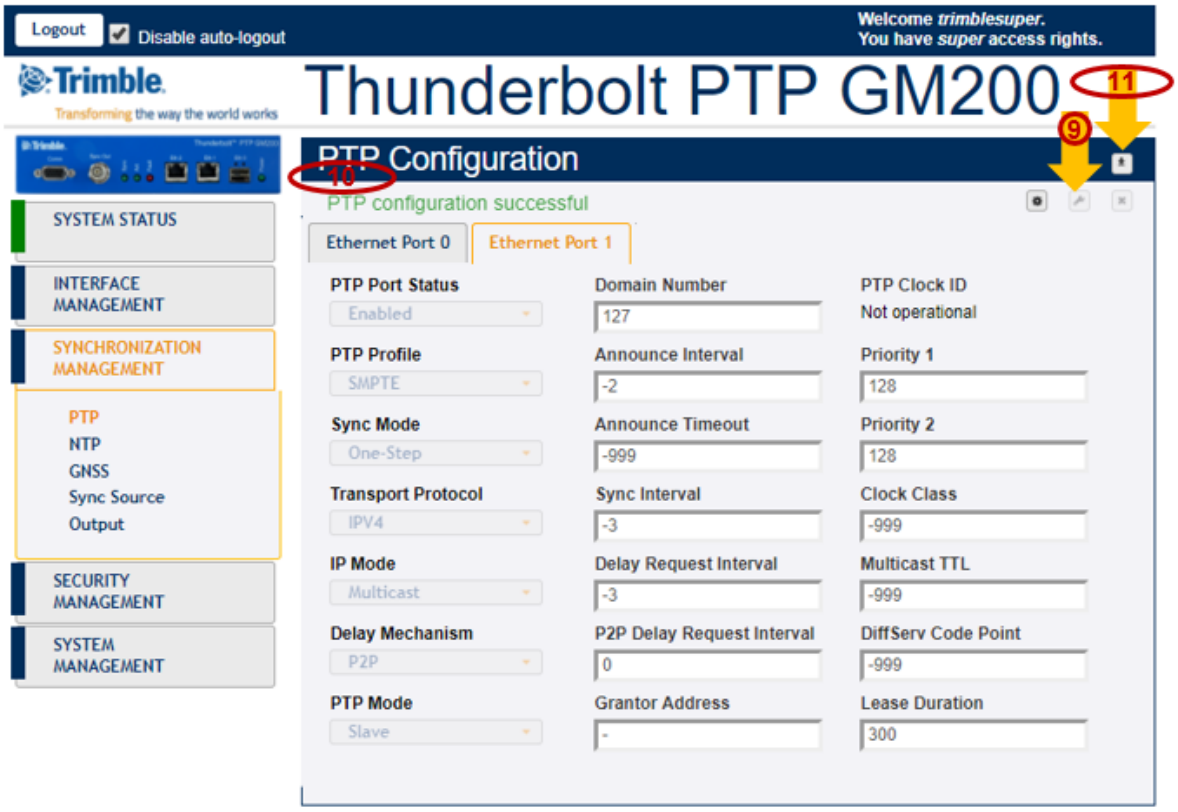
6. Select a profile from the **PTP Profile** list ❻ .
7. Most settings are changed automatically based on the selected profile, so if you don't have any specific settings for the profile you chose, just use default values for the profile ❼.
8. From the PTP Mode list, select **Slave** ❽.

> NOTE – If you are using the Unicast profile, set the **Grantor Address** field. This is the Master GM IP address. If you are using the Multicast profile, you don't need to set the **Grantor Address**.

> NOTE – Configure the PTP slave port first and enable it (it is still disabled at this point). Then, go to the PTP master port and enable it. Now both Master and Slave ports are enabled at once.

9. Click **Set**  to apply the settings ❾ .

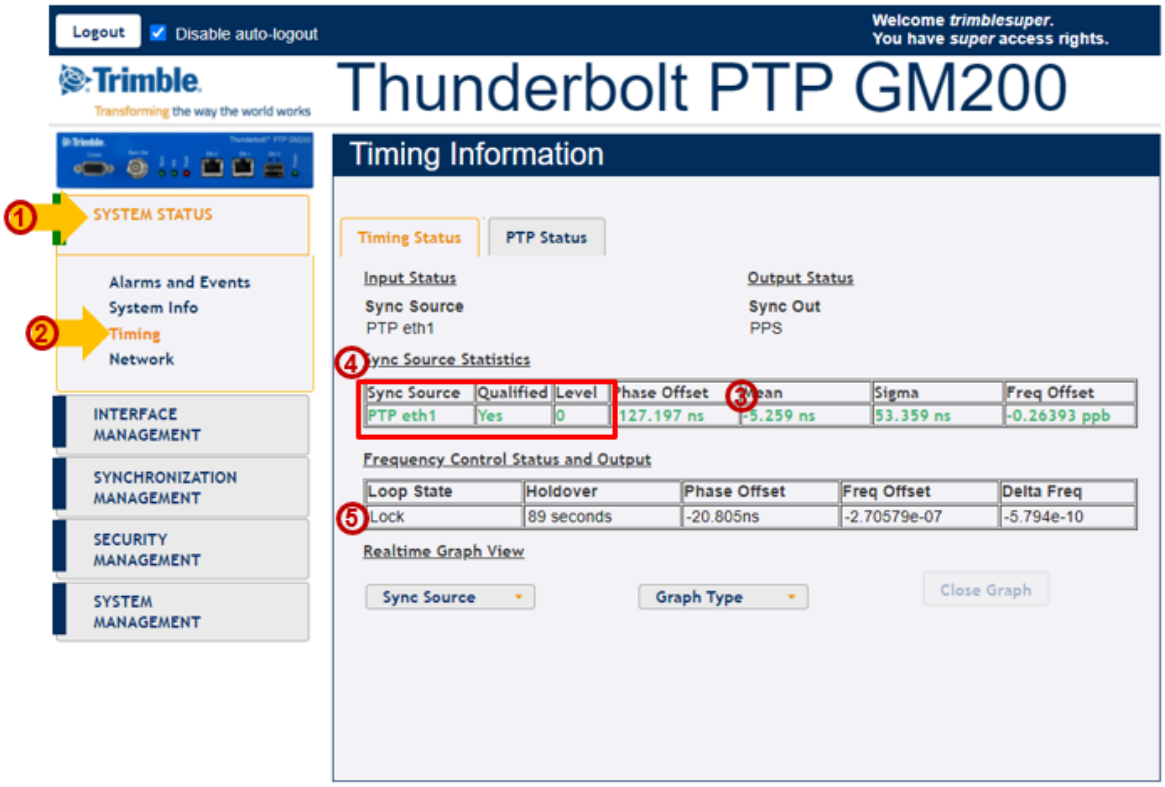
10. A confirmation message **PTP configuration successful** appears ❿.



11. Click the **Save System Configuration** icon to save the current settings ⓫.

9.1.5.8 Status of the BC PTP Slave operation

After completing the PTP slave configuration, you can confirm the status of the time server.



1. Select SYSTEM STATUS ❶ and then Timing ❷.

   After about five minutes, you will see time offset values as in the example above on PTP eth1 ❸.

2. Check the Sync Source Statistics values ❹, for the external PTP reference:

   Sync Source = PTP eth1
   Qualified = Yes
   Level = 0

3. Check that the Loop State field status is Lock ❺.

   Now the time server is locked to external PTP input.

4. If you want to see **Real-time Graph View** for phase offset of incoming PTP reference:
   a. Click **Realtime Graph View** to expand the information. The following screen appears:

   b. Click **PTP eth1** ❻.
   c. Click **Phase Offset** ❼.

      You will see a real-time graph for a selected reference source.

9.2 VLAN operation

The time server supports four VLANs each for Eth0 and Eth1, with VLAN IDs from 0 to 4094 as a Tagged VLAN 802.1q.

9.2.1. VLANs overview

The time server supports up to four virtual LANs (VLANs) on each port; eight VLANs in total.

Each VLAN must have its own address and subnet.

There is no default VLAN configuration. The VLANs can be configured with a default gateway.

All VLANs configuration can be deleted with the CLI command:

```
set network eth0/1 vlan -1
```

9.2.2 Configuring VLANs in CLI commands

Add up to four different VLAN IDs for each Ethernet port:

```
set network eth0/1 vlan ID1,ID2,…
```

Configure IP address, subnet mask, and gateway address for each VLAN ID:

```
set network eth0/1.ID addr <x.x.x.x> mask <y.y.y.y>
gateway <z.z.z.z>
```

Disable VLAN on the selected Ethernet port. Use the special ID of '-1':

```
set network eth0/1 vlan -1
```

Show Ethernet port configuration including VLAN configuration on the selected Ethernet port.

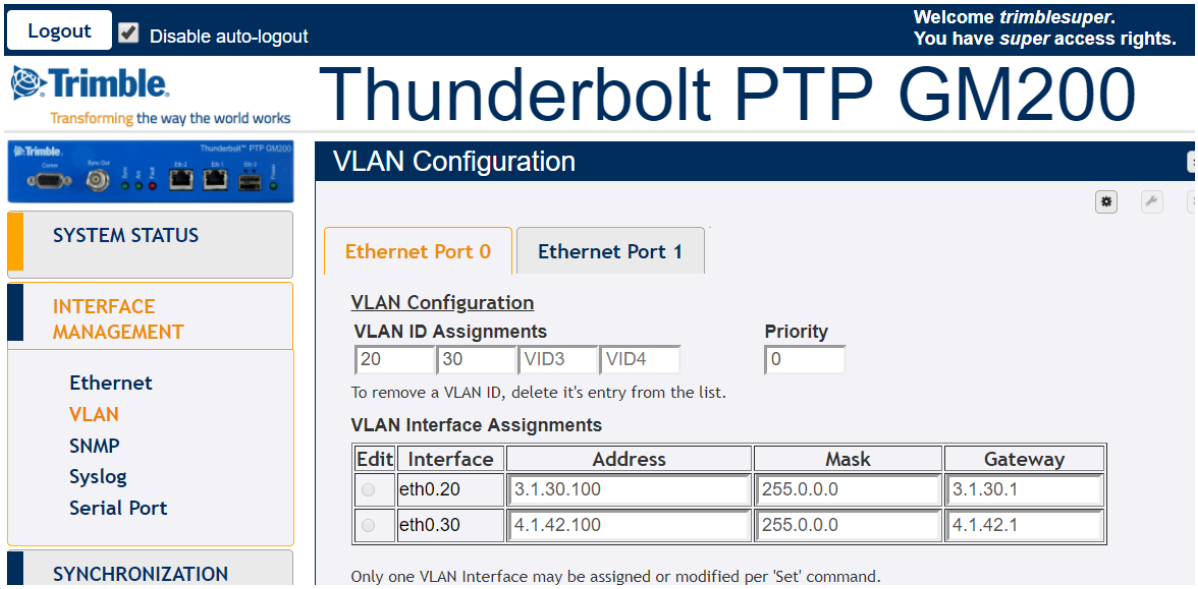
```
get network eth0/1
```

NOTE – When changes are applied to any Ethernet port, it takes up to 30 seconds to see changes in the Ethernet port configuration.

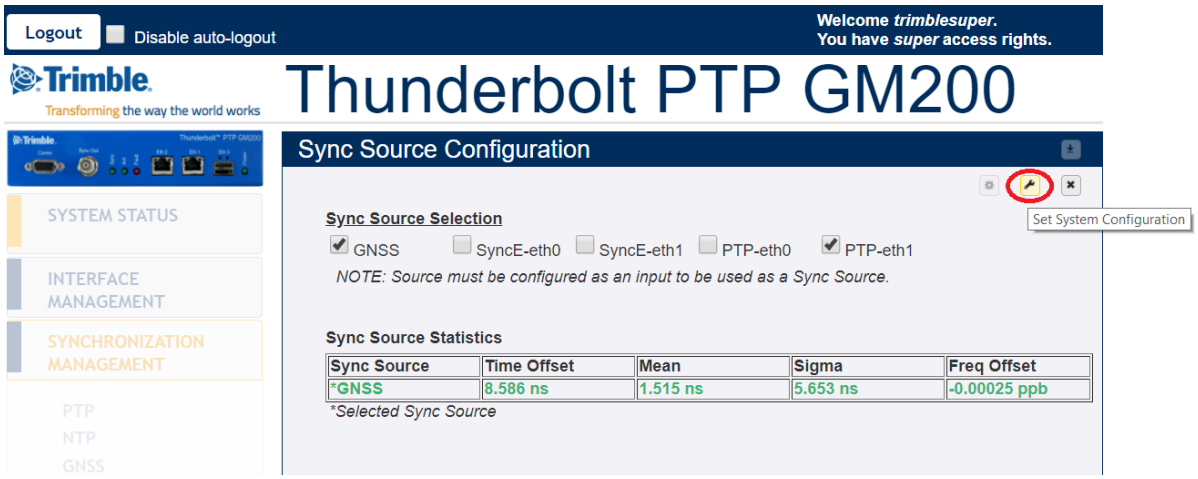
9.2.3 Configuring VLANs in the web interface

To be used as PTP input, an Ethernet port must be configured as input.

1. Connect to the time server using http or https.
2. Log in with the correct username and privileges like admin or supervisor access level.
3. Select INTERFACE MANAGEMENT and then VLAN.



4. To make changes, click Configure  .
5. Click Set  to apply the changes.



NOTE – VLAN IDs 1 and 2 are reserved, you cannot use them.

You must add the **VLAN ID**, **Priority** (0 is the highest priority), the **IP address** and **subnet mask**.

9.2.4 Configuring one VLAN ID

Example 1:

Use the following procedure to configure a VLAN on the eth0 port, an ID 452, IPv4 address of 21.153.200.230, a netmask of 255.255.255.248, and a gateway of 21.153.200.225:

1. Log in with the correct username and privileges like admin or supervisor access level.
2. Disable NTP and PTP services in order to configure any VLAN ID:

   ```
   set ptp eth0 disable
   set ntp eth0 disable
   ```

3. Type the following command and then press **Enter**:

   ```
   set network eth0 vlan 452
   ```

4. Type the following command and then press **Enter**:

   ```
   set network eth0.452 addr 21.153.200.230 mask 255.255.255.248
   gateway 21.153.200.225
   ```

5. Type the following command and then press **Enter**:

   ```
   get network eth0
   ```

   The Console output shows:

   ```
   >
   >
   > get network eth0
   Current settings for eth0:
   Status: Connected 1000MB
   Mode: Static
   Address: 192.168.0.250
   Mask: 255.255.255.0
   Broadcast: 192.168.0.255
   Gateway: 192.168.0.1
   IPv6 Addr: fe80::217:47ff:fe7f:fdad/64 Scope:Link
   VLAN IDs: 452
   syncE: Off

   Current settings for eth0.452:
   Status: Connected 1000MB
   Mode: Static
   Address: 21.153.200.230
   ```

```
Mask: 255.255.255.248
Broadcast: 21.153.200.231
Gateway: 21.153.200.225
IPv6 Addr: fe80::217:47ff:fe7f:fdad/64 Scope:Link
>
>
>
```

6. You can now enable again the NTP or PTP service:

```
set ptp eth0 enable
set ntp eth0 enable
```

> NOTE – VLAN IDs 1 and 2 are reserved; you cannot use them.

9.2.5 Adding another VLAN ID

Example 2:

Use the following procedure to add a VLAN ID 444 on Ethernet eth1 port. This port has already a VLAN ID:

```
VLAN ID 333
IP address 21.134.199.220
Subnet mask 255.255.255.248
Gateway 21.134.199.215
```

The new VLAN information will be:

```
VLAN ID 444
IP address 11.34.99.20
Subnet mask 255.255.255.248
Gateway 11.34.99.15
```

1. Log in with the correct username and privileges like admin or supervisor access level.
2. Disable NTP and PTP services to configure any VLAN ID:

```
set ptp eth1 disable
set ntp eth1 disable
```

3. Type the following command and then press Enter:

```
get network eth1
```

The Console output shows:

```
>
> get network eth1

Current settings for eth1:
Status: Connected 1000MB
Mode: Static
Address: 4.4.4.4
Mask: 255.255.255.0
Broadcast: 4.4.4.255
Gateway:
IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link
VLAN IDs: 333
syncE: Off

Current settings for eth1.333:
Status: Connected 1000MB
Mode: Static
Address: 21.134.199.220
Mask: 255.255.255.248
Broadcast: 21.134.199.223
Gateway: 21.134.199.215
IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link

>
>
>
```

4. Type the following command and then press **Enter**:

   ```
   set network eth1 vlan 333,444
   ```

5. Type the following command and then press **Enter**:

   ```
   get network eth1
   ```

   The Console output shows:

   ```
   >
   > get network eth1
   Current settings for eth1:
   Status: Connected 1000MB
   Mode: Static
   Address: 4.4.4.4
   Mask: 255.255.255.0
   Broadcast: 4.4.4.255
   Gateway:
   IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link
   VLAN IDs: 333, 444
   ```

```
syncE: Off

Current settings for eth1.333:
Status: Connected 1000MB
Mode: Static
Address: 21.134.199.220
Mask: 255.255.255.248
Broadcast: 21.134.199.223
Gateway: 21.134.199.215
IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link

Current settings for eth1.444:
Status: Connected 1000MB
Mode: Static
Address: 21.134.199.220
Mask: 255.255.255.248
Broadcast: 21.134.199.223
Gateway: 21.134.199.215
IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link

>
>
```

6. Type the following command and then press **Enter**:

   ```
   set network eth1.444 addr 11.34.99.20 mask 255.255.255.248
   gateway 11.34.99.15
   ```

7. Type the following command and then press **Enter**:

   ```
   get network eth1
   ```

   The Console output shows:

   ```
   >
   > get network eth1
   Current settings for eth1:
   Status: Connected 1000MB
   Mode: Static
   Address: 4.4.4.4
   Mask: 255.255.255.0
   Broadcast: 4.4.4.255
   Gateway:
   IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link
   VLAN IDs: 333, 444
   syncE: Off

   Current settings for eth1.333:
   Status: Connected 1000MB
   Mode: Static
   ```

```
Address: 21.134.199.220
Mask: 255.255.255.248
Broadcast: 21.134.199.223
Gateway: 21.134.199.215
IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link

Current settings for eth1.444:
Status: Connected 1000MB
Mode: Static
Address: 11.34.99.20
Mask: 255.255.255.248
Broadcast: 11.34.99.23
Gateway: 11.34.99.15
IPv6 Addr: fe80::217:47ff:fe7f:fdae/64 Scope:Link
2017-07-12T07:38:17.731Z: Set alarm 20, 'Eth-Port0-
Down'
2017-07-12T07:38:18.744Z: Set alarm 21, 'Eth-Port1-
Down'
2017-07-12T07:38:25.265Z: Clear alarm 21, 'Eth-Port1-
Down'
>
>
>
>
```

8. You can now enable the NTP or PTP service again:

```
set ptp eth1 enable
set ntp eth1 enable
```

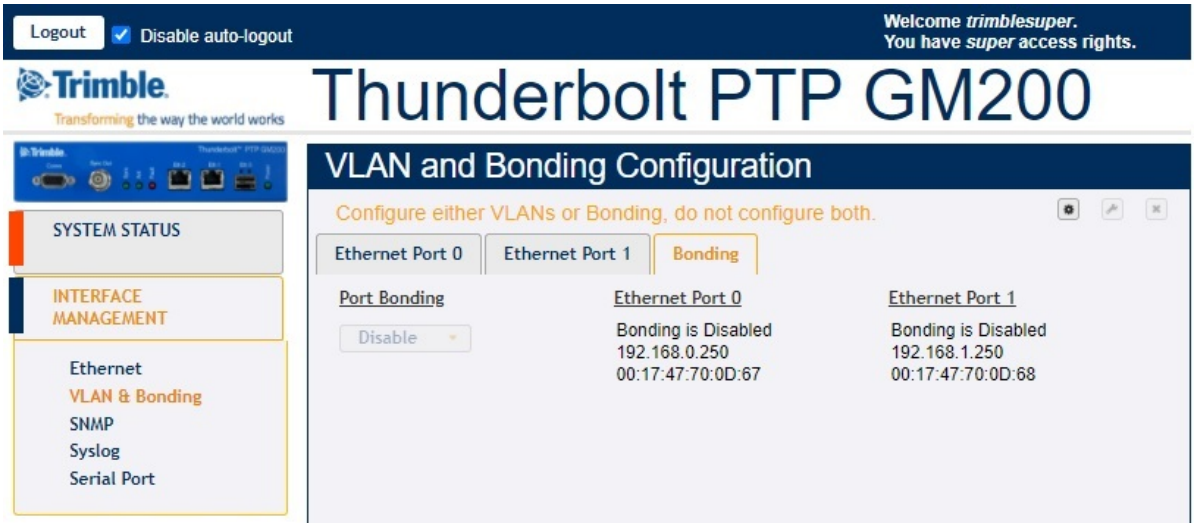
9.2.6 Removing all VLAN IDs

To disable all VLAN configuration on a specific Ethernet port, use the following command:

```
set network eth0/1 vlan -1
```

9.2.7 Port Bonding configuration with NTP

To access this tab, select SYSTEM STATUS / VLAN & Bonding / Bonding.



Port Bonding: Either Enable, Disable, or Swap.

Ethernet Port 0: Port Bonding Status on Eth0. Either Disabled, Active, or Standby with IPv4 and Mac Address.

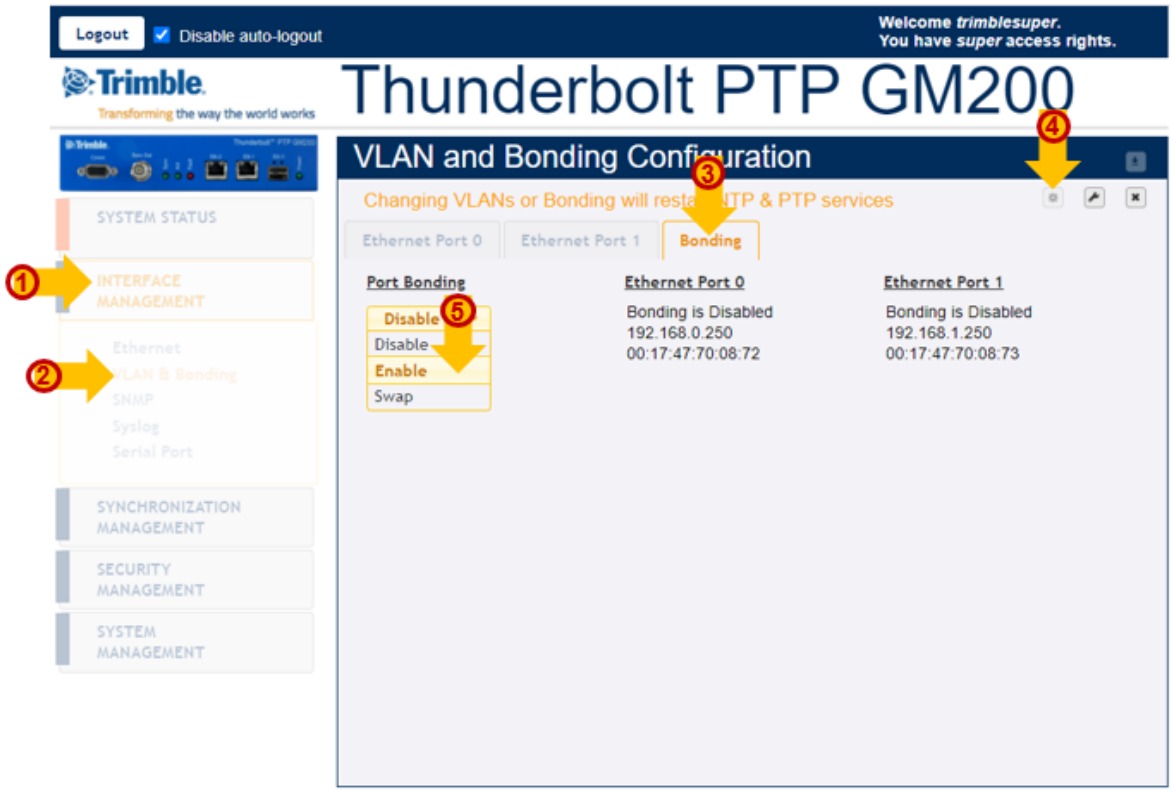
Ethernet Port 1: Port Bonding Status on Eth0. Either Disabled, Active, or Standby with IPv4 and Mac Address.

> NOTE – VLANs and Bonding cannot be configured simultaneously.

The main tasks to link the time server with NTP are:

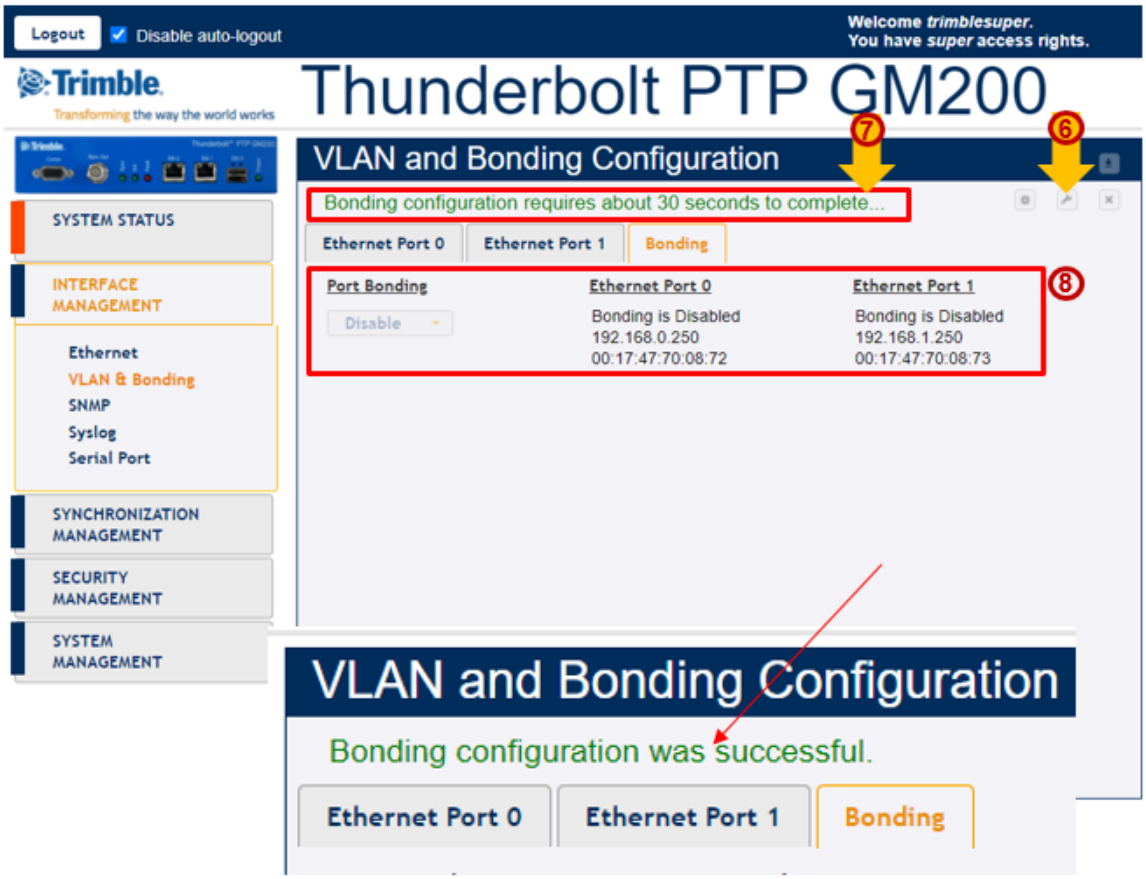
1. Link on for both Eth0 and Eth1.
2. Configure the IP address to meet with the installed network.
3. Ping to an NTP Client and then confirm it works.
4. Enable NTP operation.
5. Enable Bonding function.
6. Ping to NTP Client and then confirm it works with the “Bonding” operation.
7. Check NTP clients, whether it synchronizes with the time server.
8. Remove or Swap the “Active” interface and then confirm that NTP clients are still synchronizing with the time server.

The basic operation of the port bonding in the time server is to bond two Ethernet interfaces with the same IP address and Mac address, as one port is active and the other port is standby, so that two physical interfaces act as one logical interface.



1. Select INTERFACE MANAGEMENT ❶ and then VLAN & Bonding ❷.
2. Click the **Bonding** tab ❸.
3. Click **Configure** ❹.
4. In the **Port Bonding** drop-down list, select **Enable** ❺.

5. Click **Set** to apply the settings ❻.

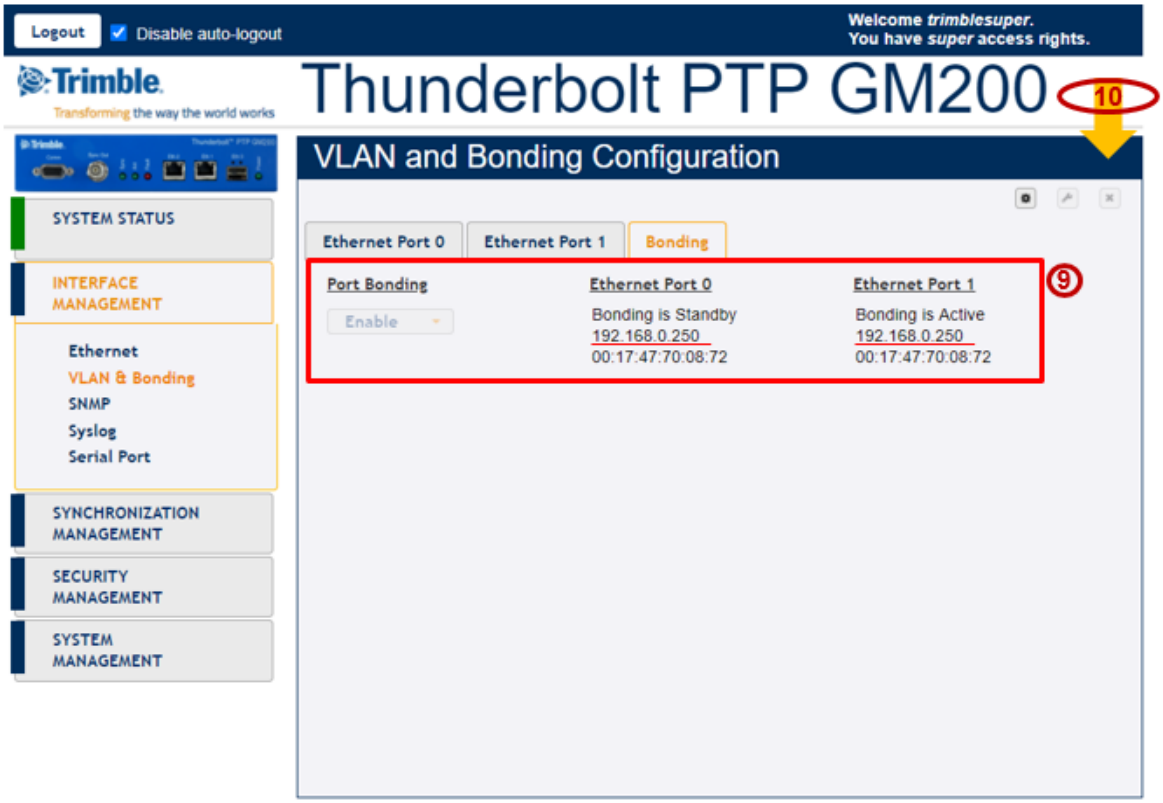


The time server shows a message with **Bonding configuration requires about 30 seconds to complete...** ❼.

After 30 seconds the **Bonding configuration was successful** message shows.

> NOTE – During these 30 seconds, the **Configure** and **Set** icons are deactivated so that you cannot set any other configuration while applying the bonding.
>
> NOTE – During the process of applying the bonding, the Eth0 and Eth1 still show **Bonding is Disabled**, with different IP address and Mac address ❽.

6. Within 30 seconds of seeing the completion message, the screen shows the same IP address and Mac address with **Bonding is Standby** in Eth0 and'**Bonding is Active** in Eth1 ❾:



7. Click **Save configuration** to store and restore your configuration after power on reset ❿.

9.3 Freerun operation

The time server needs to connect to a GNSS antenna to correctly start the PTP operation as a mandatory of the GM operation.

However, if the time server cannot connect to a GNSS antenna, the Freerun mode immediately enables the PTP operation without a GNSS antenna connection.

The PTP protocol is activated as soon as the system has started, but without GNSS tracking. This means that the PTP timestamps are either started from the PTP epoch, manually set by the user (via the web interface), set from an NTP server (see timesource option), or from GNSS.

The frequency control will be in Freerun mode until the GNSS tracks and locks. If GNSS tracks and locks, the PTP timestamps are immediately set to the time based on GNSS.

In the Freerun mode without GNSS or PTP time reference, it is limited for supplying a local phase and frequency synchronization. Estimated frequency accuracy is within 4e-8 for an hour and within 1e-8 for 24 hours in the condition of 25 °C ambient temperature over one hour aging and starting measuring after five minutes of the OCXO warm-up time.

- Configuring the Freerun mode using the CLI command
- Configuring the Freerun mode using the web interface

9.3.1. Configuring the Freerun mode using the CLI command

You can follow the example below to configure the Freerun mode with the CLI command or you can use the command "help set system" to get an explanation of how to use it.

There are three modes: GM, Freerun, and BC (Boundary Clock), which is at the system-level configuration. This means you can start the command with the "system" category to configure the Freerun mode.

To get an explanation:

```
help set system
```

To configure the Freerun mode:

```
set system opermode freerun
```

To start the PTP operation with the current time value for PTP timestamps, the time server should receive the time from the web interface or an NTP server.

```
set system opermode freerun ntpip 192.168.2.17 ntpto 60
```

If you finish the configuration, save the configuration and then reboot the system so that Freerun mode starts.

To confirm the configuration status, use the following command:

```
get system
```

Then, the time server will show as:

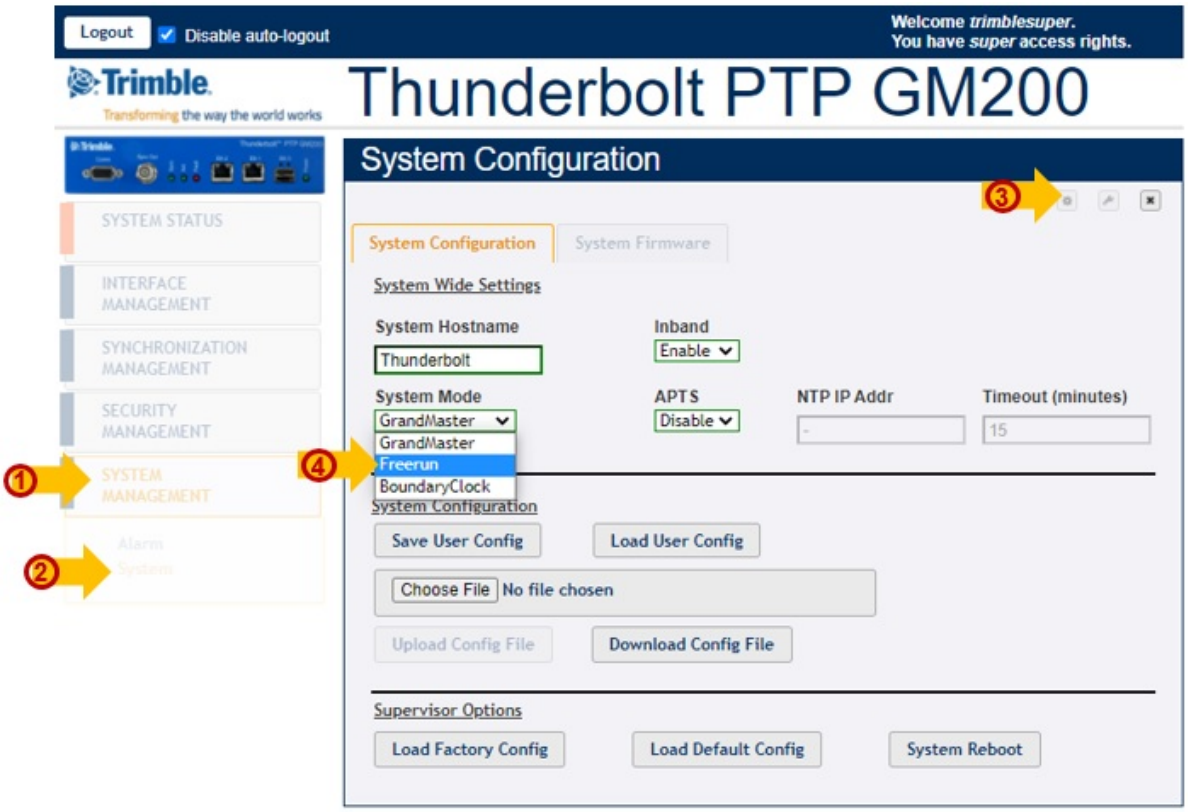
```
Thunderbolt> get system
     Hostname : Thunderbolt
    Oper Mode : freerun
       NTP IP : 192.168.2.17
      Timeout : 60 minutes
       Inband : Enabled
```

TIP – To get the current time from the time server web interface, log into the web interface.

NOTE – The Freerun mode is not supported for NTP operation.

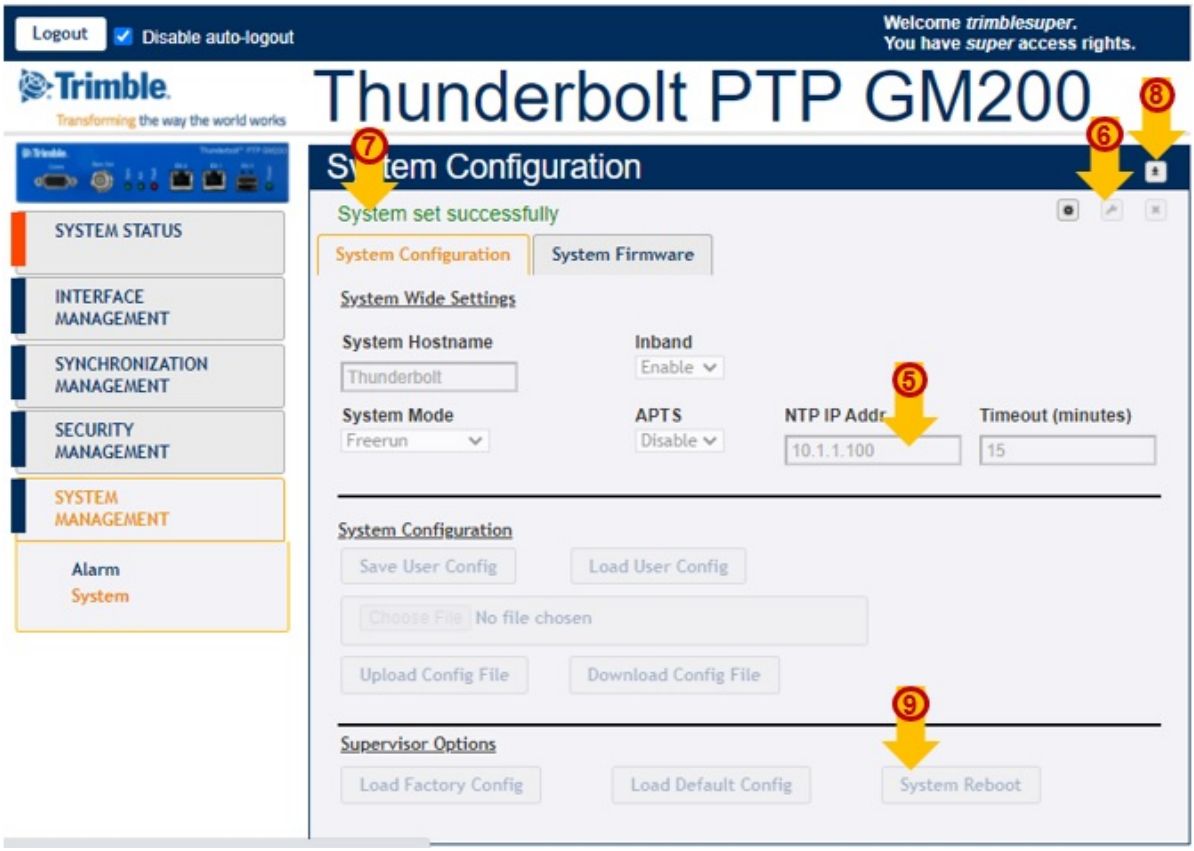
9.3.2. Configuring the Freerun mode using the web interface

To configure the Freerun mode using the web interface:



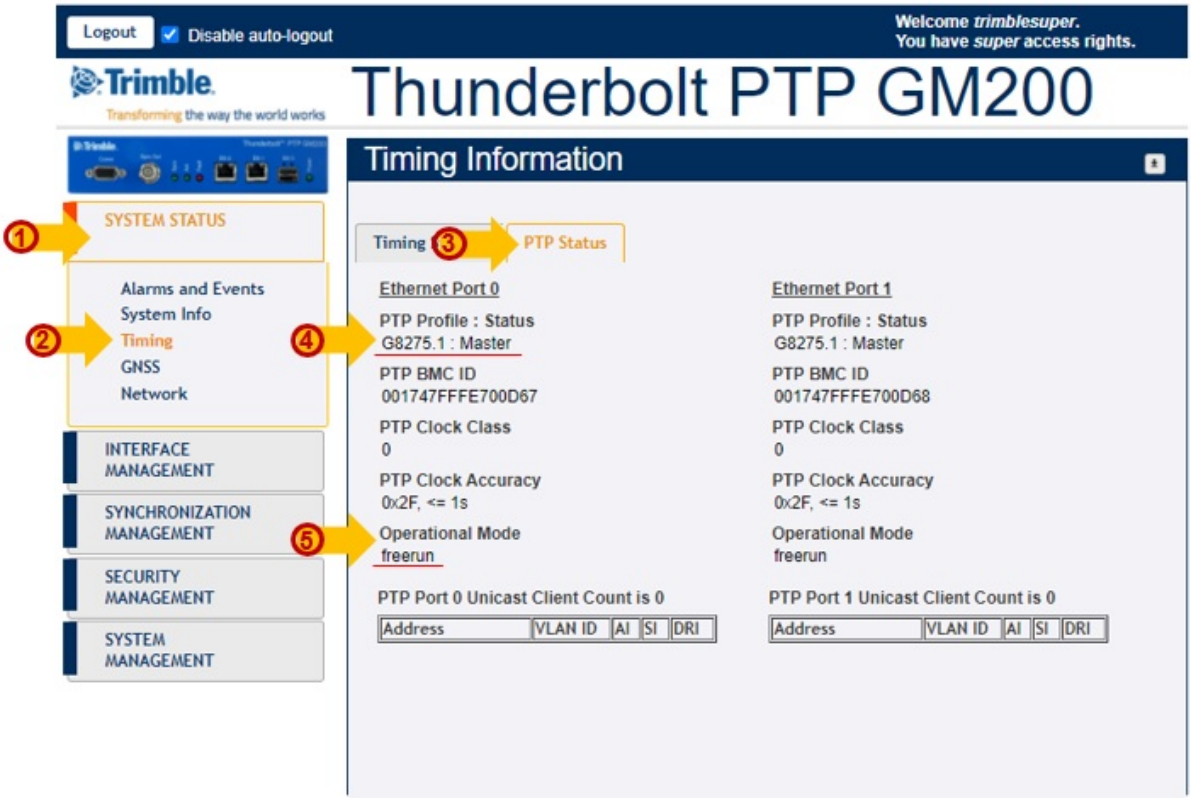
1. Click SYSTEM MANAGEMENT.
2. Click System.
3. Click Configure  . Settings are then activated in the System Configuration tab.

4. In the **System Mode** list, select the Freerun option:



5. Either configure the NTP server IP address to get a current time, or leave this field blank but log into the web interface so that the time server can receive the current time from the PC via the web interface.
6. Click **Set** to apply the settings.
7. The message **PTP configuration successful** appears.
8. Click the **Save System Configuration** button to save the current settings.
9. Apply the system reboot to restart the system in the Freerun mode.

To confirm your Freerun mode configuration:



1. Click **SYSTEM STATUS**.
2. Click **Timing**.
3. Select the **PTP Status** tab.
4. The **PTP Profile: Status** field must be showing configured by the user.
5. The **Operational Mode** field must show **freerun**.

TIP – To get the current time from the time server web interface, log into the web interface.

NOTE – The Freerun mode is not supported for NTP operation.

Appendix A: Alarms

This appendix lists the available alarms.

Alarm	Alarm Title	Level	Description	How to resolve
0	GNSS-Comm-E1	CRI	An internal GNSS communication alarm that indicates that the system is unable to process characters from the GNSS receiver as fast as it is being generated. This alarm should never be present and is used as a BIST (built-in self-test) indication of a hardware failure.	Call Trimble Technical Support (see page 26)
1	GNSS-Comm-E2	CRI	An internal GNSS communication alarm that indicates that the system is unable to process GNSS response data from the GNSS receiver as fast as it is being generated. This alarm should never be present and is used as a BIST (built-in self-test) indication of a hardware issue. This may be caused by excessive processing load on the system (denial of service attack).	Call Trimble Technical Support
2	GNSS-Comm-Loss	CRI	Complete communication has been lost to the GNSS receiver. This may be due to a bad receiver, or a bad receiver firmware update was recently applied. If an update was recently applied, the system administrator can try loading the firmware again, or loading a previous firmware version. Note that this alarm may be set on startup as the GNSS receiver is restarting.	Call Trimble Technical Support

Alarm	Alarm Title	Level	Description	How to resolve
3	GNSS-Ant-Shorted	MIN	There is an overcurrent event on the antenna feed. The unit may not be able to acquire satellites as the antenna may be damaged. The condition should be remedied before continuing operation.	Disconnect the antenna cable from the unit and verify the alarm clears; the GNSS-Ant-Open alarm should become active. Replace antenna, verify the alarm is clear; if the alarm is still active replace the antenna cable.
4	GNSS-Ant-Open	MIN	There is an undercurrent event on the antenna feed. This may be 'normal' if the antenna input is from a splitter or another device that blocks DC power. In this condition, the antenna must be externally powered. It is acceptable for the administrator to set the alarm level for this alarm to 'Ign' to clear this alarm condition.	Verify that the antenna and antenna cable are securely fastened. If they are, replace antenna.
5	GNSS-Track-No	MIN	The system cannot track any satellites at this time. This may be a 'normal' condition in the event of poor satellite coverage. For this reason, it is acceptable for this alarm to have a set and clear time associated with it to alleviate 'nuisance' type alarms.	This alarm is active whenever the system is powered-up or antenna is disconnected. Ensure the antenna is connected and the view of the sky is good.

Alarm	Alarm Title	Level	Description	How to resolve
6	PTP-PPS-Loss	MIN	The system cannot detect the 1PPS signal from the PTP input.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
7	GNSS-PPS-Loss	MIN	The system is not detecting the 1PPS signal from the GNSS system. This may be due to loss of GNSS signaling or invalid GNSS data. The unit will enter into holdover in this condition.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
8	Time-Sync-Bad	MAJ	The phase relationship for the PTP versus the time/frequency control is out of specification. This occurs during startup, while the phase is being aligned to GNSS, but it can also be an indication of extreme environmental changes that are causing the system phase to move faster than the control loop is able to compensate. This condition should clear when the conditions settle.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
9	Freq-Range-Bad	CRI	Set when the frequency control reaches a limit of 20E-6. Unless this is during a test condition, or the unit is tracking a simulator that is not locked to a valid frequency source, this is an indication of a failure of the frequency control and the unit requires service.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
10	N/A		There is no Alarm 10 within the system.	

Alarm	Alarm Title	Level	Description	How to resolve
11	GNSS-Time-Bad	MIN	Set when the GNSS system is indicating that the time has not been acquired from the satellites. This alarm will clear when the unit begins tracking valid satellite signals.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
12	Freq-Loop-Unlock	MIN	The frequency control loop has not yet established a locking condition. This is set during startup, while the control loop is settling, but may also be set during recover from holdover or in the event of severe environmental changes. This alarm will clear when the unit has achieved lock to the GNSS signal.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
13	Freq-Hold-Exceed	MAJ	The unit is in the halt condition (no compensation during holdover), or the unit has been in a holdover condition for more than 24 hours.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
14	PPS-Sync-Bad	MAJ	The PPS output (timing) from the system does not meet specification. This may occur during extreme environmental changes and should clear when the system becomes stable.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support

Alarm	Alarm Title	Level	Description	How to resolve
15	Freq-Out-Bad	MAJ	The frequency output from the unit is adversely affecting performance. This may occur during extreme environmental changes and should clear when the system becomes stable.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
16	PTP-System-Bad	CRI	The PTP system is not operational. PTP is only started after the phase and frequency alarms, as well as the time sync alarm, have all been cleared.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
17	FPGA-Load-Bad	CRI	The FPGA hardware image is too old for this firmware. The hardware should be updated using the *config firmware* command.	Call Trimble Technical Support
18	GNSS-Pos-Integrity	MIN	The unit has not tracked enough satellites to allow for a validation of the position. This is cleared once the unit has validated the position. When the position is not known then the integrity of the timing solutions may be suspect.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support
19	UTC-Corr-Unk	MAJ	The unit does not have the UTC corrections from the GNSS system. This is cleared once the UTC corrections have been acquired from the GNSS system. This is an issue because PTP requires the UTC correction be transmitted on most systems so that the sync to UTC may be established.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support

Alarm	Alarm Title	Level	Description	How to resolve
20	Eth-Port0-Down	MAJ	Ethernet Port 0 is not operational. Note that, if the user commands the port to be disabled, this alarm is cleared. The alarm is set only when it is a fault condition and disabling of the port is not considered a fault.	Check to make sure the Ethernet cable is connected at both ends. If this port is not to be used, then Ethernet Port can be disabled to clear this alarm.
21	Eth-Port1-Down	MAJ	Ethernet Port 1 is not operational. Note that, if the user commands the port to be disabled, this alarm is cleared. The alarm is set only when it is a fault condition and disabling of the port is not considered a fault.	Check to make sure the Ethernet cable is connected at both ends. If this port is not to be used, then Ethernet Port can be disabled to clear this alarm.
22	Eth-Mgmt-Down	MAJ	Ethernet Port 2 is not operational. Note that, if the user commands the port to be disabled, this alarm is cleared. The alarm is set only when it is a fault condition and disabling of the port is not considered a fault.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support

Alarm	Alarm Title	Level	Description	How to resolve
23	Eth-Same-Subnet	CRI	The Ethernet ports are on the same subnet. This is problematic for PTP because PTP requires that the data is timestamped on the physical port which received the packet. Due to the routing and socket parsing within the network, if two ports have the same subnet, the data may actually be received on a different physical port. For PTP, that would then mean that the timestamp was for a completely different path than what may be intended. Worse yet, if a timing port and the management port are on the same subnet then the PTP traffic may be received over the management port, which does not have the hardware timestamping capabilities. That makes all timestamps in the communication '0'. NOTE – The above is only an issue if you are using PTP as unicast on an IPv4 network. If you are multicast, or using IPv6 or 802.3, this alarm can be safely ignored.	Configure the ethernet ports to use different subnets.

Alarm	Alarm Title	Level	Description	How to resolve
24	SyncE0-Unsupported	CRI	Set when SyncE (either input or output) is enabled on eth0 and the SFP that is inserted does not support SyncE functions. If there is no SFP, or there are no SyncE functionality enabled for the port, this alarm is clear.	If SyncE support is required, the SFP must be changed to a model that supports SyncE, otherwise the alarm may be set to IGN. Call Trimble Technical Support
25	SyncE1-Unsupported	CRI	Set when SyncE (either input or output) is not capable to support on eth1 and If there are no SyncE functionality enabled for the port, this alarm is clear.	
26	Time-Set-Bad	CRI	The hardware time has never been set to agree with a valid phase source. This occurs only on startup and clears as soon as the unit has a valid phase time to establish a valid time reference.	If the alarm persists for longer than 60 minutes, call Trimble Technical Support

NOTE – "Level" means default set level of alarm. It has several levels and you can choose one of options below.

- IGN : This alarm condition is ignored. No indication is given.
- NFY : This alarm condition is a notification only.
- MIN : This is a minor alarm condition.
- MAJ : This is a major alarm condition.
- CRI : This is a critical alarm condition.