Thunderbolt® PTP
GM200 IEEE-1588
Grandmaster Clock
NTP Time Server

For use with: Thunderbolt® PTP Grandmaster Clock (P/N 111224-10)
Firmware version 1.5.0.0

Version D - July 2020
Part Number 106131-00
Legal Notices

Corporate Office
Trimble Inc.
935 Stewart Drive
Sunnyvale, California 94085
United States of America.
www.trimble.com
Email: tsgsupport@trimble.com

Copyright and Trademarks
© 2018, Trimble Inc.

Trimble and the Globe & Triangle logo are trademarks of Trimble Inc., registered in the United States and in other countries.
Thunderbolt 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 March 2018 release of the Thunderbolt® PTP Grandmaster Clock, part number 111224-10.

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") shall 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 tgsupport@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 THE EXCLUSION OR LIMITATION OF 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 HEREFIN SHALL BE LIMITED TO THE AMOUNT PAID BY YOU FOR THE PRODUCT AND 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 ANY WAY 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 www.trimble.com/ev.shtml.

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

Déclaration de Conformité
We, Trimble Inc.,
935 Stewart Drive
Sunnyvale, CA 94085-3913
United States of America
+1-408-481-8000

declare under sole responsibility that the product: Thunderbolt® PTP Grandmaster Clock 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

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-GPS</td>
<td>Assisted GPS</td>
</tr>
<tr>
<td>C/No</td>
<td>Carrier-to-Noise power ratio</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DOP</td>
<td>Dilution of Precision</td>
</tr>
<tr>
<td>EGNOS</td>
<td>European Geostationary Navigation Overlay Service</td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
</tr>
<tr>
<td>GLONASS</td>
<td>GlobalNaya Navigatsionnaya Sputnikovaya Sistema</td>
</tr>
<tr>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite Systems</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>I/O</td>
<td>Input / Output</td>
</tr>
<tr>
<td>LNA</td>
<td>Low Noise Amplifier</td>
</tr>
<tr>
<td>NMEA</td>
<td>National Marine Electronics Association</td>
</tr>
<tr>
<td>OCXO</td>
<td>Oven Controlled Crystal Oscillator</td>
</tr>
<tr>
<td>OD mode</td>
<td>Over-determined clock mode</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>PCB</td>
<td>Printed Circuit Board</td>
</tr>
<tr>
<td>PDOP</td>
<td>Position Dilution of Precision</td>
</tr>
<tr>
<td>PPS</td>
<td>Pulse per Second</td>
</tr>
<tr>
<td>PTP</td>
<td>Precision Time Protocol (IEEE-1588)</td>
</tr>
<tr>
<td>QZSS</td>
<td>Quasi-Zenith Satellite System</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>Sync E</td>
<td>Synchronous Ethernet</td>
</tr>
<tr>
<td>TCXO</td>
<td>Temperature Controlled Crystal Oscillator</td>
</tr>
<tr>
<td>ToD</td>
<td>Time of Day</td>
</tr>
<tr>
<td>T-RAIM</td>
<td>Timing Receiver Autonomous Integrity Monitoring</td>
</tr>
<tr>
<td>T-SUTC</td>
<td>Universal Time Coordinated</td>
</tr>
<tr>
<td>VCC</td>
<td>Voltage at the Common Collector; positive supply voltage</td>
</tr>
<tr>
<td>VSWR</td>
<td>Voltage Standing Wave Ratio</td>
</tr>
</tbody>
</table>
Safety Information

Warnings and Cautions

An absence of specific alerts does not mean that there are no safety risks involved. Always follow the instructions that accompany a Warning or Caution. The information they provide is intended to minimize the risk of personal injury and/or damage to the equipment. In particular, observe safety instructions that are presented in the following formats:

**WARNING** – A Warning alerts you to a likely risk of serious injury to your person and/or damage to the equipment.

**CAUTION** – A Caution alerts you to a possible risk of damage to the equipment and/or loss of data.

**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.

![Caution Hot surface](image)

**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® PTP Grandmaster Clock outside the specified temperature range can damage it. For more information, see the product specifications on the data sheet.

**WARNING** – The Thunderbolt® PTP Grandmaster Clock is only to be used in a restricted access location.

**WARNING** – Short-circuit (overcurrent) protection device required. The Thunderbolt® PTP Grandmaster Clock relies on the building’s installation for short-circuit (overcurrent) protection. Ensure that the protective device is listed rated not greater than 10A.

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.
# Table of Contents

## Contents

- Legal Notices .................................................................................................................. 2
- List of Abbreviations ....................................................................................................... 5
- Safety Information .......................................................................................................... 6
  - Warnings and Cautions ................................................................................................. 6
  - Operation and storage ................................................................................................. 6
  - Routing any cable ......................................................................................................... 6
- Table of Contents ........................................................................................................... 7

1. Product Overview ......................................................................................................... 18
   1.1. Product Overview ................................................................................................... 19
   1.2. Key Features .......................................................................................................... 19
   1.3. Physical Specifications ......................................................................................... 19
   1.4. Performance .......................................................................................................... 20
   1.5. Front Panel Elements ............................................................................................ 21
      1.5.1. Comm EIA-232 Serial Port ............................................................................... 21
      1.5.2. Sync Out ........................................................................................................... 21
      1.5.3. Status LED ....................................................................................................... 21
      1.5.4. Eth 2 Management Port (LAN) ...................................................................... 21
      1.5.5. Eth 1 Ethernet Port .......................................................................................... 21
      1.5.6. Eth 0 SFP Port ................................................................................................ 21
   1.6. Back Panel Elements .............................................................................................. 22
      1.6.1. GNSS Antenna Connection ............................................................................. 22
      1.6.2. Power Input ...................................................................................................... 22
      1.6.3. Alarm Relay ..................................................................................................... 22
      1.6.4. Grounding ........................................................................................................ 22
   1.7. Use and care ............................................................................................................ 22
   1.8. Technical assistance ............................................................................................... 23

2. Installation .................................................................................................................... 26
   2.1. Getting Started ...................................................................................................... 27
4.4. CLI Command Set ................................................................................................................. 45
4.4.1. get alarm ......................................................................................................................... 45
4.4.2. set alarm ......................................................................................................................... 45
4.4.3. view alarm ....................................................................................................................... 46
4.4.4. view access ..................................................................................................................... 46
4.4.5. get auth .......................................................................................................................... 46
4.4.5.1. get auth local .............................................................................................................. 46
4.4.5.2. get auth tacacs ............................................................................................................ 47
4.4.5.3. get auth radius ........................................................................................................... 47
4.4.6. set auth ........................................................................................................................ 47
4.4.6.1. set auth radius ............................................................................................................ 48
4.4.6.2. set auth tacacs ............................................................................................................ 48
4.4.6.3. set auth local ............................................................................................................. 49
4.4.6.4. set auth type .............................................................................................................. 50
4.4.7. get auto ......................................................................................................................... 51
4.4.8. set auto ........................................................................................................................ 51
4.4.9. config ........................................................................................................................... 51
4.4.9.1. config firmware ......................................................................................................... 52
4.4.9.2. config firmware list ................................................................................................... 52
4.4.9.3. config firmware stage ............................................................................................... 52
4.4.9.4. config firmware update ............................................................................................. 53
4.4.9.5. config firmware unstage ............................................................................................ 53
4.4.9.6. config load ................................................................................................................ 54
4.4.9.7. config list ................................................................................................................... 54
4.4.9.8. config save ................................................................................................................ 54
4.4.9.9. config system ............................................................................................................ 55
4.4.10. get comm .................................................................................................................... 55
4.4.11. set comm ..................................................................................................................... 55
4.4.12. get date ....................................................................................................................... 57
4.4.13. get dlog ....................................................................................................................... 57
4.4.14. set dlog ....................................................................................................................... 57
4.4.15. download ..................................................................................................................... 58
4.4.16. get freq ....................................................................................................................... 58
4.4.50. view summary............................................................................................................. 77
4.4.51. view stream.................................................................................................................. 78
4.4.52. get syslog .................................................................................................................... 78
4.4.53. set syslog .................................................................................................................... 78
4.4.54. get system .................................................................................................................. 79
4.4.55. set system .................................................................................................................. 79
4.4.56. view temp .................................................................................................................. 80
4.4.57. get time ...................................................................................................................... 80
4.4.58. view uptime ............................................................................................................... 80
4.4.59. get user ...................................................................................................................... 81
4.4.60. set user ...................................................................................................................... 81
4.4.61. set user logout .......................................................................................................... 82
4.4.62. view user ................................................................................................................... 82
4.4.63. view version .............................................................................................................. 83
4.4.64. view ........................................................................................................................... 83
4.4.64.1. view dlog ................................................................................................................. 84
4.4.64.2. view gnss stream ................................................................................................. 84
4.4.65. help whatif ............................................................................................................... 84

4.5. List of “How to” help topics ......................................................................................... 85

4.5.1. How to get current Alarm status? .............................................................................. 85
4.5.2. How to set alarm of level major, alarm number 2 with setTime as 2 and clearTime as 1? ... 85
4.5.3. How to disable Ethernet port 0/1? ............................................................................. 85
4.5.4. How to set ip address of 192.168.0.9, and also set a netmask and a gateway address on ethernet 0 port? ................................................................................................. 86
4.5.5. How to set bnc output to even? ................................................................................. 86
4.5.6. How to set periodic output of period 2 and value 1? ................................................. 86
4.5.7. How to set serial port baud rate to 19200bps? ......................................................... 86
4.5.8. How to add a new user called trimble1 with an access level of user? ...................... 86
4.5.9. How to delete an existing user trimble? ..................................................................... 86
4.5.10. How to change user password? ............................................................................... 86
4.5.11. How to restore factory default settings? ................................................................. 86
4.5.12. How to reboot the system? ...................................................................................... 86

4.6. List of “What if” help topics ......................................................................................... 87
1. Product Overview

In this chapter:

Operation Key Features

Getting started Use and care

Technical assistance
1.1. Product Overview

Trimble’s Thunderbolt® PTP Grandmaster Clock GM-200 is a high quality IEEE-1588 PTP Grandmaster clock (GMC) with an integrated Trimble GNSS receiver. The Thunderbolt® PTP GMC is designed and optimized for the deployment in wireless service provider networks to meet the stringent time & phase requirements of 4G LTE and small cell networks.

It provides NTP, PTP and Synchronous Ethernet timing protocols. Thunderbolt® PTP GMC GM-200 uses GNSS (Global Navigation Satellite Systems) signals from GPS, GLONASS, Galileo, and Beidou as the primary time source for synchronization.

Thunderbolt® PTP 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 Thunderbolt® PTP Grandmaster clocks.

Thunderbolt® PTP comes in a rack-mountable enclosure; two Thunderbolt® PTP units fit side-by-side in a 1RU height 19” rack.

1.2. Key Features

- IEEE-1588 Precision Time Protocol Grandmaster
- 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 10MHz outputs)
- IPv4, IPv6 and VLAN
- 1 EIA-232 (RS-232) Serial Port
- Small foot print – ½ Rack 1U
- CLI / SNMP traps
- DC (default) and AC power options
- PTP/SyncE Input
- PTP “Freerun” mode

1.3. Physical Specifications

The Thunderbolt® PTP GMC can be installed in a 19-inch rack mount unit. It can fit in ½ rack space, 2 Thunderbolt® PTP GMC units can be installed side-by-side in a full rack space for additional redundancy.
1.4. Performance

The system level performance is defined by the total number of packets per second. The total/maximum number of packets per second supported is 6,272.

If Thunderbolt® PTP GM-200 is configured only as Grandmaster then it can support:

- 16 unicast PTP slaves/clients @ 128 packets per second
- 32 unicast PTP slaves/clients @ 64 packets per second
- 64 unicast PTP slaves/clients @ 32 packets per second
- 128 unicast PTP slaves/clients @ 16 packets per second
- 256 unicast PTP slaves/clients @ 8 packets per second
- Supports up to 4 VLANs on each port in total 8 VLAN

The upper limit on number of PTP slaves/client is 500 (unicast or multicast)

If Thunderbolt® PTP GM-200 is configured only as NTP Time Server then it can support NTP 2,500 transactions per second.

If Thunderbolt® PTP GM-200 is configured as Grandmaster and NTP Time Server at the same time (GMC and Time Server combination), then the maximum number of packets per second supported is 6,272.
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 Thunderbolt® PTP GMC through an EIA-232 female connector.

1.5.2. Sync Out
The Thunderbolt® PTP GMC features a BNC female connector that provides 1PPS output. It can be configured for 10MHz, see the set output command.
PPS: 3.0V into 50 Ohms. 1000ns default pulse width.
10MHz: Square wave 3.0V into 50 Ohms.

1.5.3. Status LED
The Thunderbolt® PTP GMC provides 4 LEDs on the front panel that indicate the following status:
   - Power
   - Antenna
   - Sync
   - Status/Alarm

1.5.4. Eth 2 Management Port (LAN)
The Thunderbolt® PTP GMC has one dedicated management Ethernet port. The RJ-45 port provides connectivity to Ethernet LAN for the configuration of the unit.

1.5.5. Eth 1 Ethernet Port
One RJ45 Ethernet port. Provides NTP/PTP connectivity to Ethernet Networks

1.5.6. Eth 0 SFP Port
The Thunderbolt® PTP GMC support one SFP port. Provides NTP/PTP connectivity to Ethernet Networks
1.6. Back Panel Elements

1.6.1. GNSS Antenna Connection
The Thunderbolt® PTP GMC features an SMA connector for the antenna input to the embedded GNSS receiver.

1.6.2. Power Input
The standard input power is -48VDC, 330mA. The Thunderbolt® PTP GMC provides a 5pole terminal block to connect dual DC power inputs.

1.6.3. Alarm Relay
The Thunderbolt® PTP GMC provides a 3.81mm 3pin terminal header for 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 Thunderbolt® PTP GMC is available through a M5 Grounding Terminal Stud.

1.7. Use and care
The Thunderbolt® PTP is a high-precision electronic instrument and should be treated with reasonable care. Thunderbolt® PTP typically doesn’t need any care after the first setup. Should you need to clean the unit, use a dry non-static tissue or a light moist tissue for removing dust or stain from the enclosure. Make sure that no water enters the Thunderbolt® PTP enclosure anywhere. Don’t use solvents, aggressive or abrasive cleaning agents anywhere on the Thunderbolt® PTP device.

*CAUTION – There are no user-serviceable parts inside the Thunderbolt® PTP Grandmaster Clock and 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 Assistance Center at 800-767-4822 or email tsgsupport@trimble.com.
2. Installation

In this chapter:

- Getting Started Time
- References Operation
- Timing module Performance
- Holdover
- Customization

This chapter describes the procedure for installing the Thunderbolt® PTP Grandmaster Clock (GMC) GM-200.
2.1. Getting Started

This section explains how to install and configure the Thunderbolt PTP GMC GM-200.

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

- Thunderbolt PTP Grandmaster Clock GM-200
- Mounting brackets and installation accessories
- Dummy plate for single unit installation in 19” rack

2.2. Mounting the Device to a Rack

The Thunderbolt PTP GMC should be installed indoor or outdoor in an environmental controlled cabinet. The Thunderbolt PTP GMC will install in an EIA standard 19-inch rack. The unit occupies ½ rack space and if required two GMC units can be installed side-by-side.

*NOTE* Forced airflow is not required.

2.3. Connecting Power

The Thunderbolt PTP GMC supports single or dual redundant AC or DC power supplies. The Thunderbolt PTP GMC standard option is 48VDC. The Thunderbolt PTP GMC is capable of operating from -36Vdc to -72Vdc at a maximum current level of 250mA.

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

*NOTE* – The power cable should be routed separately from the data (signal) cables.
2.3.1. **Grounding the Device**

The Thunderbolt PTP GMC M5 Terminal Stud on the back panel is used for grounding.

The Thunderbolt PTP GMC is suitable for connection to the Central Office and CPE. The grandmaster clock shall be located in a restricted access location where only craft personnel are allowed access.

The Thunderbolt PTP GMC shall be grounded via a copper ground conductor. The unit shall be installed and connected to the common bonding network (CBN).

All bare grounding connection points to the Thunderbolt PTP GMC shall be cleaned and coated with an anti-oxidant solution before connections are made.

All surfaces on the Thunderbolt PTP GMC that are un-plated shall be brought to a bright finish and treated with an antioxidant solution before connection is made.

All non-conductive surfaces on the Thunderbolt PTP GMC shall be removed from all threads and connection points to ensure electrical continuity.

The Thunderbolt PTP GMC DC power returns shall be treated as DC-I (Isolated from Frame Ground).

Thunderbolt PTP GMC requires a ring terminal with a 14-AWG wire that utilizes 15in-lbs to secure to primary ground.

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

2.3.2. **Powering-Up**

After verification of the input power source, switch on the power supply to the Thunderbolt PTP GMC. The Green Power LED should turn ON.

2.4. **GNSS Considerations**

See the next chapter for a full description of how to choose the correct antenna cable/antenna combination.

When connected to a GNSS antenna the Thunderbolt PTP GMC can receive GNSS signal without user intervention—the factory default is GPS and GLONASS. The user can enable Beidou in place of GLONASS or enable single constellation mode.
The Trimble family of Bullet antennas is best matched with Thunderbolt PTP GMC. 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

Connecting the GNSS antenna will turn the Antenna LED Green.

### 2.4.1. Selecting Site for 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 GPS antenna. The best locations provide:

- Unobstructed views of the sky and horizon.
- Low electro-magnetic 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 Thunderbolt PTP GMC.
2.5. **Communication Ports**

The Thunderbolt PTP GMC has four communications ports on the front panel.

- 1 Serial Port (RS232)
- 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 Serial port or Ethernet eth2 (RJ-45) is the dedicated management port to configure the GMC GM200.

2.5.1. **Serial Port**

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

![Serial Port pin assignments](image)

*Figure 2.1: Serial Port pin assignments*

Use a straight through cable with following setting:

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

**Serial Port Pin Assignment**

<table>
<thead>
<tr>
<th>Pin</th>
<th>RS-232 Signal</th>
<th>Description on Echo Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DCD</td>
<td>PPS</td>
</tr>
<tr>
<td>2</td>
<td>RxD</td>
<td>Data Transmit</td>
</tr>
<tr>
<td>3</td>
<td>TxD</td>
<td>Data Receive</td>
</tr>
<tr>
<td>4</td>
<td>DTR</td>
<td>Not Used</td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>6</td>
<td>DSR</td>
<td>Not Used</td>
</tr>
<tr>
<td>7</td>
<td>RTS</td>
<td>Not Used</td>
</tr>
<tr>
<td>8</td>
<td>CTS</td>
<td>Not Used</td>
</tr>
<tr>
<td>9</td>
<td>RI</td>
<td>Not Used</td>
</tr>
</tbody>
</table>
2.5.2. **Management Ethernet Port**

The Thunderbolt PTP GMC 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-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 as follows:

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

2.5.3. **PTP/NTP/SyncE Electrical Ethernet Port**

The Thunderbolt PTP GMC GM-200 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”. 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-1 network port are as follows:

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

*NOTE – The Ethernet interface shall not be connected to a cable longer than 6 meters. If a distance greater than 6 meters is required, then the Ethernet interface shall be connected to a switch to comply with GR-1089.*

2.5.4. **PTP/NTP/SyncE SFP Ethernet Port**

The Thunderbolt PTP GMC GM-200 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 as follows:

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

2.6. Status Indicators

Alarm and status information is presented through the use of four LEDs. In Critical alarm condition the dry contact relay output at the rear of the Thunderbolt® device is closed.

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Indication</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Green</td>
<td>ON</td>
<td>System is powered on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>System does not have power</td>
</tr>
<tr>
<td>ANT</td>
<td>Green</td>
<td>ON</td>
<td>Reference acquired &amp; tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking, 1/2Hz</td>
<td>Reference being acquired, or no computing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>No reference active or antenna</td>
</tr>
<tr>
<td>Sync</td>
<td>Green</td>
<td>ON</td>
<td>Locked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blinking, 1/2Hz</td>
<td>Acquisition or Holdover</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFF</td>
<td>Free-run or startup</td>
</tr>
<tr>
<td>Status</td>
<td>Red</td>
<td>OFF</td>
<td>No active alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ON</td>
<td>Critical Alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blink, 1Hz</td>
<td>Minor alarm condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blink, 1/2Hz</td>
<td>Major alarm condition</td>
</tr>
</tbody>
</table>
3. GNSS Antenna

In this chapter:

- Antenna Requirements
- OPEN/SHORT Detection
- Antenna Placement
- Multipath
- Jamming
- Ground plane

A good GNSS antenna, together with a good installation site, is the key for getting 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**

The antenna receives the GNSS satellite signals and passes them to the receiver. The GNSS signals are spread spectrum signals in the 1551MHz to 1614MHz 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 LNA. The received GNSS signals are very low power, approximately -130dBm, at the surface of the earth. Trimble's active antenna includes a preamplifier that filters and amplifies the GNSS signals before delivery to the receiver.

The onboard 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 onboard Open/Short detection with integrated current limiter. The GM200™ 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: +5V DC +/-0.5V.
Current detection: Open circuit < 10mA, Short circuit > 100mA.

**3.1.2. Antenna gain requirements**

The GM200™ requires an active GNSS antenna with built-in Low-Noise Amplifier (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 frontend.

Task b) requires an amplification of at least 15dB, while 20dB is the sweet spot for the GM200™. 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 30dB 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 15dB with a 30dB LNA. With a different antenna type, take the difference between 15dB and the antenna’s LNA gain as the available compensation capability. Subtract the insertion losses of all connectors from the 15dB (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 35dB 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 20dB to 30dB with a minimum of 15dB and a maximum of 35dB.
3.2 Antenna Placement

3.2.1. Sky-Visibility
GNSS signals can only be received on a direct line of sight between 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 placed south of the obstacles, preferably, in order not to block 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 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 6 satellites, all close together, and still get a much worse DOP than a receiver which sees 4 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.

3.2.2 Multipath-reflections
Multipath occurs when the GNSS signals are reflected by objects, such as metallic surfaces, walls and shielded glass for example. The antenna should not be placed near a wall, window or other large vertical objects if it can be avoided.

3.2.3 Jamming
Jamming occurs when the receiver function is disturbed by external 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’s no general installation rule or specification though, because the effect of jamming highly depends on the nature of the jamming signal and there are uncountable many variations possible, so that it's not possible to standardize a test scenario.

3.2.4. 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.

3.2.5. 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 6.5ns/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 shall 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.**

### 3.2.6. Lightning Considerations

Although, it is not possible to 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.

### 3.3 GNSS Tuning Parameters

The default GNSS parameters are suitable for most installations of the Thunderbolt PTP or NTP Server. These can include antenna installations with good or less than ideal views of the sky.

The parameters that are set from the factory should not be changed unless there are specific identified reception problems or timing issues. We would recommend discussing any changes with your local Trimble representative beforehand.

*Note - The exception is the Antenna Delay parameter that must be changed since it needs to be custom to the specific cable length of the installation.*

The tuning parameters should only be changed once all the antenna position and cabling instructions listed earlier in this chapter have been followed correctly. The parameters can be changed either by the web interface (Synchronization Management/GNSS) or the CLI (get/set gnss).

For the following parameter descriptions the Web page for GNSS is used for demonstration purposes but the CLI commands are also available and are described in Chapter 4.
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 Thunderbolt 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 5 satellites or more. After a successful first fix only 4 satellites are required. If fewer than the required number of satellites are visible, the Thunderbolt suspends the self-survey. 3-D 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 Thunderbolt 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 14400s or 4 hours. Four hours allows for the satellites to move either completely, or halfway, through their trajectory.
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 (2000s). This may be a factor in the user application but otherwise lengthening the self-survey period can potentially improve our solution.


### 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 (due to dense foliage for example), or reflected RF signals (multipath).

Multipath can degrade the position and timing solution. Multipath is most 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 35dB-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 0dB-Hz (zero) is recommended.

Permitted range: 0.0 to 55.0. Default 3.
4 CLI Reference

In this chapter:

- CLI Overview
- CLI Command Set

This chapter describes the Command Line Interface conventions, prompts, features and command syntax used in Thunderbolt® PTP Grandmaster Clock.
4.1. CLI Overview

The Command Line Interface (CLI), also called the ASCII command set, can be used to control the Thunderbolt® PTP GMC GM200 from a terminal connected to the RS-232 serial port, or the Ethernet port via Telnet/SSH access.

4.2. Command User Levels

The Thunderbolt® PTP GMC GM200 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 next 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. This is the Trimble user access level by default.

4.2.1. Initial Default Login Password

**NOTE** – There is a change in default password to comply with California State Bill SB-327. The SB-327 Information privacy: connected devices bill requires that the pre-programmed password is unique to each device manufactured.

The SB-327 bill is effective since January 1, 2020. To meet this requirement, Trimble has removed the trimble and trimbleadmin default 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. If desired, 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.
4.3. Command Line Format

The command line format is as follows:

    [action] command [parameter] [data] enter ( \ ) The type

of action to be taken with a command

- **Config** enables you to configure the device parameters
- **Get** allows you to retrieve specific information
- **Set** allows you to provision a specific parameter
- **View** enables you to display system information. This information cannot be altered
  by the user.

Help is available on the following topics:

- **help intro** an introduction to the Thunderbolt® PTP GMC
- **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 possible alarm conditions within the system

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

*NOTE – The GM200 has an extensive on-line, user level context aware, help system. The on-line help for the
most part is more up-to-date and accurate than the information in the user guide.*

*NOTE – After any configuration change via the SET command issue a “config save” command to store the
user configuration.*
4.4. CLI Command Set

This section provides an alphabetical listing and details of all CLI commands. This section describes the topic “help commands”.

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

4.4.1. get alarm

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

Command Syntax:

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

- `<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: User, Admin and Supervisor

4.4.2. set alarm

The set alarm command allows configuration of the system alarms. This is a multi-option command of the format:

Command Syntax:

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

Where:

- `<n>` The alarm number, this can be viewed with the 'get alarm' command
- `<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. This is the time, in seconds, that the alarm condition must be active before the alarm is actually asserted. Range is 0 - 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 actually cleared. Range is 0 - 86400 (1 day)

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

Level: Admin and Supervisor
4.4.3.  **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

4.4.4.  **view access**

This command shows access level of current logged in user. Command Syntax:

```
view access
```

Level: User, Admin and Supervisor

4.4.5.  **get auth**

Return the current authentication settings. You can query specific settings with the options:

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

4.4.5.1.  **get auth local**

Return the current settings for the local authentication parameters.

Syntax:

```
get auth local
```

Level: Supervisor
4.4.5.2.  **get auth tacacs**  
Return the current TACACS+ authentication settings.

Syntax:

```
get auth tacacs
```

Level:  Supervisor

4.4.5.3.  **get auth radius**  
Return the current RADIUS authentication settings.

Syntax:

```
get auth radius
```

Level:  Supervisor

4.4.6.  **set auth**  
The `set auth` command allows to change the authentication settings.

Command Syntax:

```
set auth <options>
```

Where `<options>` are:

- `default`  
  Set the authentication to the default settings

- `type [options]`  
  Set the authentication type options. Please see `help set auth type` for additional information

- `radius [options]`  
  Set the RADIUS authentication options. Please see `help set auth radius` for additional information.

- `Tacacs [options]`  
  Set the TACACS+ authentication options. Please see `help set auth tacacs` for additional information.

**NOTE** – Authentication `<options>` cannot be combined on one line, all command variants must be presented separately.

Level:  Supervisor
4.4.6.1. set auth radius

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

Command Syntax:

```
set auth radius (options)
```

Where the 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 be enclosed in "" to allow setting of characters that might be interpreted as parameter separators.
- `timeout` Set the RADIUS server timeout value. 1-60 seconds

Level: Supervisor

4.4.6.2. set auth tacacs

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

Command Syntax:

```
set auth tacacs (options)
```

Where the 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 be 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 RADIUS server timeout value. 1-60 seconds

Level: Supervisor
4.4.6.3. **set auth local**

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

Command Syntax:

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

- **minlen <n>** establishes a measure of complexity related to the password length (more in a moment on this).
  - Range: $2 < minlen < 30$

- **lcredit <n>** sets the minimum number of required lowercase letters.
  - Range: $|lcredit| < 6$

- **ucredit <n>** sets the minimum number of required uppercase letters.
  - Range: $|ucredit| < 6$

- **dcredit <n>** sets the minimum number of required digits.
  - Range: $|dcredit| < 6$

- **ocredit <n>** sets the minimum number of required other characters.
  - These characters can be any printable character, except for space.
  - Range: $|ocredit| < 6$

- **difok <yes|no>** sets 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> is:
  - p0 : require a minimum of 6 characters, no other requirements (default)
  - p1 : require at least 1 uppercase letter. The password must be at least 6 characters long.
  - p2 : require at least 1 uppercase and 2 lowercase letters. The password must be at least 6 characters long.
  - p3 : require at least 1 uppercase, 2 lowercase, and 1 number. The password must be at least 6 characters long.
  - p4 : require at least 1 uppercase, 2 lowercase, 1 number and 1 'other' character. The password must be at least 6 characters long.

'minlen' is actually 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. So let's see how this works.

The minlen complexity measure is calculated in a number of 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's 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 instance:

set auth local p1 dcredit -1

Would set the criteria to be: require at least 1 uppercase, 1 digit and a minimum length of 6 characters.

Examples include:

set auth local minlen 12
set auth local pre p2 minlen 10

4.4.6.4. set auth type

The set auth type command allows changing of 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 'help 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**: Used 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 in that it will enable all of the above.

*NOTE – Note that 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'.

Examples:

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

Level: Supervisor

### 4.4.7. **get auto**

Show the current status of the auto-logoff setting for this session. Default is to automatically log off this port after approximately 5 minutes of inactivity.

Command Syntax:

```
get auto
```

### 4.4.8. **set auto**

Control the auto-logoff setting for this session. This allows the port to remain active even beyond the 5-minute timeout period of inactivity. This is effective only for this session (not stored). Default 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
```

### 4.4.9. **config**

Use the `config` command to view, change and select Thunderbolt® PTP GMC configuration.

Command Syntax:

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

- **config list** output configuration as a list of 'set' commands
- **config load** load Thunderbolt® PTP GMC configuration previously dumped
- **config save** The "save" stores current settings for restore on restart.
- **config firmware** utilities to handle firmware updates and loading
- **config system** restart or reboot system

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

Level: Admin and Supervisor
4.4.9.1. **config firmware**

Use the `config firmware` command to maintain the firmware versions used by the Thunderbolt® PTP GMC GM200.

Command Syntax:

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

Additional help on each of the commands is available.

Level: Supervisor

4.4.9.2. **config firmware list**

Use the `config firmware` command to view the currently available firmware packages on the Thunderbolt® PTP GMC GM200.

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

4.4.9.3. **config firmware stage**

Use the `config firmware stage` command to put the firmware into system to allow updating (or rolling back) firmware versions. A maximum of 8 (the most recently released) firmware images will be stored and displayed in the list of available patches. It is suggested that the number of staged files be managed (unstaged) to keep the number of staged packages to 8 or less.

Command Syntax:

```
config firmware stage [tftp <ipaddr><fname] 
```

Where:

- `tftp` to retrieve the firmware.
  
  Note that the Thunderbolt PTP GMC GM200 is not running a tftp server. The user must have a tftp server, with the firmware desired, available to use this option.

- `<ipaddr>` The IP address of the tftp server.

- `<fname>` The filename of the update package to load from the server

- `unlock` Use this option (by itself) to unlock the staging. This may be necessary in the event that a web page has started the upload process but was abandoned before being complete.

If 'tftp' is not used, then the system will use X-Modem protocol to load the firmware.
**NOTE** – **X-Modem** is available only on serial port connections, and through telnet or SSH connections. 
**NOTE** – The firmware package can be updated through Web interface which will be familiar to users.

Examples include:

```plaintext
config firmware unlock
(unlock an abandoned staging process)

config firmware stage
(X-Modem transfer from serial port)

config firmware stage tftp 10.1.1.1 patchFile.tar.gz
(tftp transfer of 'patchFile.tar.gz' from server 10.1.1.1)
```

Level: Supervisor

### 4.4.9.4. **config firmware update**
Use the **config firmware update** command to update the firmware on the Thunderbolt® PTP GMC GM200.

Command Syntax:

```plaintext
config firmware update <id>
```

Where:

- `<id>` One of the IDs as given with the 'config firmware list' command

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

Level: Supervisor

### 4.4.9.5. **config firmware unstage**
Use the **config firmware unstage** command to remove the firmware load from the Thunderbolt® PTP GMC for use by **config firmware update** command.

Command Syntax:

```plaintext
config firmware unstage <id>
```

Where:

- `<id>` One of the IDs as given with the 'config firmware list' command

**NOTE** – After a firmware load is unstaged the `<id>` values will change so you will need to use 'config firmware list' to view the new firmware load IDs.

Level: Supervisor
4.4.9.6. **config load**

Use the `config load` command to reset Thunderbolt® PTP GMC’s configuration.

Command Syntax:

```
config load [ user / factory ]
```

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

If one of the options is given, then the appropriate settings will be 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 the all users are removed and the 'trimble' user restored

Level:  Admin and Supervisor

4.4.9.7. **config list**

Use the `config list` command to output Thunderbolt® PTP GMC’s configuration as a list of CLI commands.

Command Syntax:

```
config list
```

You can make a backup of GM200's 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.

*NOTE 1* – For security reasons, the list command and subsequent upload cannot be used to restore user settings

*NOTE 2* – The list command and subsequent upload cannot be used to restore the network settings.

*NOTE 3* - To avoid network conflicts on a subsequent load, the "config list" command does not output the current Ethernet settings.

Level:  Admin and Supervisor

4.4.9.8. **config save**

Use the `config save` command to save the current settings of the Thunderbolt® PTP GM200 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
4.4.9.9. **config system**

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

Command Syntax:

```
cfg 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 real 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 aid in debugging of issues.

Level: Supervisor

4.4.10. **get comm**

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

Command Syntax:

```
get comm
```

Level: User, Admin and Supervisor

4.4.11. **set comm**

The `set comm` command configures the communication 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>` Sets the serial port to output TOD on demand. This is used in conjunction 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>` Set a delay for the TOD output in us. This delays the TOD message for `<d>` us 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 there is currently a user logged into that port. The port baud rate will change once the user is logged out.

Examples include:

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

Level: Admin and Supervisor
4.4.12.  get date
The get date command retrieves the current system date.

Command Syntax:

   get date [full]

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

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

Level:  User, Admin and Supervisor

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

Command Syntax:

   get dlog

Level:  User, Admin and Supervisor

4.4.14.  set dlog
The set dlog command allows for starting or stopping the datalogging process.

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 Reserved, do not use.
   stop     Stop the datalogger.

Level:  User, Admin and Supervisor
4.4.15. **download**
The `download` command to download log files from the current system GM200.
Usage:

```
download [ sats | pos | freq ]
```

Options:

- **sats**: Download TEXT logfile of the satellites the receiver has been tracking over time.
- **pos**: Download TEXT logfile of position information of the receiver over time.
- **freq**: Download TEXT logfile of the oscillator statistics over time.

4.4.16. **get freq**
The `get freq` command retrieves the current operating mode of the control system.

Command Syntax:

```
get freq
```

Level: User, Admin and Supervisor

4.4.17. **set freq**
The `set freq` command sets the current operating mode of the control system. This command is only for test 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 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' and is not a mechanism to override the operation of the control system.
- **<resync>**: Command the unit to force the output PPS to align with the current reference immediately. Note that this can cause jumps in time.

Example:
**4.4.18. view freq**
The `view freq` command displays the current frequency control information. Command Syntax:

```
view freq <stream>
```

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

Level: User, Admin and Supervisor

**4.4.19. get gnss**
This command displays the current settings for the GNSS receiver

Command Syntax:

```
get gnss
```

Level: User, Admin and Supervisor

**4.4.20. set gnss**
This command allows change to 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 (dHz) 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 GM200. Negative numbers advance the internal time reference, positive numbers retard (delay) the time reference. To compensate for an antenna delay of 500ns you would enter -500 as the GM200 antenna delay setting.\( \langle d \rangle \) is in nanoseconds with a range of +/- 50000000 (50ms).

**pos \(<p>\)**

Set the receiver position or mode. Where \(<p>\) is of the format:

\{<lat> <lon> <ht>\} | auto | survey

Where:

\(<\text{lat}>\) and \(<\text{lon}>\) are in degrees and \(<\text{ht}>\) in meters (HAE).

*Note that the position will be 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 will be recomputed.*

'auto' sets the unit to not force a user entered position on startup. If the unit has a stored position then it will be used on startup, with the same validation criteria as used for a user entered position.

'survey' forces the unit to recomputed a surveyed position. The surveyed position will then be used by the system on the next startup (to speed startup). This also forces 'auto' mode.

**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 will be 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 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

### 4.4.21. *view gnss*

The **view gnss** command displays the current GNSS receiver tracking information.

**Command Syntax:**

```
view gnss
```

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

Examples include:

```
view gnss
view gnss stream
```

**Level:** User, Admin and Supervisor
4.4.22. help
The help command allows to get an overview of the GM200 (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).

Examples include:

   help intro
   help commands
   help set

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

Command Syntax:

   help howto <n> ↵

Where <n> is number 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 19200bps?
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?

Examples include:

   help howto 4

Level: User, Admin and Supervisor
4.4.24. **get input**

The **get input** command generates a list of the frequency control input candidates.

Command Syntax:

```
get input <input type>
```

Where:

- `<input type>` is 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.

Examples include:

```
get input
get input gnss
```

Level: User, Admin and Supervisor

4.4.25. **set input**

The **set input** command allows setting of the frequency control reference input candidates. You can avoid the unit going into holdover due to the loss of an input as it will be able to select from other input candidates in the event of the loss of an input.

Command Syntax:

```
set input [ <input type> ] {enable/disable}
```

Where:

- `<input type>` is from the list:
  - `GNSS*` Use the GNSS receiver as source for time/frequency
  - `syncE0*` Use the SyncE input on interface 0 as source for frequency
  - `syncE1` Use the SyncE input on interface 1 as source for frequency
  - `ptp0*` Use the PTP input on interface 0 as source. The PTP setting for interface 0 must be set to slave to be usable as an input source.
  - `ptp1` Use the PTP input on interface 1 as source. The PTP setting for interface 1 must be set to slave to be usable as an input source.
  - `enable` Enable the `<input type>`(s) as valid inputs. If no `<input type>` is given then the entries marked with `'*'` above are enabled.
  - `disable` Disable the `<input type>`(s) as usable inputs. If no `<input type>` is given then all inputs are disabled.
The order of preference of the input selection is:

GNSS
synce0
synce1
ptp0 | ptp1

**NOTE** – Only one of the synce0 and synce1 inputs can be enabled at a time. If both are enabled then synce0 is automatically disabled.

**NOTE** – Only one of the ptp0 and ptp1 inputs can be enabled at a time. If both are enabled then ptp1 is automatically disabled.

Examples include:

- `set input synce0 enable`
- `set input synce1 enable`
- `set input GNSS ptp0 enable`
- `set input enable`

The last example would enable all ‘*’ inputs as valid candidates.

Level: Admin and Supervisor

**4.4.26. view input**

The `view input` command displays 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. Examples include:

- `view input`
- `view input gnss`

Level: User, Admin and Supervisor
4.4.27. **view logs**

The **view logs** command displays the system messages. Each message displayed will include the data and time of the event as well as short description of the event itself.

Command Syntax:

```
view logs xxxx<head/tail/all> <n X>
```

Where:

When `xxxx` is following:
- `<alarm>` View only alarm log information
- `<freq>` View only Time/Frequency control log information
- `<gnss>` View only GNSS log information
- `<synce>` View only SyncE log information
- `<cfg>` View only configuration log information
- `<cli>` View only CLI log information
- `<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>` Notice log information, these are normal but, significant conditions.
- `<info>` View only informational log information. These are normal but insignificant conditions
- `<head>` View the beginning of the log (default is tail)
- `<tail>` View the end of the log (latest)
- `<n X>` View only a count of “X” from the log (default is 20)

Examples include:

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

Level: Admin and Supervisor

4.4.28. **get network**

This 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
4.4.29. **set network**

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

**Command Syntax:**

```
set network [<iface>] [default] | [disable] | [<ip>] [<ip6>] [synce <sop>]
```

**NOTE** – The default must be used by itself and restores the network settings to their default values.

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 default value. This must be used with no other setting options.

- `disable`: Completely disable this interface. This stops all activity from this interface. The interface is enabled by commanding '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.

- `<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.xxx.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, of the format:
    [vlan <vl>] [prio <p>].

Where:
<vl> Comma separated list of VLAN IDs to use as the current VLAN list. Note that 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 will delete all VLANs associated with this port. Value VLAN ID numbers are from 0-4094, with the addition of '-1' to disable VLAN entirely.

prio Set the priority byte for the VLAN to <p>, where <p> can be a number between 0 (lowest) to 7 (highest). This priority applies to all VLAN connections.

<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

Examples include:
    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::/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 eth0 synce output
    set network eth1 synce input

Level: Admin and Supervisor

4.4.30. view network

The view network command allows user to view current network interfaces stats. Command

Syntax:
    view network <eth0|eth1|eth2> ↓

If no interface name is given, then statistics for all interfaces are presented. Examples include:
    view network ↓
    view network eth1↓

Level: User, Admin and Supervisor
4.4.31. **get ntp**

The `get ntp` command allows user to display current NTP broadcast setting for eth0 or eth1 ports. If no option given then all ports are returned. If you desire to view the current NTP statistics then use 'view ntp'.

If NTP broadcast is enabled then this command will return 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 present 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). The information presented should be copied from the terminal into a file, named to the filename indicated in the information and then that file distributed, securely, to your clients. (This option is available only to supervisor level user)

Examples include

```
get ntp
```

```
get ntp eth0
```

```
get ntp iff
```

Level: User, Admin and Supervisor

4.4.32. **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 supplied then all ports are affected. This option may not be used with any other options.
- *bcast <ip>|off: Set broadcasting on/off for the port. If an `<ip>` address is given, 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 host name for the encryption certificate to <hn>. Only the characters '-', '_', 0-9, A-Z, and a-z are valid within the host name. The max size of the host name is 32 characters.

group <gn>  Set the group name for the encryption certificate to <gn>. Only the characters '-', '_', 0-9, A-Z, and a-z are valid within the group name. The max 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 4 peers to use. This list must contain no spaces and may 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 will renew the IFF certificate for NTP certification. This should be done approximately every 30 days to keep the certificate valid.

Examples include:

```
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.**

**Level:** Admin and Supervisor

### 4.4.33. **view ntp**

The `view ntp` command allows user to display current NTP stats. Command Syntax:

```
view ntp [stream]
```

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

Examples include:

```
view ntp stream
```

**Level:** User, Admin and Supervisor
4.4.34. get output

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

Command Syntax:

\[
\text{get output } [<\text{sel}>] \downarrow
\]

Where <sel> may be:

- bnc Get output settings for BNC output only

Examples include:

get output bnc
get output

Level: Admin and Supervisor

4.4.35. set output

The set output command allows setting of the output signal(s) for the system. If no output signal selection is given, 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. This affects all levels for the given signal. That means that if the output is set 'high' for instance the 'invert' option changes the output to 'low'. The “falling” modifier is an edge trigger.

\text{Note that this is a modifier and cannot be used alone.}

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

\text{Note that the 'periodic' output has its own width, set with the 'set periodic' command.}

The 'delay' option allows setting of 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 will not see any effect from this value.

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

```
set 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.

Examples include:

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

Level: Admin and Supervisor

4.4.36. **get periodic**

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

Command Syntax:

```
get periodic```

Level: User, Admin and Supervisor

4.4.37. **set periodic**

The *set periodic* command allows setting of 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 go from 0 to <p> - 1.
- **width <w>** set the pulse width for the periodic output in ns. Range is 100ns to 5E8 (1/2 second)

Examples include:

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

Level: Admin and Supervisor

4.4.38. **ping**

The *ping* command allows validation of a route to another IP system on the network.
Command Syntax:

\texttt{ping [eth0|eth1|eth2] <ipaddr>}

Where:
\begin{itemize}
\item \texttt{<eth0>} Network interface Ethernet 0
\item \texttt{<eth1>} Network interface Ethernet 1
\item \texttt{<eth2>} Network interface Ethernet 2
\item \texttt{<ipaddr>} Valid IPv4 address of the unit, in xxx.xxx.xxx.xxx format
\end{itemize}

\textit{NOTE – If no port is given then the management port is assumed. The ports may be on separate physical networks, make sure the network interface corresponding to the device pinged is used.}

Level: User, Admin and Supervisor

\textbf{4.4.39. ping6}

The \texttt{ping6} command allows validation of a route to another IP system on the network.

Command Syntax:

\texttt{ping6 [eth0|eth1|eth2] <ipaddr>}

Where:
\begin{itemize}
\item \texttt{<eth0>} Network interface Ethernet 0
\item \texttt{<eth1>} Network interface Ethernet 1
\item \texttt{<eth2>} Network interface Ethernet 2
\item \texttt{<ipaddr>} IPv6 address of the unit without any mask information
\end{itemize}

\textit{NOTE – If no port is given then the management port is assumed. The ports may be on separate physical networks, make sure the network interface corresponding to the device pinged is used.}

Level: User, Admin and Supervisor

\textbf{4.4.40. view pos}

The \texttt{view pos} displays the current receiver position information. Command

Syntax:

\texttt{view pos [stream]}

Where:
\begin{itemize}
\item \texttt{<stream>} View a continuous stream of frequency control data
\end{itemize}

Level: User, Admin and Supervisor

\textbf{4.4.41. view prodconf}

The \texttt{view prodconf} displays the production configuration information that was set by Trimble
manufacturing during production.

Command Syntax:

`view prodconf` 

Examples include:

`view prodconf` 

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

**Level:** User, Admin and Supervisor

### 4.4.42. `get ptp`

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

If you desire to view the current PTP operation then use 'view ptp'.

Command Syntax:

`get ptp <eth0 / eth1>` 

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

**Level:** User, Admin and Supervisor

### 4.4.43. `set ptp`

The `set ptp` command allows setting of the PTP interface.

Command Syntax:

`set ptp <eth0 / eth1> <options>` 

Examples include:

`set ptp <options>` 
`set ptp eth0 <options>` 

Where options are:

- **default**  
  Restore default settings for the used 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. Note that for this to be used also requires the port
is set as a selectable input with the 'set input' command.

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.
telecom:  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. Note that 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 - 1000.
        Most profiles have a default 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 3 GMs to
use. This list must contain no spaces and be made up of the same transport types (i.e.
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. May be one of:
        multi   set multicast mode
• uni set unicast mode
• hybrid set Hybrid mode; allow multicast for GM announcement, but time information 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. 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 (1-255) 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 1-6 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)

NOTE: stop the ptp first to setup up.
NOTE: selecting/changing to a different profile will set all PTP parameters to default values for the profile, this includes the PTP Operational Mode.

Examples:
  set ptp eth1 disable profile g8275 domain 30 ttl 3

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

Level: Admin and Supervisor

4.4.44. view ptp
The view ptp displays the current PTP stats. Command

Syntax:

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

Examples include:
  get ptp eth0
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 allows to have a list of all PTP slaves taking synchronization from GM-200.

Level: User, Admin and Supervisor
4.4.45. **quit**
The *quit* command is used to end a CLI session. You can use either "quit" or "q" to end the session.

Command Syntax:

```
quilt
q
```

Level: User, Admin and Supervisor

4.4.46. **view realtime**
Show/Change the current level of the messages display. This command allows changing of the realtime event message level for this session (not stored).
Default is level 1 (alarms only).

Command Syntax:

```
view realtime [<level>]
```

Where the `<level>` value means:

- 0  No events will be shown in realtime
- 1  Only alarm events will be shown in realtime (default)
- 2  All events will be shown in realtime

Examples include:

```
view realtime
view realtime 2
```

4.4.47. **help set**
The *help set* command allows users to set system parameters. Command Syntax:

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

Level: Admin and Supervisor
**4.4.48. get snmp**

The `get snmp` command 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

**4.4.49. set snmp**

The `set snmp` command allows configuring 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 & 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.

Examples include:

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

Level: Admin and Supervisor

**4.4.50. view summary**

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

The `view stream` command displays a continuous stream of system performance data. This includes frequency control data as well as GNSS tracking information.

Command Syntax:

```
view stream
```

Level: User, Admin and Supervisor

4.4.52. **get syslog**

This 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

4.4.53. **set syslog**

The `set syslog` command allows user 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. Note that until the address is configured with the address of a valid syslog server no messages will be sent, regardless of whether the service is enabled or not.
- **disable** Disable the sending of syslog messages to the syslog server. This has no effect on 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 GM, 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.

Examples include:
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

**4.4.54. get system**

This command returns the current system wide host settings for the system.

Command Syntax:

get system

**4.4.55. set system**

Configure 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 '-', '0-9', 'a-z', and 'A-Z' are valid within the host name. The min size size of the host name is 1 alpha-numeric character. The max size size of the host name is 63 characters.

- **opermode <m>**
  
  Set the operational mode for the system. <m> may be one of:
  
  - **normal**
    
    PTP will not be activated until the system is locked to the GNSS signal and the UTC correction information is available.
  
  - **freerun**
    
    the PTP protocol will be activated as soon as system has booted, but without GNSS tracking. This means that the PTP timestamps will either be started from the PTP epoch, hand-set by the user, set from an NTP server (see timesource option), or from GNSS. The frequency control will be in freerun, until GNSS tracks and locks. If GNSS tracks and locks the PTP timestamps will immediately be set to the time based on GNSS.

- **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 'none' the unit 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. In the event that the server is unavailable at system startup a sync will be 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, default of 15 minutes. <t> has the range of 1 <= t <= 120 to allow the system to attempt to acquire time from an NTP server from 1 minute to 2 hours.
Examples include:
set system hostname GM200.bdg11.flr3
set system opermode freerun ntp 192.168.2.17 ntpto 60

4.4.56. **view temp**
The *view temp* command displays the current system temperature in °C.

Command Syntax:
```
view temp 
```

Level: User, Admin and Supervisor

4.4.57. **get time**
This command retrieves the current system UTC time.

Command Syntax:
```
get time [full] 
```

If the option 'full', is given this returns both the date and time.
```
get time full 
```

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 (00-31)
- Y is the full year, including century
- hh:mm:ss is the current UTC hour, minute and second

Level: User, Admin and Supervisor

4.4.58. **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
4.4.59. **get user**

This 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

4.4.60. **set user**

The *set user* command allows changing 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 then you will be queried 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. Note that 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.
  
  Please see 'help set user logout' for information about the options.

Level: Supervisor
4.4.61. **set user logout**

The *set user logout* command allows the Thunderbolt PTP GMC GM200 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> will be logged out. This will affect all services and sessions.

<s> The session ID to log out. Users logged in with this session ID will be logged out. This limits the logout to only a single entry since session ID's are unique. The session ID can be found using the 'view user' command.

<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 will not be affected.

Examples:

```
set user logout sid 4
set user logout service 10.1.140.111
set user logout name trimble service 10.1.140.111
```

In the above examples, the first would log out a single user session. The second example logs out all users connected from a specific IP address. The third example will only log out a certain user, logged in from a specific IP address.

Level: Supervisor

4.4.62. **view user**

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

Command Syntax:

```
view user
```

Level: User, Admin and Supervisor
4.4.63. **view version**

The `view version` command displays the current versioning information for the product.

Command Syntax:

```
view version <hardware|gnss>
```

Where:

- `<hardware>` View the hardware version of the Thunderbolt PTP GMC
- `<gnss>` View only the GNSS version

Examples include:

```
view version
view version hardware
```

Level: User, Admin and Supervisor

4.4.64. **view**

The `view` command allows seeing 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

Examples include:
  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

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

Usage: view dlog gnss
Usage: view dlog pos
Usage: view dlog freq

4.4.64.2.  view gnss stream
View the current GNSS receiver tracking information as a continuous streaming output. The streaming may be stopped by pressing one of the following keys on your terminal:
  ctrl-C, 'q', 'Q', 'x' or 'X.

4.4.65.   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 is an indication of an out-of-date FPGA load. This can be remedied by a supervisor level person applying a hardware update load to the system. The supervisor can refer to the 'config firmware' section for more information.

    2) 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 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 an admin can change the PTP operation on that port to disable the PTP operation, which will clear the alarm.

Level:    User, Admin and Supervisor
4.5. List of “How to” help topics

The howto command provide a list of frequently used task and help on the related CLI options.

The list of frequently used tasks is the following:

1. How to get current Alarm status
2. How to set alarm of level major, 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 19200bps?
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?

Command format:

```
help howto <n>
```

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

For example,

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

    get alarm

4.5.2. How to set alarm of level major, alarm number 2 with setTime as 2 and clearTime as 1?

    NOTE: This is only possible from an admin (or higher) access level

    set alarm 2 maj 2 1

4.5.3. How to disable Ethernet port 0/1?

    NOTE: This is only possible from an admin (or higher) access level

    set network eth0 disable
    set network eth1 disable
4.5.4. **How to set ip address of 192.168.0.9, and also set a netmask and a gateway address on ethernet 0 port?**

*NOTE: This is only possible from an admin (or higher) access level*

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

4.5.5. **How to set bnc output to even?**

*NOTE: This is only possible from an admin (or higher) access level*

```
set output bnc even
```

4.5.6. **How to set periodic output of period 2 and value 1?**

*NOTE: This is only possible from an admin (or higher) access level*

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

4.5.7. **How to set serial port baud rate to 19200bps?**

*NOTE: This is only possible from an admin (or higher) access level*

```
set comm baud 19200
```

4.5.8. **How to add a new user called trimble1 with an access level of user?**

*NOTE: This is only possible from a supervisor access level*

```
set user adduser trimble1 user
```

4.5.9. **How to delete an existing user trimble?**

*NOTE: This is only possible from a supervisor access level*

```
set user deluser trimble
```

4.5.10. **How to change user password?**

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

4.5.11. **How to restore factory default settings?**

*NOTE: This is only available from an admin (or higher) access level*

```
config load factory
```

4.5.12. **How to reboot the system?**

*NOTE: This is only available from a supervisor access level*

```
config system reboot
```
4.6. List of “What if” help topics

This section gives some information about some scenarios, you may encounter and how to recover from those.

4.6.1. 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 refer to the 'config firmware' section for more information.

4.6.2. 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 'get network' 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.
5 Web Interface

In this chapter:
- Configuration Pages
- Status Pages

This chapter provides explanation on the web interface of Thunderbolt® PTP Grandmaster Clock.
5.1 Home Page
Launch a web browser and open a connection to Thunderbolt® PTP Grandmaster Clock GM-200 by entering 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** – Trimble recommends using Google Chrome browser for better rendering of Thunderbolt® PTP Grandmaster Clock GM-200 web pages.

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

The main page will display a brief status of the Thunderbolt® PTP GMC. The components of this page are:

- **Alarm Status**: Shows the list of active alarms
- **Input Status**: Shows the input reference of GM200
- **Configuration Status**: Shows the status of the current configuration saved
- **Product ID**: Shows the Trimble part number of GM200
- **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/SyncE Ethernet Port 0
- **Ethernet Port 1 Status**  
  Displays the status of PTP/NTP/SyncE Ethernet Port 1

Log in to the Thunderbolt® PTP GMC GM200 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 1 second.
5.2 Login Page

Use the Thunderbolt® PTP GMC GM200 Login page to view system status. The login page requires a valid username and password.

NOTE – There is a change in default password to comply with California State Bill SB-327. The SB-327 Information privacy: connected devices bill requires that the pre-programmed password is unique to each device manufactured.

The SB-327 will become effective on January 1, 2020.
Trimble has removed the trimble/trimble user/password as the initial default login.

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.
5.3 How to Edit a Configuration Page

All configuration pages have 3 icons on the top right of the configuration area. Numbered from left to right they are:

1) Enable System Configuration – put the screen in edit mode. Editable fields and pull down items will change from greyed to highlighted.
2) Set – Sets the configuration. You will need to SAVE the configuration in a separate step.
3) Exit – Returns the screen to read only mode.

Example: Alarm Configuration – Read Only

Example: Alarm Configuration – Edit Mode

4) To save the configuration. Click on the Save System Configuration icon.

Click on the confirmation box to save the system configuration.

10.1.141.1 says
Commit system configuration?

Please confirm.

OK Cancel
5.4 System Page

After entering the valid credentials, the Thunderbolt® PTP Grandmaster Clock GM-200 launches the System Page. The system page is organized in two frames – the navigation and content.

The start page gives general status information of the Thunderbolt® PTP Grandmaster Clock GM-200. By using the navigation menu on the left side of the screen, user can view a number of configuration pages which are described in following pages.
5.5 System Status

Alarms and Events - Alarms

The page shows currently active alarm condition on the system.

The Alarm Description window provides the details of each alarm and the alarm level

- **Alarm #:** Alarm code
- **Alarm Description:** Description of the alarm condition
- **Alarm Level:** Severity of alarm condition, can be notification only, minor, major or critical
Alarms and Events – Event Log

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

- **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.
**System Info**

The System Info status provides overall system information:

- **Product ID or Model:** The model number of the Thunderbolt® PTP GMC.
- **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 Thunderbolt® PTP GMC.
- **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 GM200.
- **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 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 realtime graph of the following values:
  - CPU Load
  - Temperature
  - Mem – Active
• Mem - Available
**Timing Status**

This page provides the status information of System clock

- **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 GM200
  - Holdover: The estimated holdover time available
NTP Status

- **Ethernet Port:** Identifies the Ethernet port – Eth0 or Eth1
- **NTP Status:** Show the status of port connection
- **NTP Time Server Statistics:** Shows the statistics of various server parameters
- **Ethernet Port:** Identifies the Ethernet port – Eth0 (RJ45) or Eth1 (SFP)
- **PTP Status:** Show 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 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.
- **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)
**GNSS Receiver Status**

The page displays the status of GNSS receiver:

- **Latitude:** The latitude of the Thunderbolt PTP GMC GM200
- **Longitude:** The longitude of the Thunderbolt PTP GMC GM200
- **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 GNSS Almanac
- **Constellations in use:** Current constellations that are being used
- **GNSS Quality Status:** A metric used to provide the user with a snapshot of the number of SVs with Very Good, Good, or Poor Signal Strength/Quality.
  - 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 not SVs that have SNR > 20
- **Antenna Delay:** Displays the compensation delay of antenna cable.

The antenna delay setting affects the system time base of GM200. Negative numbers advance the internal time reference, positive numbers retard (delay) the time reference. To compensate for an antenna delay of 500ns you would enter -500 as the GM200 antenna delay setting.<d> is in nanoseconds with a range of +/- 50000000 (50ms).

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 GM200, 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 GM200 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.
### Satellite Data

- **SV:** Satellite Vehicle
- **C/No:** Carrier-to-Noise power ratio
- **Az:** Azimuth
- **Elev:** Elevation

<table>
<thead>
<tr>
<th>SV</th>
<th>C/No</th>
<th>Az</th>
<th>Elev</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>45.0</td>
<td>191.0</td>
<td>38.0</td>
</tr>
<tr>
<td>9</td>
<td>48.0</td>
<td>279.0</td>
<td>32.0</td>
</tr>
<tr>
<td>10</td>
<td>47.0</td>
<td>150.0</td>
<td>60.0</td>
</tr>
<tr>
<td>1</td>
<td>44.0</td>
<td>44.0</td>
<td>22.0</td>
</tr>
<tr>
<td>17</td>
<td>50.0</td>
<td>321.0</td>
<td>59.0</td>
</tr>
<tr>
<td>7</td>
<td>48.0</td>
<td>148.0</td>
<td>33.0</td>
</tr>
<tr>
<td>3</td>
<td>47.0</td>
<td>271.0</td>
<td>25.0</td>
</tr>
<tr>
<td>28</td>
<td>43.0</td>
<td>25.0</td>
<td>45.0</td>
</tr>
<tr>
<td>76</td>
<td>31.0</td>
<td>379.0</td>
<td>25.0</td>
</tr>
<tr>
<td>87</td>
<td>44.0</td>
<td>221.0</td>
<td>16.0</td>
</tr>
<tr>
<td>75</td>
<td>45.0</td>
<td>29.0</td>
<td>62.0</td>
</tr>
<tr>
<td>74</td>
<td>47.0</td>
<td>119.0</td>
<td>37.0</td>
</tr>
<tr>
<td>85</td>
<td>42.0</td>
<td>15.0</td>
<td>40.0</td>
</tr>
<tr>
<td>86</td>
<td>48.0</td>
<td>265.0</td>
<td>67.0</td>
</tr>
</tbody>
</table>
Network eth0

- IPv4 Address: 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
- **IPv4 Address:** 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
**Network Management Port**

- **IPv4 Address:** 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
## Ethernet Statistics

### Ethernet Statistics Table

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Ethernet Port 0</th>
<th>Ethernet Port 1</th>
<th>Management Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Bytes</td>
<td>N/A</td>
<td>N/A</td>
<td>15 MB</td>
</tr>
<tr>
<td>RX Packets</td>
<td>N/A</td>
<td>N/A</td>
<td>39331</td>
</tr>
<tr>
<td>RX Packets/Sec</td>
<td>N/A</td>
<td>N/A</td>
<td>2</td>
</tr>
<tr>
<td>RX Dropped</td>
<td>N/A</td>
<td>N/A</td>
<td>3</td>
</tr>
<tr>
<td>RX Errors</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
</tr>
<tr>
<td>TX Bytes</td>
<td>N/A</td>
<td>N/A</td>
<td>34 MB</td>
</tr>
<tr>
<td>TX Packets</td>
<td>N/A</td>
<td>N/A</td>
<td>67666</td>
</tr>
<tr>
<td>TX Packets/Sec</td>
<td>N/A</td>
<td>N/A</td>
<td>3</td>
</tr>
<tr>
<td>TX Dropped</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
</tr>
<tr>
<td>TX Errors</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
</tr>
<tr>
<td>RX+TX Pkts/Sec</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1-second 10-seconds avg
## 5.6 Interface Management

**Ethernet Port 0**

<table>
<thead>
<tr>
<th>Port Configuration</th>
<th>Connection Status</th>
<th>SyncE Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Either DHCP, Static, Default or Disable this interface</td>
<td>Either Connected, Not Connected</td>
<td>Either Output, Input, Off</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv4 Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address: 192.168.3.250</td>
</tr>
<tr>
<td>Subnet Mask: 255.255.255.0</td>
</tr>
<tr>
<td>Gateway:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: DHCPv6</td>
</tr>
<tr>
<td>Address:</td>
</tr>
<tr>
<td>Gateway:</td>
</tr>
</tbody>
</table>

| IPv4 Address: Enter IPv4 Address to test ping |
| Ping IPv4 |
| IPv6 Address: Enter IPv6 Address to test ping |
| Ping IPv6 |

- **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**: Either DHCPv6, SLAAC, 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
- **Port Configuration**: Either DHCP, Static, Default or Disable this interface
- **Connection Status**: Either Connected, Not Connected
- **SyncE Configuration**: Either Output, Input, 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**: Either DHCPv6, SLAAC, 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
- **Port Configuration:** Either DHCP, Static, Default or Disable this interface
- **Connection Status:** Either Connected, 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:** Either DHCPv6, SLAAC, Static
- **IPv6 Address:** IPv6 Address of the Ethernet interface with the subnet mask.
- **IPv6 Gateway:** IPv6 gateway address for the port.
- **Ping IPv4:** Enter IPv4 Address to test ping
- **Ping IPv6:** Enter IPv6 Address to test ping
- **VLAN IDs:** List of all VLAN IDs configured
- **Priority:** 0 to 7 where 7 is the highest priority
- **NOTE:** There is a limit of 4 VLANs per port
- **VLAN IDs:** List of all VLAN IDs configured
- **Priority:** 0 to 7 where 7 is the highest priority
- **NOTE:** There is a limit of 4 VLANs per port
- **SNMP Configuration**: Enable or Disable
- **Download MIBs**: This option allows download SNMP MIB files
- **SNMP Agent Version**: SNMP v2c, SNMPv3,
- **Read Community**: Community string for read
- **Write Community**: Community string for write
SNMP Configuration 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.
- **Trap Community String**: Community string id for SNMP
- **SNMP Manager IP**: IP address of SNMP manager that receives the TRAP
- **SNMP Manager Port**: Port number of SNMP manager
- **Syslog Protocol**: Enable or Disable
- **Syslog Server**: IP Address of Syslog Server
- **Syslog Port**: Enter Syslog Port
- **Baud Rate:** Serial port speed: 9600, 19200, 38400, 57600, 115200. The default value is 115200
- **Parity:** Serial port parity setting – even, none, 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 in conjunction 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
- **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 are not user configurable.*
5.7 Synchronization Management

PTP Grandmaster Ethernet Port 0

PTP Configuration

- **PTP Port Status:** PTP port status - enabled or disabled
- **PTP Profile:** G8275, G8265, G8265 –I, telecom or 1588
- **Sync Mode:** 1-step or 2-Step
- **Transport Protocol:** Transport mechanism – IP or Ethernet
- **IP Mode:** Multicast or Unicast
- **Delay Mechanism:** E2E or P2P
- **PTP Mode:** Master or Slave clock.

*Note before the PTP grantor is assigned an IPv6 address, the user 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 between successive announce
- **Sync Interval:** Mean time interval between successive sync messages
- **Delay Request Interval:** Mean time interval between delay requests
- **P2P Delay Req 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.

- **PTP Clock Id:** ID of the PTP clock

- **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**

Normal or Freerun. This feature is configured through the System Management, System Configuration tab. 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 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.
PTP Grandmaster Ethernet Port 1

PTP Configuration

- **PTP Port Status:** PTP port status - enabled or disabled
- **PTP Profile:** G8275, G8265, G8265 –I, telecom or 1588
- **Sync Mode:** 1-step or 2-Step
- **Transport Protocol:** Transport mechanism – IP or Ethernet
- **IP Mode:** Multicast or Unicast
- **Delay Mechanism:** E2E or P2P
- **PTP Mode:** Master or Slave clock.

**Note before the PTP grantor is assigned an IPv6 address, the user 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 between successive announce
- **Sync Interval:** Mean time interval between successive sync messages
- **Delay Request Interval:** Mean time interval between delay requests
- **P2P Delay Req 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.
PTP Clock Id: ID of the PTP clock
- 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 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 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.
- **NTP Server:** Enabled, disabled or default.
- **NTP Broadcast:** Enabled or disabled
- **NTP Broadcast IP:** Broadcast IP for NTP (has to be in same domain as that of port)
- **NTP Broadcast Interval:** Values between 4 and 17 representing $2^4(16$ secs) and $2^{17}(36.4$ hours)
- **NTP Broadcast TTL:** Values between 1 to 7 hops.
- **NTP Server**: Enabled, disabled or default.
- **NTP Broadcast**: Enabled or disabled.
- **NTP Broadcast IP**: Broadcast IP for NTP (has to be in same domain as that of port).
- **NTP Broadcast Interval**: Values between 4 and 17 representing $2^4(16\text{ secs})$ and $2^{17}(36.4\text{ hours})$.
- **NTP Broadcast TTL**: Values between 1 to 7 hops.
NTP Time Server NTP security

- **NTP Encryption**: Disabled or Enabled
- **NTP Encryption Hostname**: Hostname of encryption certificate
- **NTP Encryption Group**: Group name for encryption certificate
NTP Time Server - NTP Peers

- **NTP Peers**: IP Addresses for up to 4 NTP Peers, valid for Port0 and Port1.
- **GNSS Constellations:** Combination of GPS, GLONASS, Beidou, Galileo and/or QZSS
- **Positioning Mode:** Automatic, Surveyed or Manual
- **Latitude:** Latitude in degrees
- **Longitude:** Longitude in degrees
- **Height:** Height in meters
- **Elevation Mask:** Satellite elevation mask level
- **PDOP Mask:** Satellite PDOP mask level
- **Signal Level Mask:** Set signal level mask
- **Antenna Delay (ns):** The antenna delay setting affects the **system time base** of the GM200. Negative numbers advance the internal time reference, positive numbers retard (delay) the time reference. So, to compensate for an antenna delay of 500ns you would enter -500 as the GM200 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 GM200, 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 GM200 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
This page displays the list of Sync Sources or Inputs of the system. It is possible to select or deselect the possible Inputs of the system:

- GNSS
- PTP-eth0
- PTP-eth1
- SyncE-eth0
- SyncE-eth1

The list displays as well the selected Sync Source actually used by GM-200.
**Output Configuration**

- **BNC Output:** The type of output signal – PPS, PP2S, Periodic or 10MHz
- **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 shall NOT be used for compensating the antenna delay!
- **Periodic Width:** Periodic width in ns
- **Period:** Period in seconds
- **Periodic Value:** Periodic value
5.8 Security Management

User Management - Active Sessions

- **Name:** Existing username
- **Email:** Updated email
- **Service:** IP Address used to connect to
- **Active:** The time that the session has been active
User Management - User 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, 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.
- **Email**: New email
- **User Account Selection**: This is a list of all users created in GM200
User Management – Password Rules

- **Preconfigured password criteria:** 5 criteria of password already configured
  - None: the password doesn’t require any rule to be accepted by GM200
  - p0: 6 characters as minimum (complexity = 6)
  - p1: 7 characters as minimum, 1 uppercase letter as minimum (complexity = 8)
  - p2: 9 characters as minimum, 1 uppercase letter as minimum
    2 lowercase letter as minimum (complexity = 12)
  - p3: 10 characters as minimum, 1 uppercase letter as minimum
    2 lowercase letter as minimum, 1 digit as minimum (complexity = 14)
  - p4: 11 characters as minimum, 1 uppercase letter as minimum
    2 lowercase letter as minimum, 1 digit as minimum, 1 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.
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 GM200.
- **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. 1-60 seconds.
- **Secret:** Sets the shared secret value for the RADIUS server.
- **RADIUS Dictionary**
- **Set Defaults Button:** Sets the RADIUS server information to defaults.
Authentication TACACS+

- **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. 1-60 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 RADIUS server
- **Set Defaults Button:** Sets the TACACS+ server information to defaults.
**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 certificates valid 'From' and 'To' date range is displayed.
5.9 System Management

**Alarm**

- **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 alarm condition is inactive before it is cleared

The table shows the list of available alarms along with their current level, set and clear time.
The table allows changing the severity level, the set and clear time.
System Configuration

This tab allows Users to Configure System with following options:

- **System Hostname**: Enter hostname
- **System Mode**: Allows changing the system operating mode for Freerun or Normal. See the description in the Synchronization Management 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 file selected in ‘Choose File’ button.
- **Download Conf File**: Download a user configuration file that can later be uploaded through "Upload Config File".
- **Load Factory Config**: To set factory configuration. This restores settings to those configured during Trimble production.
- **System Reboot**: Reboot the system.
**System Software Upload**

This page displays the Current System version running on Thunderbolt PTP GM200 alone with the current GNSS version and current FPGA version. This page allows users to upload the Thunderbolt PTP GM200 firmware package to the system.

The uploading of the package doesn’t automatically update the system firmware. Another step to “Update System” is required.

A maximum of 8 (the most recently released) firmware images will be stored and displayed in the list of available patches. It is suggested that the number of staged files be managed (unstaged) to keep the number of staged packages to 8 or less.

*NOTE* – *The software upload tab is available when logged with super user level access.*
6 SNMP Support

In this chapter:

- SNMP Overview
- SNMP Traps & MIB

This chapter describes the SNMP and SNMP notification setting procedure for Thunderbolt PTP Grandmaster Clock GM200.
### 6.1 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 which runs on managed devices
- Network management station (NMS) — software which 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).

Thunderbolt PTP GMC supports SNMP v2c.

### 6.2 SNMP Traps

SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

Thunderbolt PTP Grandmaster Clock GM-200 provides a command line interface to enable the traps. (Refer to 4 CLI Reference)

### 6.3 Accessing the SNMP MIB Files

Thunderbolt PTP Grandmaster Clock GM-200’s private MIB files can be downloaded through the WebUI of the system. The MIB download option is available under the “Interface Management” tab of the unit.

The Thunderbolt PTP Grandmaster Clock GM-200’s SNMP MIB consist of two files:

- TRIMBLE-MIB.mib
- TRIMBLE-TBOLT2-MIB.mib
7 PTP Input

In this chapter:

PTP Input Overview

How it works

Configuring with CLI commands

Configuring with Web Interface

Procedure to configure PTP Input

Trimble GNSS receivers are used to deliver timing references accurate to ±15ns. 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, GNSS is complemented by network-based timing distribution to maintain the time base during GNSS reference failure.
7.1 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. It is always exposed outside the building, in order to have the best line-of-sight to multiple satellites. The consequence is that it is always subject to lighting strikes, interference due to weather conditions, reflections, and jamming, etc.

Thunderbolt PTP Grandmaster Clock GM-200 has the best holdover in the market, however, in order to provide even more protection and trying to keep longer time accuracy, Thunderbolt PTP Grandmaster Clock GM-200 also has a feature called PTP Input that is a network-based timing distribution backup reference.

The Thunderbolt PTP Grandmaster Clock GM-200 will continue utilizing GNSS as the primary time reference. PTP Input will work as a complement that will help and maintain the time when GNSS reference is not available.

PTP Input feature is then a secondary reference and will be active if GNSS tracking is lost. GM-200 will never work as a Boundary Clock because the GM-200 has superior holdover specifications to a network device due to excellent oscillator specifications.

7.2 How it works

PTP Input is designed as a secondary (backup) reference of GNSS reference of PTP Grandmaster Clock GM-200. It can be configured in Ethernet port 0 or 1. It will be an additional input for the PTP Grandmaster Clock GM-200. The Ethernet port will be configured as a PTP slave for GM-200.

Since the Ethernet port will be configured as PTP slave then it will require a grandmaster reference or ‘grantor’. GM200’s PTP Input supports up to 3 (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.
7.3 Configuring with CLI commands.

PTP Input is related to the following CLI commands: (please don’t forget that you need to first configure the network interface (IP addresses and/or VLAN IDs) in order to use any Ethernet port:

In order to do any ptp configuration change, it is required to disable ptp service in Ethernet port. This commands allows to disable/enable ptp service:

```
set ptp eth0/1 enable/disable
```

Command set ptp allows to do changes in PTP configuration. In this case, the command will change the profile required, the mode from grandmaster to slave and to add at least one grantor:

```
set ptp eth0/1 profile yyyyyyy mode slave grantor x.x.x.x
```

x.x.x.x is an IP address

yyyy is one of the following options:

- g8265 - Profile G.8265.1 Option II (clock class 80)
- g8265-l - Profile G.8265.1 Option I (clock class 84)
- telecom - Profile IEEE-1588 Telecom Profile v2 (unicast)

This command allows to configure port Ethernet 0 or 1 into PTP input:

```
set input ptp1/0 enable
```

This command allows to see all inputs/references of GM-200 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)
```

This command allows to see PTP configuration in Ethernet ports (for verification purposes). If you need to use this command after doing any change in PTP configuration, please at least 15 seconds before seeing the changes done:

```
get ptp eth0/1
```
7.4 Configuring with Web Interface.

**Configuring Ethernet Port as input.**

Ethernet port needs to be configured as input in order to be used as PTP input.

- Open web page using http or https
- Login with proper credentials (admin or super user)
- Click on “SYNCHRONIZATION MANAGEMENT” and then on “Sync Source”

- In order to do changes, it is required to click on “Configure” icon.

The web page will be grayed and it will be possible to select SyncE-eth0 or SyncE-eth1 or PTP-eth0 or PTP-eth1 Inputs.

- Click on PTP-eth0 or PTP-eth1.
- Click on “Set” icon in order to apply the changes

- There will be a green message of confirmation “Sync Source configuration successful” and a new line on the Sync Source Statistics will appear.
**PTP protocol configuration (slave mode)**

- Open web page using http or https
- Login with proper credentials (admin or super user)
- Click on “SYNCHRONIZATION MANAGEMENT” and then on “PTP”
- Select the Ethernet port tab that will be used as PTP Input

- Configure the profile, the PTP Mode as slave, the Grantor address (es) and the possible changes on Sync and Delay Request Intervals.
- In order to save changes, it is required to click on “Configure” icon and in order to apply the changes, it is required to click on “Save System Configuration” icon.
**View PTP configuration.**
- Open web page using http or https
- Login with proper credentials (admin or super user)
- Click on “SYNCHRONIZATION MANAGEMENT” and then on “PTP”

---

**View the list of Sync Sources.**
- Open web page using http or https
- Login with proper credentials (admin or super user)
- Click on “SYSTEM STATUS” and then on “Timing”
7.5 Procedure to configure PTP Input

In order to provide configuration steps, some examples will be used.

**Example 1:**
Let’s assume 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 reference of GM-200) with IP addresses 10.173.230.225 and 10.75.134.224. It will be used IEEE-1588 Telecom Profile v2 (unicast). The sequence of commands is:

- set ptp eth0 disable
- set ptp eth0 profile telecom mode slave grantor 10.173.230.225,10.75.134.224
- set ptp eth0 enable
- get ptp eth0
- set input ptp0 enable
- view input ptp0

**Example 2:**
Let’s assume 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 GM-200) with IP addresses 10.73.130.251. It will be used G.8265.1 Option I Profile. The sequence of commands is:

- set ptp eth1 disable
- set ptp eth1 profile telecom mode slave grantor 10.73.130.251
- set ptp eth1 enable
- get ptp eth1
- set input ptp1 enable
- view input ptp1
8 VLANs

In this chapter:

VLAN Overview

Configuring with CLI commands

Configuring with Web Interface

Configuring one VLAN ID

Adding another VLAN ID

Procedure to remove all VLAN IDs

This chapter describes the VLAN setting procedure for Thunderbolt PTP Grandmaster clock GM200.

NOTE: THE GM-200 SUPPORTS UP TO 4 VLANs ON EACH PORT IN TOTAL 8 VLAN.
8.1 VLANs Overview

Thunderbolt PTP Grandmaster Clock GM-200 supports up to 4 VLANs on each port in total 8 VLAN. Each VLAN must have its own address and subnet. There is no default VLAN configuration. These VLANs can be configured with a default gateway. All VLANs configuration can be deleted with a CLI command “set network eth0/1 vlan -1”.

8.2 Configuring VLAN support with CLI commands

set network eth0/1 vlan ID1,ID2,...
   This command allows to add up to 4 different VLAN IDs for each Ethernet port.

set network eth0/1.ID addr x.x.x.x mask y.y.y.y gateway z.z.z.z
   This command allows to configure IP address, subnet mask and gateway address for each VLAN ID

set network eth0/1 vlan -1
   This command allows to disable VLAN on the Ethernet port selected.
   Please use the special ID of ‘-1’.

get network eth0/1
   This command allows to show Ethernet port configuration including VLAN configuration on the Ethernet port selected.

**NOTE:** When changes are applied to any Ethernet port, it takes up to 30 seconds to see changes in Ethernet port configuration.

8.3 Configuring VLAN with Web Interface

Connect to GM-200 using web interface using https. Then login with a proper username with correct privileges like admin or super access level.
Then click on “INTERFACE MANAGEMENT” and then click on “VLAN”.

![Web Interface Screenshot]

*Trimble. Transforming the way the world works*
In order to save changes, it is required to click on “Configure” icon and in order to apply the changes, it is required to click on “Set” icon.

*Note – VLAN IDs 1 and 2 are reserved, you cannot use them.*  
It is required to add the VLAN ID, Priority (0 is the highest priority), the IP address and subnet mask.
8.4 Configuring one VLAN ID

In order to provide configuration steps, some examples will be used.

**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:

- Login with username with admin or super level.
- Disable NTP and PTP services in order to configure any VLAN ID
  
  ```
  set ptp eth0 disable
  set ntp eth0 disable
  ```
- Type
  ```
  set network eth0 vlan 452
  ```
- Press Enter
- Type
  ```
  ```
- Press Enter
- Type
  ```
  get network eth0
  ```
- Console output is below
  ```
  >
  >
  > 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
  >
  >
  ```
- It is now possible to enable again NTP or PTP service
  ```
  set ptp eth0 enable
  set ntp eth0 enable
  ```

*Note – VLAN IDs 1 and 2 are reserved, you cannot use them.*
8.5 Adding another VLAN ID

In order to provide configuration steps, some examples will be used.

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

- Login with username with admin or super level.
- Disable NTP and PTP services in order to configure any VLAN ID
  
```plaintext
  set ptp eth1 disable
  set ntp eth1 disable
```
- Type
  
```plaintext
  get network eth1
```
- Press Enter
- Console output is below

```plaintext
  >
  > 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
  >
  >
```
  ```
- Type
  
  ```
  set network eth1 vlan 333,444
  ```

- Press Enter

- Type
  
  ```
  get network eth1
  ```

- Press Enter

- Console output is below

  ```
  >
  > 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
  ```

  >

- Type
  
  ```
  set network eth1.444 addr 11.34.99.20 mask 255.255.255.248 gateway 11.34.99.15
  ```

- Press Enter

- Type
  
  ```
  get network eth1
  ```

- Press Enter

- Console output is below

  ```
  >
  > 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'

- It is now possible to enable again NTP or PTP service
  set ptp eth1 enable
  set ntp eth1 enable

8.6 Procedure to remove all VLAN IDs
The command is used to disable all VLAN configuration on a specific Ethernet port:
  set network eth0/1 vlan -1
Appendix A: SNMP Traps

In this appendix:

SNMP Traps

This appendix lists the available alarms through SNMP trap in Thunderbolt® PTP Grandmaster Clock.
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.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

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.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

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.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

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.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

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.tblt2EvNfyObject.tblt2EvNfyAlDescr.0

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.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Description: Set alarm 3, GNSS-Ant-Shorted (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 3, GNSS-Ant-Shorted (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 4, GNSS-Ant-Open (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 4, GNSS-Ant-Open (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 5, GNSS-Track-No (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 5, GNSS-Track-No (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm
Description: Set alarm 6, PTP-PPS-Loss (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 6, PTP-PPS-Loss (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 7, GNSS-PPS-Loss (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 7, GNSS-PPS-Loss (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 8, Time-Sync-Bad (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 8, Time-Sync-Bad (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm
Description: Set alarm 9, Freq-Range-Bad (CRI)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 9, Freq-Range-Bad (CRI)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 11, GNSS-Time-Bad (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 11, GNSS-Time-Bad (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 12, Freq-Loop-Unlock (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 12, Freq-Loop-Unlock (MIN)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
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

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

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

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

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

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
Description: Set alarm 16, PTP-System-Bad (CRI)
 trapsoid
Description: Clear alarm 16, PTP-System-Bad (CRI)
 trapsoid
Description: Set alarm 17, FPGA-Load-Bad (CRI)
 trapsoid
Description: Clear alarm 17, FPGA-Load-Bad (CRI)
 trapsoid
Description: Set alarm 18, GNSS-Pos-Integrity (MIN)
 trapsoid
Description: Clear alarm 18, GNSS-Pos-Integrity (MIN)
 trapsoid
Description: Clear alarm 19, UTC-Corr-Unk (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 19, UTC-Corr-Unk (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 20, Eth-Port0-Down (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 20, Eth-Port0-Down (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Clear alarm 21, Eth-Port1-Down (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm

Description: Set alarm 21, Eth-Port1-Down (MAJ)
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyObject.tblt2EvNfyAlDescr.0
Trap OID:
1.trimble.trimbleTiming.trimbleTBlt2.tblt2Events.tblt2EvNotifications.tblt2EvNfyPrefix.tblt2EvNfyAlarm
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

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

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

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

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

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
Description: Set alarm 25, SyncE1-Unsupported (CRI)
.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-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

Description: Clear alarm 25, SyncE1-Unsupported (CRI)
.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-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

Description: Set alarm 26, Time-Set-Bad (CRI)
.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-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

Description: Clear alarm 26, Time-Set-Bad (CRI)
.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-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
Appendix B: Alarms

In this appendix:

List of alarms
This appendix lists the available alarms in Thunderbolt® PTP Grandmaster Clock

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Alarm Desc</th>
<th>Level</th>
<th>Set Time</th>
<th>Clear Time</th>
<th>Description</th>
<th>How to resolve</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GNSS-Comm-E1</td>
<td>CRI</td>
<td>0</td>
<td>0</td>
<td>An internal GNSS communication alarm that indicates that the system is unable to process character from the GNSS receiver as fast as it is being generated. This alarm should never be present and is used as a BIST (build-in self-test) indication of a hardware failure.</td>
<td>Call Trimble Technical Support</td>
</tr>
<tr>
<td>1</td>
<td>GNSS-Comm-E2</td>
<td>CRI</td>
<td>0</td>
<td>0</td>
<td>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 (build-in self-test) indication of a hardware issue. This may be caused by excessive processing load on the system (denial of service attack).</td>
<td>Call Trimble Technical Support</td>
</tr>
<tr>
<td>2</td>
<td>GNSS-Comm-Loss</td>
<td>CRI</td>
<td>2</td>
<td>5</td>
<td>An indication that 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.</td>
<td>Call Trimble Technical Support</td>
</tr>
<tr>
<td>3</td>
<td>GNSS-Ant-Shorted</td>
<td>MIN</td>
<td>0</td>
<td>2</td>
<td>An indication of an overcurrent indication on the antenna feed. This is an indication that the unit may not be able to acquire satellites as the antenna may be damaged. The condition should be remedied before continuing operation.</td>
<td>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.</td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>-----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>GNSS-Ant-Open</td>
<td>MIN</td>
<td>0</td>
<td>2</td>
<td>An indication of an undercurrent indication 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.</td>
<td>Verify that the antenna and antenna cable are securely fastened. If they are, replace antenna.</td>
</tr>
<tr>
<td>5</td>
<td>GNSS-Track-No</td>
<td>MIN</td>
<td>0</td>
<td>2</td>
<td>An indication that the system is unable to track any satellites at this time. This may be a 'normal' condition 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.</td>
<td>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.</td>
</tr>
<tr>
<td>6</td>
<td>PTP-PPS-Loss</td>
<td>MIN</td>
<td>0</td>
<td>10</td>
<td>An indication that the system is unable to detect the 1PPS signal from the PTP input.</td>
<td>If the alarm persists for longer than 60 minutes, call Trimble Technical Support</td>
</tr>
<tr>
<td>7</td>
<td>GNSS-PPS-Loss</td>
<td>MIN</td>
<td>0</td>
<td>10</td>
<td>An indication that 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.</td>
<td>If the alarm persists for longer than 60 minutes, call Trimble Technical Support</td>
</tr>
<tr>
<td>8</td>
<td>Time-Sync-Bad</td>
<td>MAJ</td>
<td>2</td>
<td>10</td>
<td>An indication that the phase relationship for the PTP vs the time/frequency control is out of specification. This occurs during startup, while the</td>
<td>If the alarm persists for longer than 60 minutes, call Trimble Technical Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Freq-Range-Bad</td>
<td>CRI</td>
<td>0</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>GNSS-Time-Bad</td>
<td>MIN</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Freq-Loop-Unlock</td>
<td>MIN</td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Freq-Hold-Exceed</td>
<td>MAJ</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **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.

- **Freq-Range-Bad**
  - if the alarm persists for longer than 60 minutes, call Trimble Technical Support

- **GNSS-Time-Bad**
  - if the alarm persists for longer than 60 minutes, call Trimble Technical Support

- **Freq-Loop-Unlock**
  - if the alarm persists for longer than 60 minutes, call Trimble Technical Support

- **Freq-Hold-Exceed**
  - if the alarm persists for longer than 60 minutes, call Trimble Technical Support

- **Freq-Range-Bad** is 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.

- **GNSS-Time-Bad** indicates that 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.

- **Freq-Loop-Unlock** is an indication that 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.

- **Freq-Hold-Exceed** is set when 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.
<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>PPS-Sync-Bad</td>
<td>MAJ</td>
<td>5</td>
<td>10</td>
<td>is set when the PPS output (timing) from the system will not meet specification. This may occur during extreme environmental changes and should clear when the system becomes stable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Freq-Out-Bad</td>
<td>MAJ</td>
<td>0</td>
<td>10</td>
<td>is set when 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>PTP-System-Bad</td>
<td>CRI</td>
<td>5</td>
<td>10</td>
<td>is set when 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>FPGA-Load-Bad</td>
<td>CRI</td>
<td>0</td>
<td>0</td>
<td>is set if the FPGA hardware image is too old for this firmware. The hardware should be updated with the config firmware command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>GNSS-Pos-Integrity</td>
<td>MIN</td>
<td>60</td>
<td>2</td>
<td>is set if 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>UTC-Corr-Unk</td>
<td>MAJ</td>
<td>0</td>
<td>0</td>
<td>is set if 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Description</td>
<td>Severity</td>
<td>Status</td>
<td>Alarm Condition</td>
<td>Action</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------</td>
<td>----------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Eth-Port0-Down</td>
<td>MAJ 0 2</td>
<td></td>
<td></td>
<td>is set when 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.</td>
<td>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.</td>
</tr>
<tr>
<td>Eth-Port1-Down</td>
<td>MAJ 0 2</td>
<td></td>
<td></td>
<td>is set when 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.</td>
<td>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.</td>
</tr>
<tr>
<td>Eth-Mgmt-Down</td>
<td>MAJ 0 2</td>
<td></td>
<td></td>
<td>is set when 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.</td>
<td>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.</td>
</tr>
<tr>
<td>Eth-Same-Subnet</td>
<td>CRI 0 0</td>
<td></td>
<td></td>
<td>is set when any of 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 2 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</td>
<td>Configure the ethernet ports to use different subnets.</td>
</tr>
</tbody>
</table>
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 then this alarm can be safely ignored.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>24</strong></td>
<td>SyncE0-Unsupported</td>
<td>CRI</td>
<td>0</td>
<td>0</td>
<td>is 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>25</strong></td>
<td>SyncE1-Unsupported</td>
<td>CRI</td>
<td>0</td>
<td>0</td>
<td>is set when SyncE (either input or output) is enabled on eth1 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>26</strong></td>
<td>Time-Set-Bad</td>
<td>CRI</td>
<td>0</td>
<td>0</td>
<td>indicates that the hardware time has never been set to agree with a valid phase source. This occurs only on startup and will clear as soon as the unit has a valid phase time to establish a valid time reference.</td>
</tr>
</tbody>
</table>

**Note 1:** "Level" means default set level of alarm. It has several levels and user can choose one of options below.
- 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.

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.

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.

If the alarm persists for longer than 60 minutes, call Trimble Technical Support.
## Contact Information

<table>
<thead>
<tr>
<th>Region</th>
<th>Location</th>
<th>Phone Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NORTH AMERICA</strong></td>
<td>Trimble Inc. Corporate Headquarters</td>
<td>+1-800-787-4225, +1-408-481-7741</td>
</tr>
<tr>
<td></td>
<td>Sunnyvale, CA 94085</td>
<td></td>
</tr>
<tr>
<td><strong>EUROPE</strong></td>
<td>Trimble Inc Europe Phone:</td>
<td>+46-8-622-12-79</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>KOREA</strong></td>
<td>Trimble Export Ltd, Korea Phone:</td>
<td>+82-2-555-5361</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CHINA</strong></td>
<td>Trimble Navigation Ltd, China Phone:</td>
<td>+86-10-8857-7575</td>
</tr>
</tbody>
</table>