Disclaimer

The information in this quick start guide is provided to assist users in the installation, first-time setup, and operation of the Masterclock GMR6000. While every effort has been made to ensure accuracy, Masterclock, Inc. assumes no responsibility for any errors or omissions that may appear.

Specifications, features, and firmware functionality are subject to change as part of Masterclock's policy of continuous product improvement. Some functions or options described may not be available in all versions or configurations of the GMR6000.

If discrepancies are found between this document and the operation of your unit, or if further clarification is needed, please contact Masterclock Technical Support for assistance.

Contact and Technical Support

If you have questions or require information not found in this manual, or need assistance with setup, configuration, or troubleshooting, please contact Masterclock Technical Support.

Our team is available to provide detailed guidance for your specific application and ensure your equipment operates at its full capability.

Masterclock, Inc.
2484 West Clay Street
St. Charles, MO 63301 USA

Email: support@masterclock.com
Phone (U.S. & Canada): 800-940-2248
Phone (International): +1-636-724-3666

For additional documentation, firmware updates, or technical resources, visit www.masterclock.com.

1. Safety Information

To ensure proper use of the GMR6000 and to avoid damage to the unit or injury, follow the guidelines below:

⚠ Electrical Safety:

- Operate only within rated AC/DC ranges.
- Ensure proper grounding.
- Do not operate with damaged cables or connectors.

⚠ Environmental Safety:

- Operate between 0-60 °C, <90% RH non-condensing.
- Avoid exposure to liquids or corrosive environments.

⚠ Mechanical Safety:

- Use rack-mount hardware for installation.
- Units with Rubidium oscillators require 1U spacing above and below for airflow.
- Do not place on desktops or block vents.

⚠ Warnings:

- No user-serviceable parts inside.
- Opening the unit risks electric shock or shorting sensitive components.

Compliance:

- Meets IEC 62368-1 and EN IEC 55035 standards.

2. Package Contents

Each GMR6000 shipment includes the following items:

- GMR6000 Unit
- Power cable supplied according to configuration (IEC cable for AC models, DC terminal block connector for DC models)
- Quick Start Guide
- Rack-mount hardware
- Ethernet Cable (10ft)

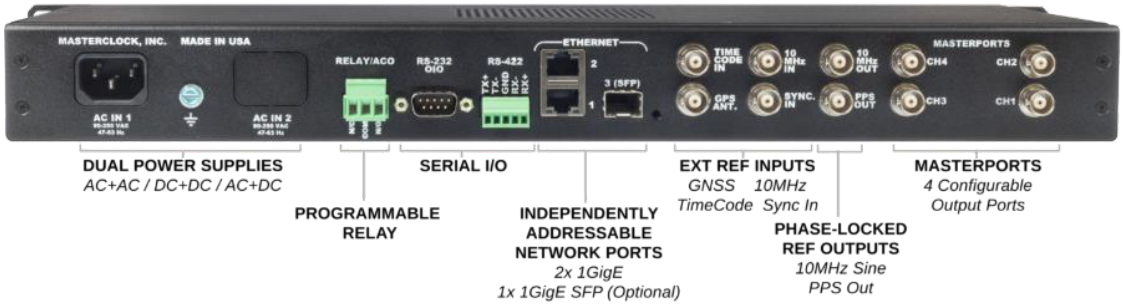
Optional accessories may also be included if ordered, such as GNSS antenna, or SFP modules. Verify all contents before installation and retain packaging for warranty service.

3. Product Overview

3.1 Front Panel Features

• 13-Digit LED Display: Displays date/time or DOY/time; configurable UTC/local; brightness and DST adjustable.
• Multicolor LED Indicators: Power, Holdover, Lock, Stability, and Reference Source (GNSS/PTP/NTP/TC)

3.2 Rear Panel Features



• Power Inputs: Configurable for Single AC, Single DC, Dual AC, Dual DC, or AC+DC redundancy.
• Ethernet Ports: Two RJ45 Gigabit Ethernet ports, plus optional SFP cage.
• Serial Interfaces: RS232 and RS422 for NMEA, NENA, Truetime/Kinemetrics.
• Reference Inputs: GNSS, PPS, IRIG/SMPTE.
• Reference Outputs: PPS, 10 MHz.
• MasterPorts (4x): Four BNC outputs, each independently programmable.

4. Installation & Setup

This section provides a step-by-step walkthrough for installing and preparing the GMR6000 for operation. Follow these instructions in order:

4.1 Unpack and Inspect

Before installation, verify that the GMR6000 and all accessories are present and undamaged. Handle the unit carefully during unpacking to prevent accidental impact or static discharge.

1. Unpack the Unit
   - Remove the GMR6000 and all included components from the shipping box.
   - Retain all packaging materials in case the unit needs to be stored or shipped in the future.

2. Verify Package Contents
   The standard shipment typically includes:
   - One (1) GMR6000 Master Clock
   - One (1) or more AC or DC power cables (depending on model and redundancy options)
   - Rack-mount ears (pre-installed on the unit)
   - Quick Start Guide or safety documentation
   - Optional accessories, if ordered (such as GNSS antenna, SFP module, or DC terminal connector)
   Compare the contents with your packing list or purchase order to confirm all ordered accessories are included.

3. Inspect for Shipping Damage
   - If damage to the shipping box is visible, inspect the GMR6000 before installation.
   - Contact Masterclock technical support if any damage to the unit is found.

4. Record Device Information
   - Note the serial number, MAC address, and initial password printed on the rear label.
   - This information is required for technical support or service inquiries.
   - Product registration is not required for warranty coverage.

5. ESD Precautions
   - When installing or connecting the unit within a rack or system, wear ESD-appropriate accessories such as a wrist strap or grounding device.

4.2 Mount the Unit

1. Select a Suitable Location
   - Install the unit in a standard 19-inch equipment rack that provides stable support and proper ventilation.
   - Ensure the ambient temperature remains within the specified operating limits (see Section 11).
   - Avoid areas with excessive dust, vibration, or direct airflow from adjacent cooling fans.

2. Ventilation Requirements
   - The GMR6000 passively dissipates heat through its side, top, and bottom vents.
   - Allow a minimum of 1U of open space above and below the unit for airflow.
   - Do not block or cover the vent openings. Provide additional rack ventilation if required to maintain stable temperatures.

3. Rack Installation
   - The rack-mount ears are pre-installed on the chassis.
   - Position the unit in the desired 1U space and secure it using four user-supplied rack screws compatible with the rack rails. This unit needs 1U of space above and below for ventilation.

- Support the unit from underneath during installation to prevent twisting or stress on the rack ears.
- Tighten screws evenly to keep the front panel level and flush with adjacent equipment.

4. Temporary Testing Setup
- The GMR6000 may be placed on a stable table or bench for short-term testing before rack installation.

5. Grounding
- Ensure the equipment rack or installation site is properly grounded according to local electrical codes.
- If required by site policy, connect the chassis ground terminal on the rear panel to a known earth ground using an appropriate grounding conductor.

⚠️ Caution: Inadequate ventilation or improper mounting may cause overheating, resulting in reduced performance or shortened component life.

4.3 Connect Reference Inputs

The GMR6000 can synchronize to several external timing references, such as GNSS, time code, or a PPS source. Connect the appropriate inputs based on your system requirements.

1. GNSS Connection
- Attach the supplied or site-provided GNSS antenna cable to the GPS ANT connector on the rear panel.
- The antenna should have an unobstructed view of the sky.
- Avoid routing the cable near strong RF sources or power lines to reduce interference.
- If using a surge protector or lightning arrestor, install it near the building entry point and ensure proper grounding.

2. Time Code Input
- For synchronization to an external time code source (IRIG-B or SMPTE LTC), connect the source to the TIME CODE IN BNC connector.
- Verify that the time code format matches the configuration expected by the unit.
- Use high-quality 50 Ω shielded coaxial cable for accurate transmission.

3. PPS Reference Input
- Connect a stable PPS reference to the SYNC IN BNC connector.
- Ensure the reference source and GMR6000 share a common ground to maintain signal integrity.

4. Verifying Connections
- Confirm that all BNC connectors are fully seated.
- Avoid excessive cable strain or sharp bends near connectors.
- Tip: Labeling reference cables is considered best practice for easier maintenance and troubleshooting, though it is not required.

4.4 Connect Reference Outputs

The GMR6000 can output many different signals for time synchronization, such as PPS and 10MHz, as well as many licensable formats such as Timecode, Genlock, Wordclock, and TLS, using the user-configurable MasterPorts. Connect the appropriate outputs based on your system requirements.

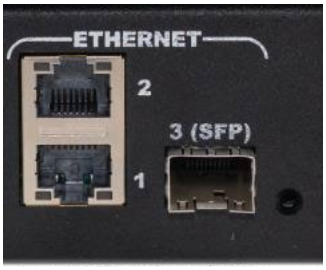
1. PPS Reference Output
   - To synchronize a device to PPS, connect the device to the PPS OUT BNC connector.

2. 10Mhz Reference Output
   - To synchronize a device to 10Mhz, connect the device to the 10MHz OUT BNC connector.

3. MasterPort Reference Outputs
   - For all other signal outputs, such as IRIG or SMPTE Timecode, NTSC or PAL Genlock, TLS, Wordclock, or Square Waves, use one of the four user-configurable MasterPorts.
   - By default, MasterPorts are set to output nothing, unless the Timecode feature is licensed, in which case it will default to IRIG-B00. Make sure to configure a selected MasterPort Channel to the required output. If an output type is not available, make sure it is licensed for your unit.
   - To synchronize a device to a MasterPort, connect the device to the appropriate MasterPort Channel (CH) BNC connector.

4.5 Connect to Network(s)

The GMR6000 provides multiple Ethernet interfaces for time synchronization, network communication, and administrative access. Connect the appropriate ports according to your network design.



1. Identify Network Ports
   - The GMR6000 includes three network interfaces: Ethernet 1, Ethernet 2, and 3 (SFP).
   - Each interface operates independently and can be configured for specific roles such as PTP, NTP, or Syslog.
   - only Interface 1 (Ethernet 1) can be used for management, including configuration.
   - Each port supports 10/100/1000 Mbps operation and automatically negotiates link speed and duplex.
   - Ports default to DHCP Enabled. Refer to Section 4.8 to set static addressing for interfaces.

2. Ethernet Connections
   - Connect Ethernet 1 and/or Ethernet 2 to network switches using Cat-5e or higher cabling.
   - If fiber connectivity is required, insert a compatible SFP transceiver (Masterclock has a list of known compatible transceivers available) into Ethernet 3 (SFP) and attach the appropriate fiber patch cable.
   - Ensure that all connections are fully seated.

3. Connection Verification
- Once power is connected (4.6), observe the rear-panel network activity LEDs to confirm link and data transfer.
- If a port remains inactive, verify cabling, switch configuration, and SFP compatibility.

4.6 Power Connections

The GMR6000 is available in both AC and DC power configurations. Optional redundant inputs are available if selected at time of purchase for continuous operation in the event of a power-source failure. Device will begin to boot once power is connected.

1. Verify Power Requirements
- Confirm that the power source matches the input type indicated on the rear label.
- Refer to Section 11 Specifications for allowable voltage ranges and current requirements.
- Ensure all power connections comply with local electrical and safety regulations.

2. AC-Powered Units
- Connect the supplied AC power cord to the AC IN connector.

- Plug the other end into a properly grounded outlet rated 100–240 VAC, 50/60 Hz.
- For models with dual AC inputs, connect both cords to independent circuits for redundancy.

3. DC-Powered Units
- Connect the DC input connector to a stable DC source within the specified voltage range.
- Observe correct polarity when attaching leads; positive (+) and negative (–) are labeled on the connector label, along with voltage and current rating.

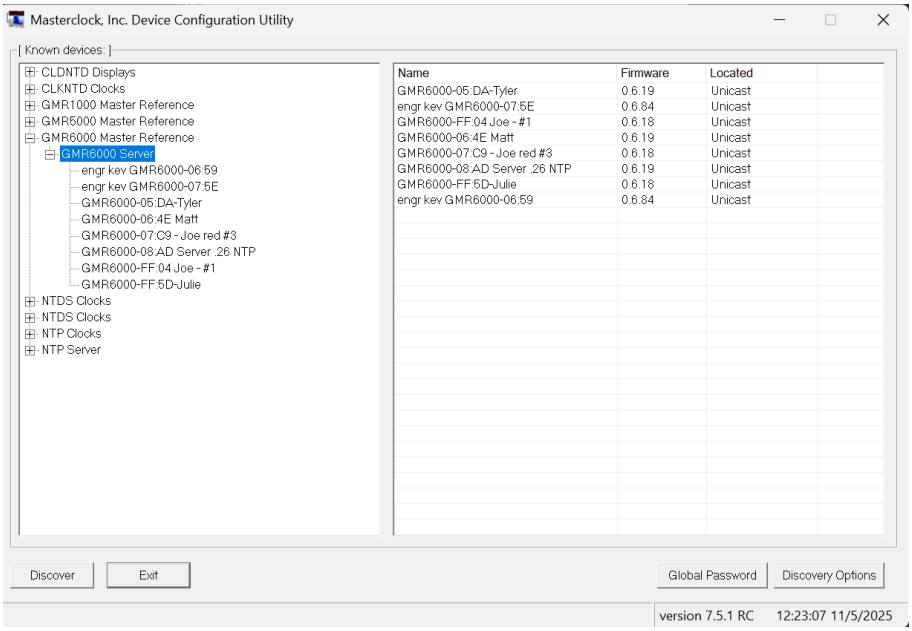
- If dual DC inputs are provided, connect each to a separate supply for reliability.

4. Cable Management and Safety
- Route power cables away from signal and network cables.
- Avoid sharp bends or strain on connectors.
- Use cable ties or routing clips to maintain clear airflow.

5. Grounding
- The chassis is bonded to earth ground through the power connection.
- A rear-panel chassis ground terminal is provided for optional direct bonding to facility ground if required.

✅ **Note:** In redundant configurations, the GMR6000 automatically uses **Power Input 1** as the primary supply, while **Power Input 2** remains in standby. If Power Input 1 fails, the unit seamlessly switches to **Power Input 2** to maintain uninterrupted operation. When Power Input 1 is restored, the GMR6000 automatically reverts to it as the primary power source.

4.7 WinDiscovery Overview



WinDiscovery is Masterclock's configuration and management software for the GMR6000 and other Masterclock devices. It provides a graphical interface for network discovery, setup, and monitoring, making it the preferred tool for system administrators who want to configure, verify, or troubleshoot their device without command-line access. The application can be used for initial setup, live monitoring, or day-to-day configuration, providing access to nearly all features available through SSH or the front panel.

Installation and Access

WinDiscovery is available from Masterclock's official website and is compatible with Windows 10 and later. Installation requires administrator rights on the PC. When launched, the program scans all local subnets for connected Masterclock devices after pressing the "Discover" button. Detected units appear in the main window with their model, firmware version, IP address, status, and reference state.

As the GMR6000 is password-protected, WinDiscovery prompts for the administrator password before configuration can be made.

Tip: You can view basic device properties or status without a password by right-clicking the device entry and selecting the appropriate option.

Network Discovery

WinDiscovery automatically discovers devices using UDP broadcast communication upon pressing the "Discover" button. Devices appear automatically if located within the same subnet. Devices with static IP addresses outside the subnet can be added manually by entering the address in the Add Device dialog.

Tip: If a device does not appear in the discovery list, verify that the PC and GMR6000 are on the same network segment, and confirm that Windows Firewall allows UDP traffic for WinDiscovery.

Configuration Features

WinDiscovery provides access to nearly all configuration options available on the device, including:

- Network configuration for each interface (DHCP or Static).
- Input and Output Control for NTP, PTP, Time Code, MasterPorts, and GNSS.
- Administrative Functions (Set Time/Date, Reboot, Password, etc.).
- Status and monitoring.

4.8 Initial Power-On and Reset

1. Power-On Sequence
   - Apply power to the unit using the connected AC or DC source. There is no on/off switch.
   - The front-panel display and status LEDs illuminate while the system performs its internal boot sequence.

2. Reset and Credential Display
   - Perform a single short press of the Reset button on the front panel (to the right of the USB jack).
   - The display will show the unit's assigned IP address(es) followed by a unique, factory-generated password, which remains visible for several seconds.
   - Record the password carefully for first-time access.

Note: This password can also be found on the device label.

3. First-Time Access via WinDiscovery

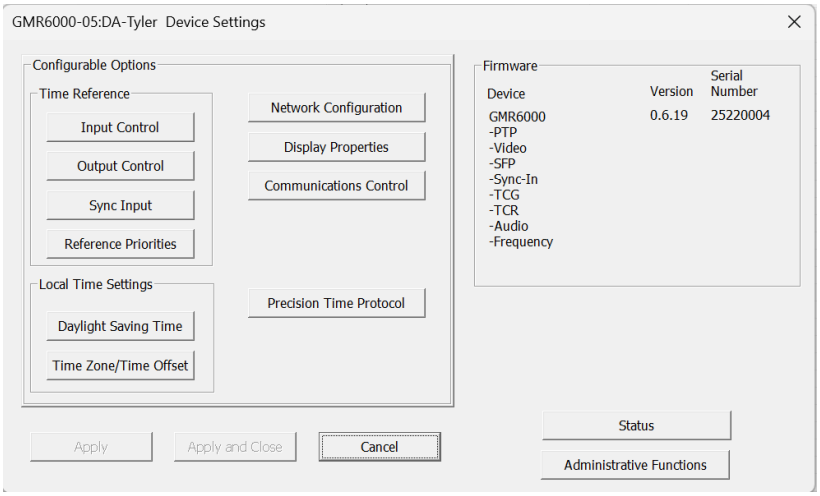
Note: Advanced users can also perform first-time setup through SSH. Refer to Section 5.6 for more information.

- Launch WinDiscovery on a computer connected to the same network. Ethernet interface 1 must be connected.

- If a network connection is unavailable, you can use WinDiscovery with the USB port on the front panel. This is recommended if you are setting up a device in a static-IP only networking environment.

- Press the "Discover" button on the bottom left of the main window. Devices are listed in a tree by family and device type.
- When the GMR6000 appears in the device list, select it from the drop-down to begin first-time setup.
- Enter the unique, factory generated password when prompted (See 4.8.2).
- You will then be asked to create a new administrative password. The default password will already be filled in for you. Choose a secure password and store it safely.

- Select the device again to begin device configuration, entering the administrative password if asked:



- To set static IP information or change device name, select “Network Configuration”.
- To change display brightness or information, select “Display Properties”.
- To change SNMP or Syslog settings, select “Communications Control”.
- To change PTP settings, select “Precision Time Protocol”.
- To change NTP Client, Time Code Reader, NMEA Client, or GNSS settings, select “Input Control”.
- To change NTP Server, MasterPort, or NMEA output settings, select “Output Control”.
- To change the PPS input settings, select “Sync Input”.
- To change the Reference Priority settings, select “Reference Priorities”.
- To change Daylight Savings or Time zone Settings, select the “Daylight Saving Time” or “Time Zone / Time Offset” buttons under “Local Time Settings”.
- To change date or time, set password, reboot device, install a new licensable option, configure leap seconds, or default configuration, select “Administrative Functions”.
- To view device status, select “Status”, or right-click the device in the device list and select “Status”.

- To queue configuration changes, make sure to press “OK” on dialogs. This will enable the “Apply” button on the primary “Device Settings” dialog box (or sometimes in some other dialogs).

- Pressing the “Apply” button will send configuration to the device. WinDiscovery will validate that the device accepts the configuration changes. Some configuration changes (such as network configuration) will require a few seconds to reconnect to the device before continuing.

⚠️ Caution: If the administrative password is lost or forgotten, a full factory reset is required to regain access.

4.9 Verifying System Operation

After powering on and configuring access credentials, verify that the GMR6000 is functioning properly and synchronized to the intended reference.

1. Check Front-Panel Indicators
   - Confirm that the Power, Reference, and Locked LEDs display expected states (See 5.2 for front panel LED behavior).
   - The Locked indicator will blink once per second, at top of second, once synchronization is achieved.
   - If the unit remains in Holdover, confirm that external references are properly connected and active.

2. Confirm Reference Status
   - Allow several minutes for GNSS or other references to stabilize.
   - Verify correct lock indication on the panel.

Note: References are selected by the GMR6000 automatically, based on a user-configurable priority list and reference eligibility. By default, the highest priority reference is GNSS.

3. Check Network Connectivity
   - Confirm network link and activity LEDs indicate valid connections.
   - Assuming the user is using WinDiscovery, verify that the device appears in WinDiscovery with the expected IP address(es).

4. Verify Output Functions
   - Confirm that connected clients or downstream devices (NTP clients, PTP endpoints, time code receivers, etc.) are receiving valid time from the GMR6000 by checking the device status in Windiscovery or the SSH 'status' command.
   - Compare output time with the reference source to confirm proper synchronization. Note that it can take several minutes after locking to a reference before the PPS output is aligned with the active reference.

5. Operational Readiness
   - Once synchronization and connectivity are verified, the GMR6000 is fully operational.
   - The unit will automatically maintain synchronization using the highest-priority available reference according to user-defined settings.

5. Operation

5.1 Startup & Shutdown

When power is applied, the GMR6000 performs an internal self-test. The front-panel LEDs illuminate in sequence during boot to confirm LED function. The display will show basic system initialization status until the unit has completed boot. Once the self-test passes, the unit begins acquiring its reference based on the configured input priority

Time to Synchronization

• Synchronization time to external references depends on the source:
- GNSS: May take several minutes depending on satellite visibility and antenna placement.
- PTP/NTP: Typically less than a minute, depending on network latency.
- Time Code / PPS / 10 MHz: Near immediate, once signal is detected.

• Once a valid external reference is available, the unit automatically transitions from internal oscillator holdover to locked synchronization.

Shutdown Behavior

The GMR6000 is designed as a continuous-operation device with no soft shutdown process. To power off the unit, remove AC or DC power via the rear-panel inlet(s). If redundant supplies are installed, both must be disconnected for complete power-down.

Holdover Operation

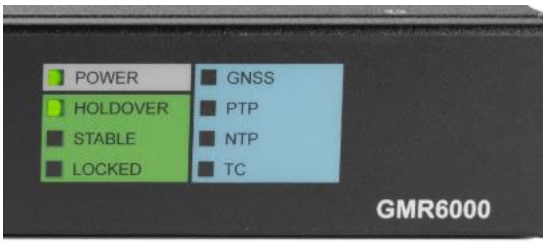
If the configured reference is lost, the GMR6000 automatically enters holdover mode, disciplined by its internal oscillator (Standard, High-Stability OCXO, or Premium Rubidium depending on configuration). In holdover, LEDs and relay alarms indicate loss of synchronization. Normal operation is maintained and seamlessly continues when a valid reference is restored.

Note: This assumes the device was not in holdover mode for an extended period, such as several weeks, and that the device went from one UTC locked reference to another.

5.2 Front Panel Operation

13-Digit LED Display

The GMR6000 is equipped with a 13-digit, 7-segment LED display. The display can be configured to show Date and Time or Day of Year and Time. Users can configure display preferences via WinDiscovery or SSH CLI: date format, UTC vs Local time, Time zone offset, DST adjustments, display brightness, and format.



Multicolor LED Indicators

The GMR6000 has eight front-panel LEDs, each providing system and synchronization status.

The Power, Holdover, and Stable LEDs will be solid green upon meeting their requisite conditions.

If a unit has dual power supplies, then the Power LED will glow amber if only one power supply is detected.

The Locked LED with either be off without a lock, or blink once per second with a lock.

For the GNSS, PTP, NTP, and TC LEDs, they will be off without any reference, amber if they are ready but not being used as the system reference, or solid green if they are being used as the system reference. The PTP and NTP LEDs also blink if the GMR6000 is being used as a master/server.

5.3 Reference Monitoring

The GMR6000 supports multiple synchronization reference sources, all of which can be prioritized by the user. The device constantly monitors the health of each configured input and automatically selects the highest-priority valid source.

Reference Inputs

• GNSS – GPS, GLONASS, Galileo, BeiDou; optional M-Code.
• PTP (IEEE 1588) – v2 and v2.1, supporting Default, Delay Request-Response, Peer-to-Peer, Telecom G.8275.1, Power 61850-9-3, Power C37.238-2011, Power C37.238-2017, SMPTE 2059-2 (i.e. SMPTE 2110), AES67 media, and SMPTE/AES compatibility profiles.
• NTP Client – When configured to reference an upstream NTP server.
• Time Code Input – IRIG-B(DCLS/AM), SMPTE 12M, or SMPTE 309M.
• PPS (Pulse-Per-Second) – TTL-level sync input, optional time and date information from NMEA.

Input Priority

The active reference is determined by a user-defined priority list set through WinDiscovery or SSH. If the primary reference becomes invalid or unavailable, the unit seamlessly switches to the next available input. Once the preferred source returns, the device will automatically revert to it.

Monitoring & Status

• Front Panel Indicators: Reference status shown by the Lock, Reference Source, and GNSS Satellite LEDs.
• Relay Output: Can be configured to trigger on reference loss.
• Management Interfaces: WinDiscovery (GUI – detailed status), SSH CLI (detailed status), SNMP (reference health and alarms), Syslog (event logging).

Holdover Behavior

If no valid external reference is available, the GMR6000 remains in holdover mode, referencing its internal oscillator (OCXO, Rb, depending on configuration). Drift is minimized according to the oscillator's performance (see Section 9). When an external reference returns, the system disciplines and corrects any accumulated drift before resuming locked synchronization. Normally, when going from holdover to a lock to an external reference, a jam sync does not occur. However, a jam sync is possible if the device was in holdover for an extended period of time, such as two weeks.

5.4 Using the Reset Button

The GMR6000 includes a recessed front-panel reset button that provides various options depending on its usage.

Initial Setup

Pressing Reset briefly during first-time installation causes the unit to show a randomly assigned password on the LED display. Enter this password in WinDiscovery or SSH, then define a new secure password when prompted. (Refer to 4.8)

Password Recovery

User-defined passwords are not recoverable, loss of a password will require a full factory reset.

System Restart

- Single quick press: Does not interrupt normal operation, briefly shows network info on display.
- Long press (>3 seconds): Triggers a full factory reset (Hard reset)

Safety Notes

Reset should be used cautiously, as a system restart will temporarily interrupt all outputs.

5.5 Alarm & Relay Behavior

The GMR6000 includes an integrated alarm relay output to provide hardware-level alerting for loss of lock to a reference.

Alarm Indication

- Syslog/SNMP Alerts: Alarms are logged and reported for integration with monitoring systems.
- Alarms are typically indicated using syslog or SNMPv3 traps. Relay Contact Behavior: NO contact closes on alarm; NC opens on alarm—allowing energized or de-energized alarm circuits.

5.6 Remote Management

The GMR6000 supports several remote interfaces for configuration, monitoring, and maintenance.

WinDiscovery

Windows-based GUI application that auto-discovers Masterclock devices, provides full configuration, and displays graphical status. Access requires a valid administrator password. It is highly recommended that you utilize WinDiscovery as your primary application for configuration.

SSH CLI

Secure Shell command-line access for configuration, diagnostics, and automation. Access requires a valid administrator password. Type "?" at the CLI prompt for a list of commands, and "command ?" for instructions on how to use a specific command. For example, "network ?" will list basic information on how to use the "network" command. Section 7 contains a full list of SSH commands.

The default Username is **admin**

SNMP (Simple Network Management Protocol)

Supports v1, v2c, and v3 for monitoring device health, reference lock, oscillator state, and alarms. SNMPv3 provides authentication and encryption (AES-256). Configuration access requires a valid administrator password.

Syslog

Logs events (reference loss, alarms, authentication attempts, etc.) to an external Syslog server for centralized monitoring.

Note: Syslog is configurable for all network interfaces.

USB Port

Provides local management when network access is unavailable, including first-time setup and configuration using WinDiscovery, as well as firmware updates. Access requires a valid administrator password.

6. Maintenance & Troubleshooting

The GMR6000 is designed for long-term reliability and minimal maintenance. Regular checks and proper monitoring ensure consistent performance.

6.1 General Maintenance

• Operate within specified environmental limits. This is a precision electronic device and should be treated as such.
• Keep vents clear of dust; clean exterior surfaces with a clean, dry cloth.
• Perform firmware updates when provided by Masterclock.
• Inspect cabling regularly for wear or damage if problems arise.

⚠ **No user-serviceable parts inside**. Contact support@masterclock.com for assistance.

6.2 Preventive Checklist

Routine checks can be performed using WinDiscovery or CLI status:
• Reference lock status (GNSS, PTP, etc.).
• Time and frequency accuracy against trusted sources.
• Relay alarm functionality.
• Network connectivity (ping, NTP/PTP responses).
• Redundant power supply operation.

6.3 Troubleshooting

Below you will find some common issues and corrective actions, if you are still unable to resolve the issue please contact Masterclock at support@masterclock.com for assistance:

• Loss of Synchronization:
- Verify reference priorities and network configuration are correct.
- Check the Status window in Device Settings using WinDiscovery.

• NTP/Network Issues:
- Verify NTP (client/server) service is enabled.
- Check firewall settings on network equipment for UDP port 123.
- Confirm authentication keys match.
- Verify there are no IP address conflicts when using static IP. In general IP address conflicts do not occur when using DHCP. But, they are still possible if there is a device on a DHCP network that is

not using DHCP.
- Check the configuration of your network switch.

• PTP Issues:
- Confirm correct PTP profile is selected. Avoid deviating from default profile configuration to ensure maximum compatibility with other equipment.
- Verify the correct PTP domain is configured.
- IEEE 1588 hardware timestamping in network switches is generally not required. However, if PTP is being used it is highly recommended that PTP aware switches with hardware timestamping are being used.

- Certain PTP configurations and profiles, such as Layer 2 Peer-to-Peer and Power Profiles, **require** a compatible network switch to function without relying on potentially erroneous network switch behavior.

- Network switches must be configured to be compatible with the PTP configuration in all PTP devices.

- All PTP devices on the network must be configured to be compatible with each other.
- Use CLI or WinDiscovery to check status.

• Power Problems:
- Confirm correct power supply type (AC/DC).
- Verify redundant supplies (if installed) are functional.
- Inspect cables and connections at both ends.

6.4 Troubleshooting Tips

All GMR units are fully checked and system tested at the factory for proper operation before shipment. Unless physical damage is found, the unit is probably functional and the issue lies with configuration. The following problems can be readily solved by the customer/user.

Software Tip: WinDiscovery uses bi-directional UDP messaging on port **6163** for both the discovery process and to communicate configuration. It also sends status packets to and from all Masterclock network devices on this port. Delivery of UDP messages (packets) is NOT guaranteed. If needed, to cross subnets, Windiscovery will use multicast addresses 224.0.1.255, 224.0.1.254, port 6172, and port 6173.

Troubleshooting WinDiscovery Connectivity: If you experience intermittent communication or connection problems with WinDiscovery, first close the current session and restart the application. If the issue persists, review and apply the troubleshooting tips provided in this section.

If these steps do not resolve the problem, use an alternate configuration method such as SSH.

PROBLEM:

Unable to find (discover) the new GMR in WinDiscovery.

POSSIBLE REASONS/SOLUTIONS:

1. Verify that you have supplied power to the GMR.

2. Verify that all the network cables, hubs, etc. are in proper working order.

3. After clicking the **Discover** button, wait until the status indicates 100% completion.

4. Verify that the GMR is on the same physical network as the computer from which you are running WinDiscovery.

5. If the computer is separated from the GMR by a router (on a remote network) or a firewall it is likely that the router/firewall is blocking communication with the device. Run WinDiscovery from a computer within the remote network or ask a network system administrator to configure the router/firewall in question to pass through (in both directions) UDP broadcasts on port 6163. See "Software Tip" above.

6. Unfortunately, some routers will not forward UDP broadcasts across networks, but WinDiscovery requires this. If you are running a personal firewall product, or the built-in Windows firewall, you may need to adjust their configurations to pass through (in both directions) UDP traffic on port 6163. See "Software Tip" above.

7. Verify that the hub/router/switch is capable of supporting the speed the GMR requires.

8. Verify that a DHCP server is present on the network. If the GMR has been configured to use DHCP for network configuration, but none is present, the GMR may not respond to discovery requests for up to twenty seconds after power-on.

9. Reset the GMR to initiate a new DHCP IP address request or use the static IP address mode.

10. Consult your network system administrator to obtain a list or range of available IP addresses.

Note: DHCP configuration is enabled as a factory-default. In addition, the clock will reset its address (during fallback) to a default address within the link-local address space (169.254.xxx.yyy where xxx.yyy are the last two bytes of the MAC address) when no DHCP server is present or cannot be reached.

PROBLEMS:

- WinDiscovery finds the GMR, but the status display is intermittent or not updating.
- The GMR clock is not responding to configuration changes made in WinDiscovery.
- Now that the GMR is hooked up other device(s) do not appear in WinDiscovery.
- The status or settings characters are garbled.

POSSIBLE REASONS/SOLUTIONS:

1. WinDiscovery may have been left open too long and the GMR's configuration may have changed during the session. This can occur if the DHCP server has issued new or refreshed addresses without alerting you. Remedy: close and restart WinDiscovery.

2. The discovery process was not complete before selecting your device. After clicking the **Discover** button, please wait until the status indicates 100% completion.

3. Verify that the physical network cables and equipment and configuration for UDP have not changed.

4. Verify that you are currently the only user accessing the device via WinDiscovery, SSH.

5. Heavy network traffic reduces the bandwidth and/or causes collisions with the UDP messages/packets. Heavy traffic can cause WinDiscovery to show outdated or garbled information. Remedy: Press the **Discover** button again and wait until the process completes to refresh WinDiscovery.

6. Take steps to increase the bandwidth and/or reduce network traffic. If this is an ongoing problem, consider the SSH method or move the GMR to an isolated LAN.

PROBLEMS:

- GMR name appears in RED in WinDiscovery.
- GMR assigned an IP address of 169.254.xxx.xxx.
- GMR does not maintain its assigned IP address.
- Function is erratic. It appears to periodically reset.

POSSIBLE REASONS/SOLUTIONS:

1. Incorrect network configuration may cause the GMR to use a fallback IP address or perform soft restarts. Verify that the IP address is correct. If you manually enter (or DHCP assigns)

an IP address that already exists on the network, this will create a conflict. The GMR will reset its address (fallback) to one within the link-local address space. Determine the cause of the fallback IP address and resolve the issue.

2. View the error status field at the bottom of the **GMR Status** window for messages.

3. If static IP addressing is being used the original conflicting static IP address can be restored by doing a soft restart of the device using either WinDiscovery or SSH prior to changing any other configuration parameters.

Note: Devices which have resorted to using a fallback IP address of 169.254.xxx.xxx will be displayed in the main WinDiscovery window with RED text, indicating a problem with the configuration.

6.5 Contact Support

If issues persist, contact Masterclock technical support:

- Email: support@masterclock.com
- Phone (US/Canada): (800) 940-2248
- Phone (International): +1 (636) 724-3666

Provide the model number, serial number, and firmware version when contacting support.

7. GMR6000 SSH Commands

Commands are grouped with the command name shown once, followed by its variables and usage. Blank cells under 'Command' indicate additional variables for the same command.

Command	Variables	Usage
admin	lockout	Enables or disables network administrative management lockout.
brightness		Show display brightness level.
	x	Set display brightness level.
devicename		Show the current device name.
	xxx	Set device name to xxx.
display		Show the current format.
	12eu	Change the format to 12-hour Time, European (dd/mm/yy) Date.
	12us	Change the format to 12-hour Time, U.S. (mm/dd/yy) Date.
	12asian	Change the format to 12-hour Time, Asian (yy/mm/dd) Date.
	24eu	Change the format to 24-hour Time, European (dd/mm/yy) Date.

	24us	Change the format to 24-hour Time, U.S. (mm/dd/yy) Date.
	24asian	Change the format to 24-hour Time, Asian (yy/mm/dd) Date.
	eu12	Change the format to European (dd/mm/yy) Date, 12-hour Time.
	us12	Change the format to U.S. (mm/dd/yy) Date, 12-hour Time.
	asian12	Change the format to Asian (yy/mm/dd) Date, 12-hour Time.
	eu24	Change the format to European (dd/mm/yy) Date, 24-hour Time.
	us24	Change the format to U.S. (mm/dd/yy) Date, 24-hour Time.
	asian24	Change the format to Asian (yy/mm/dd) Date, 24-hour Time.
	dayofyear on	Turn on day-of-year.
	dayofyear off	Turn off day-of-year.
dropframe	jam	Command drop frame to jam sync top-of-second.
	jamtime hh:mm	Set the local daily time of drop frame jam.
dst		Show Daylight Saving Time settings.
	eu	Set Daylight Saving Time to EU standard.
	us	Set Daylight Saving Time to US/Canada standard.
	off	Turn off Daylight Saving Time (begin/end dates are wiped out).
	ex	Show examples of how to enter relative and absolute dates.
gnss		Show info about the GNSS receiver.
	offset #	Set the nanosecond offset (#= signed nanosecond offset).
	sat x y z	Select 1-3 satellite constellations to receive.
	interference x	Turn interference detection on or off where x is 'on' or 'off'.
	jam-bb #	Set the jamming broadband detection threshold (#= 1dB-15dB).
	jam-cw #	Set the jamming continous wave detection threshold (#= 1db-31db).

	aug x y z	Augmentation system where x, y, or z is one of SBAS, QZSS, IMES, D-GPS, none.
	survey-in x	Improved timing performance can be achieved in stationary applications, where x is 'on' or 'off'.
	defaults	Set the GNSS receiver back to default settings.
	dynamic x	Set the GNSS receiver dynamic mode to either the normal or airborne where x is 'normal' or 'airborne'.
	acquisition x	Set the acquisition mode where x is 'normal', 'high', or 'highest'.
hso		Show the HSO status information.
	savecal	Save the current HSO calibration.
	reset	Reset the oscillator calibration.
	jam	Jams PPS output to the current reference.
	jam_threshold	Shows the threshold for triggering a jam (in microseconds).
	jam_threshold x	Sets the jam threshold. A value of '0' disables jamming.
	eval osc	Recalibrate the oscillator frequency range.
hsoholdover		Show the HSO holdover settings.
	[on/off]	Set the device to immediately not use any external references.
	start hh:mm:ss	Enter the scheduled UTC start time for the holdover to begin.
	stop hh:mm:ss	Enter the scheduled UTC stop time for the holdover to end.
	enable	Enable scheduled holdover to start at the selected time.
	disable	Disable scheduled holdover.
igmpmode	x	Sets the reporting mode where x is 0-3.
leapsecond		Show the leap second parameters.
	on yyy mm/dd/yyyy	Enable a positive/negative Leap Second at 23:59:59 UTC time for the date entered.
	off	Disable Leap Second processing.
ledtest		Show the current format.
	1	Turn on all segments.

	2	For each digit, rotate between the segments at full brightness.
	off	Turn the LED test off.
memfree		Displays current system/extended memory usage and status.
memtest		Tests and reports status of system/extended memory.
mport		Show Masterport settings for all outputs.
	[i]	Show Masterport settings for a specific output.
	[i] local	Offset timecode using local time settings for daylight savings and time zone.
	[i] utc	Apply no offsets to timecode, use UTC.
	[i] custom	Offset timecode using custom settings for daylight savings and time zone.
	[i] dst	Set custom daylight savings offset for timecode.
	[i] tz	Set custom time zone offset for timecode.
	[i] smpte	Enable a SMPTE timecode on a Masterport.
	[i] irig	Enable an IRIG timecode on a Masterport.
	[i] wave	Enable a waveform output on a Masterport.
	[i] video	Enable a video/audio sync output on a Masterport.
	[i] off	Disable a Masterport.
network		Show network interface summary.
	[I]	Show details for interface where [I] = interface.
	[I] dhcp (on/off)	Set DHCP on/off for the interface.
	[I] a4 [address]	Set a static IPv4 address for the interface.
	[I] n4 [address]	Set a static IPv4 netmask for the interface.
	[I] g4 [address]	Set a static IPv4 default gateway for the interface.
	[I] dns 1 [address]	Set a static IPv4 DNS server address for the interface.
	[I] dns 2 [address]	Set a static IPv4 DNS server address for the interface.
	[I] static show	Show configured static information for the interface.
	[I] static commit	Commit static configuration changes on the interface.

	[I] arp	Show the ARP table for the interface.
	[I] mcast report	Trigger a multicast report for the interface.
	[I] mcast show	Show multicast subscriptions on the interface.
	[I] dhcp release	Immediately release DHCP lease on the interface and revert to fallback IP.
	[I] dhcp renew	Immediately renew a DHCP lease on the interface.
nenaoutput		Display basic information about NENA output.
	xxx yyy port baud parity	Enable NENA Output, where x is the format (format0, format1, format8), y is lock or nolock, port is output port (rs232, rs422, or rs232/rs422), baud is baud rate (4800, 9600, 19200, 38400), and parity is none, odd, or even.
	off	Disable NENA Output.
nmeainput		Display basic information about NMEA Input.
	port baud parity	Enable NMEA Input, where port is input port (rs232 or rs422), baud is baud rate (4800, 9600, 19200, 38400).
	timeout n	Set timeout, where n is the number of seconds to wait for a NMEA message.
	max n	Set max change of time, where n is the max change of time in seconds.
	off	Disable NMEA Input.
nmeaoutput		Display basic information about NMEA Output
	off	Disable NMEA Output
	on	Enable all NMEA Output Messages
	on xxx	Enable NMEA Output Message x.
	port baud parity	Enable NMEA Output on a port, where port is the output port (rs232, rs422 or rs232/rs422), baud is the baud rate (4800, 9600, 19200, 38400), and parity is none, odd, or even.
ntpclient		Display current NTP Client settings.
	stats	Show detailed stats about current servers.

	start/stop	Start/stop NTP client.
	dhcp on/off	Use DHCP-provided NTP servers.
	alarm on/off	Ignore packets with the alarm flag set.
	set interface [i]	Set the interface NTP client operates on.
	set timeout [number]	Set server timeout in seconds (not working).
	set offset [number]	Apply a microsecond offset to received packets (not working).
	set broadcast on/off	Enable/disable client broadcast mode.
	set broadcast addr [ip]	Set the IP address for broadcast messages.
	set broadcast timeout [number]	Set timeout for broadcast servers.
	set broadcast auth on/off	Enable/disable authentication for broadcast.
	list	View current NTP server list.
	list on/off	Enable/disable NTP server list.
	list add [server name] interface [i]	Add server to list (IP or URL).
	list remove [server num]	Remove server from the list.
	list [server num] name [server name]	Change server name.
	list [server num] interface [i]	Change interface for server.
	list [server num] interval [number]	Set polling interval (log2 seconds).
	list [server num] burst on/off	Send initial burst of requests after connecting.
	list [server num] auth enable/disable	Enable/disable authentication for server.
	list [server num] key [number]	Set the key ID for server authentication.
ntpclientauth		Show the current NTP client authentication settings and keys.
	key x y z –a “str”	Add key, where x is the key entry (up to 15), y is the key number (1-65535), z is the hash type (MD5, SHA1, or SHA2), and “str” is an ASCII string.
	key x y z –h “hex”	Add key, where x is the key entry (up to 15), y is the key number (1-65535), z is the hash type (MD5, SHA1, or SHA2), and “str” is a hexadecimal string.

	trusted x y ... z	Set keys to trusted, where x y ... z is a list of key numbers.
	nottrusted x y ... z	Set keys to untrusted, where x y ... z is a list of key numbers.
ntpserver		Display current NTP server settings.
	start/stop	Start/stop the NTP server.
	interface [i] on/off	Enable/disable NTP server on an interface.
	alarm on/off	Set the alarm flag in outgoing NTP packets upon reference loss.
	set id [name]	Set the reference ID of the NTP server (≤4 characters).
	set offset [number]	Set microsecond offset applied to outgoing NTP packets (not working).
	set stratum_locked [number]	Set stratum level reported when locked to non-NTP reference.
	set stratum_unlocked [number]	Set stratum level reported when not locked.
	broadcast on/off	Enable/disable broadcast server.
	broadcast frequency [number]	Set frequency of broadcast messages in seconds.
	broadcast addr [ip]	Set the IP address for broadcast messages.
	broadcast ttl [number]	Set TTL for broadcast packets.
	broadcast auth enable/disable	Enable/disable broadcast authentication.
	broadcast auth keyid [number]	Set the key ID used by the broadcast server.
ntpserverauth		Show the current NTP server authentication settings and keys.
	key x y z –a “str”	Add key, where x is the key entry (up to 15), y is the key number (1-65535), z is the hash type (MD5, SHA1, or SHA2), and “str” is an ASCII string.
	key x y z –h “hex”	Add key, where x is the key entry (up to 15), y is the key number (1-65535), z is the hash type (MD5, SHA1, or SHA2), and “str” is a hexadecimal string.
	trusted x y ... z	Set keys to trusted, where x, y ... z is a list of key numbers.
	nottrusted x y ... z	Set keys to untrusted, where x, y ... z is a list of key numbers.
options		Display licensable features.

password	password xxx yyy zzz	Change password (xxx=current, yyy=new, zzz=confirm).
ping	-I intf	Network interface to use for transmitting requests.
	-c count	Stop after sending count packets.
	-h hoplimit	Set IPv6 hoplimit or IPv4 TTL
	-i interval	Wait interval seconds between packets.
	-p pattern	Set byte pattern for packet data.
	-s size	Set number of data bytes.
properties		Show system properties like model, serial, software versions, MAC
ptp	status	Show PTP service status summary.
	config	Enter PTP interactive configuration.
	[start/stop]	Start/stop PTP service.
	[enable/disable]	Enable/disable PTP service at system start.
	syslog [enable/disable]	Enable/disable PTP diagnostic to syslog.
	verbosity [0-7]	Set PTP diagnostic verbosity level.
reflossallowserver		Show the allow time server setting.
	x	Set timeout (seconds) for disabling server on reference loss.
	allow	Allow server during reference loss.
	disallow	Disallow server during reference loss.
reflossdashes		Show the clock-mode reference loss display setting.
	x	Set colon flash duration before display blanking.
	colonflash	Flash colons on reference loss.
	nodashes	Do not display dashes on reference loss.
refpri		Show current reference priority status and settings.
	<reference> <enable/disable>	Enable/disable a specific reference.
	<reference> <priority>	Set priority for a specific reference.
	default	Reset references to default priorities.

	10 mhz [auto/internal/external]	Set 10 MHz to use only internal, only external input, or auto to use external if present.
refstatus		Show reference priority level, condition, and eligibility.
settodefault	y	Reset configuration to defaults (network unchanged).
	all y	Reset configuration + network configuration to defaults
snmp		Show basic SNMP settings.
	start	Start the SNMP agent.
	stop	Stop the SNMP agent.
	contact abc	Set system.sysContact to abc.
	name abc	Set system.sysName to abc.
	location abc	Set system.sysLocation to abc.
	add xxx.xxx.xxx.xxx	Add IP address for traps.
	del x	Delete IP address number x.
	coldstart	Send a test cold-start trap.
	warmstart	Send a test warm-start trap.
	linkup	Send a test link-up trap.
	linkdown	Send a test link-down trap.
	sendtrap abc	Send a test trap with text abc.
	community add abc	Name the custom community the text abc.
	community del	Delete the name of the custom community.
	v12 [on/off]	Enable/disable SNMP v1 and v2 read-only access.
snmplogin	trapuser X	Set Xth trap user.
	authpriv 1	Use SHA128/AES128 authentication & privacy.
	authpriv 2	Use SHA256/AES256 authentication & privacy.
	names	Show the SNMP names.
	add name pw	Add a new SNMP name and password.
	del name	Delete a SNMP name.
status		Show system time dissemination status and current references.
syncinput	disable	Disable SYNC IN.
	nmea [on/off]	Require NMEA input for date/time, SYNC IN for top of second.
	manual [on/off]	Sync current or manually set system time to SYNC IN.
	edge [rising/falling]	Capture using rising or falling edge.

	offset #	Set nanosecond offset for SYNC IN.
syslog	[enable/disable]	Enable/disable syslog output.
	interface [interface name]	Set network interface for syslog.
	server [hostname/IP]	Set remote syslog server.
	port [port-number]	Set remove syslog port.
	test	Send a test message.
tcr		Show Time Code Reader settings.
	nanoseconds #	Set nanosecond offset for TCR top of second.
	smpte_nodate	Set SMPTE date encoding to none.
	smpte_leitch	Set SMPTE date encoding to Leitch type.
	smpte_309m	Set SMPTE date encoding to 309M type.
	smpte_309m_no_time_zone	Set SMPTE date encoding to 309M type, no time zone.
	irig_nodate	Set IRIG date encoding to none.
	irig_1344year	Set IRIG date encoding to use IEEE 1344.
	local	Offset timecode using local time settings.
	utc	No offset, UTC time.
	custom	Offset timecode using custom time settings.
	dst [eu/us/off/ex]	Set custom timecode daylight savings offset (ex is for manual examples).
	tz xx:yy:zz	Set custom timecode time zone offset to x hours + y minutes + z seconds.
tcr_cal		Show calibration setting.
	auto	Auto calibration mode.
	manual x	Manual calibration gain x (1–255).
	saved	Saved calibration mode.
	timeout x	Set timeout of saved mode for re-calibration after lock is lost for x seconds.
	now	Break lock and calibrate now.
time		Show the current time and date.
	hh:mm:ss mm/dd/yyyy	Set UTC time and date (24-hour format, year >=2000).
timezone		Show the current time zone.
	xx:yy:zz	Set time zone UTC + x hours y minutes z seconds.

truetime		Show TrueTime/Kinemetrics output parameters.
	on	Enable TrueTime output.
	on xxx port baud parity	Enable TrueTime output, where xxx indicates "lock" or "nolock", port is output port (rs232 or rs422), baud is baud rate (4800, 9600, 19200, 38400), and parity is none, odd, or even.
	off	Disable TrueTime output.
	time utc	Output UTC time.
	time local	Output Local time.
zeros		Show leading zeros setting.
	on	Turn on leading zeros (24-hour mode).
	off	Turn off leading zeros (24-hour mode).