EndRun TECHNOLOGIES
"Smarter Timing Solutions"

Sonoma N22 *Network Time Server*

GPS-Synchronized

User Manual

USM3052-0000-000 Revision NC
September 2025

Sonoma N22 *GPS*

Network Time Server User Manual

Preface

Thank you for purchasing the Sonoma Network Time Server. Our goal in developing this product is to bring precise, Coordinated Universal Time (UTC) into your network quickly, easily and reliably. Your new Time Server is fabricated using the highest quality materials and manufacturing processes available today, and will give you years of trouble free service.

About EndRun Technologies

EndRun Technologies has been dedicated to the development and refinement of the technologies required to fulfill the demanding needs of the time and frequency community since 1998.

The instruments produced by EndRun Technologies have been selected as the timing reference for such rigorous applications as computer synchronization, research institutions, aerospace, network quality-of-service monitoring, satellite base stations, and calibration laboratories.

Trademark Acknowledgements

Linux, UNIX, and Windows are registered trademarks of the respective holders.

EndRun Contact Information

Address: EndRun Technologies
2270 Northpoint Parkway
Santa Rosa, CA 95407
U.S.A.
Phone: (707)573-8633
Fax: (707)573-8619
Sales: 1-877-749-3878 or (707)573-8633
sales@endruntechnologies.com
Support: 1-877-749-3878 or (707)573-8633
support@endruntechnologies.com

Part No. USM3052-0000-000 RevisionNC
September 2025

About This Manual

This manual will guide you through simple installation and set up procedures.

Introduction – The Sonoma N22, how it works, where to use it, its main features.
Basic Installation – How to connect, configure and test your Sonoma with your network.
NTP Server and Client Set-Up – Two client sections; one for Unix-like platforms and one for Windows.
Network Protocols - Covers Security, LDAP, TACACS+, RADIUS, SNMP, HTTPS, IPv6 and PTP/IEEE-1588.
Console Port – Description of the console commands for use over the network and USB ports.
Options – Description of any optional features that your Sonoma might have.

If you detect any inaccuracies or omissions, please inform us. EndRun Technologies cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice.

Warranty

This product, manufactured by EndRun Technologies, is warranted against defects in material and workmanship for a period of three years from date of shipment, under normal use and service. During the warranty period, EndRun will repair or replace, at its option, products which prove to be defective. Products not manufactured by EndRun Technologies are warranted for ninety days or longer, as provided by the original equipment manufacturer, from date of shipment.

Extended Warranty

EndRun products are supported by a strong, comprehensive standard warranty (see paragraph above). Extended warranties are available to expand the coverage period. The extended warranty can be purchased at the time of order, or during the last year of the standard warranty period.

Limitation of Warranty

The foregoing express warranty shall not apply to defects resulting from improper or inadequate maintenance by Buyer or User, Buyer-supplied software or interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product, or improper site preparation or maintenance.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS, OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, ENDRUN SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Warranty Repair

If you believe your equipment is in need of repair, contact EndRun Customer Support. It is important to contact us first as many problems may be resolved by phone or email. Please provide the serial number of the unit and the nature of the problem. If it is determined that your equipment will require service, we will issue an RMA number and specific shipping instructions.

Ship the unit prepaid in the original container or a container of sufficient strength and protection to EndRun Technologies. EndRun will not be responsible for damage incurred during shipment to us. Buyer shall prepay shipping charges to send product to EndRun and EndRun shall pay shipping charges to return product to Buyer. However, if returned product proves to be operating normally (not defective) then Buyer shall pay for all shipping charges. If Buyer is located outside the U.S.A. then Buyer shall pay all duties and taxes, if any.

Be sure the RMA number is clearly identified on the outside of the shipping container. Our policy is to repair the unit within 5 business days. If it is necessary to order parts or if other circumstances arise that require more than 5 days, an EndRun service technician will contact you.

Loaner units are not included as part of the standard warranty.

Repair After Warranty Expiration

If the warranty period has expired, we offer repair services for equipment you have purchased from EndRun. Contact EndRun Customer Support. It is important to contact us first as many problems may be resolved by phone or email. Please provide the serial number of the unit and the nature of the problem. If it is determined that the equipment has failed and you want EndRun to perform the repairs, we will issue you an RMA number and specific shipping instructions.

Ship the unit prepaid in the original container or a container of sufficient strength and protection to EndRun Technologies. EndRun will not be responsible for damage incurred during shipment to us. Customer is responsible for shipping costs to and from EndRun Technologies. Be sure the RMA number is clearly identified on the outside of the shipping container. After the equipment has been received we will evaluate the nature of the problem and contact you with the cost to repair (parts and labor) and an estimate of the time necessary to complete the work.

Limitation of Liability

The remedies provided herein are Buyer's sole and exclusive remedies. EndRun Technologies shall not be liable for any direct, indirect, special, incidental or consequential damages, whether based on contract, tort or any other legal theory.

Table of Contents

Chapter *One*

Introduction

This chapter introduces the GPS-Synchronized Sonoma Network Time Server and gives a brief overview of what it is and how it works.

What It Is

The Sonoma Network Time Server is a precision server of Coordinated Universal Time (UTC) that can be connected via an Ethernet port to any TCP/IP network. Available timing protocols include: Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), and the optional Precision Time Protocol (PTP/IEEE-1588).

In its most basic operation, the Sonoma sends NTP reply packets in response to NTP request packets which it has received from clients. The timestamps it sends in its NTP reply packets are accurate to 10 microseconds, typical. For an introductory paper on NTP see:

endruntechnologies.com/pdf/NTP-Intro.pdf

GPS Timing-How It Works

The GPS Subsystem in the Sonoma receives transmissions from satellites that are operating in compliance with the Navstar GPS Interface Specification (IS) known as GPS-IS-200. It specifies the receiver interface needed to receive and demodulate the navigation and time transfer data contained in the GPS satellite transmissions. The GPS navigation system requires a means of synchronizing the satellite transmissions throughout the constellation so that accurate receiver-to-satellite range measurements can be performed via time-of-arrival measurements made at the receiver. For the purposes of locating the receiver, measurements of the times-of-arrival of transmissions from at least four satellites are needed. For accurate time transfer to a receiver at a known position, reception of the transmissions from a single satellite is sufficient.

The GPS system designers defined *system time* to be *GPS time.* GPS time is maintained by an ensemble of high-performance cesium beam atomic frequency standards located on the earth's surface (GPS Master Clock Ensemble). GPS time is measured relative to UTC, as maintained by the United States Naval Observatory (USNO), and maintained synchronous with UTC-USNO except that it does not suffer from the periodic insertion of leap seconds. Such discontinuities would unnecessarily complicate the system's navigation mission. Contained in the data transmitted from each satellite is the current offset between GPS time and UTC-USNO. This offset is composed of the current integer number of leap seconds difference and a small residual error that is typically less than +/- 10 nanoseconds.

Each satellite in the constellation contains redundant cesium beam or rubidium vapor atomic frequency standards. These provide the timebase for all transmissions from each satellite. These transmis-

sions are monitored from ground stations located around the world and carefully measured relative to GPS time. The results of these measurements for each satellite are then uploaded to that satellite so that they may be incorporated into the data contained in its transmissions. The receiver can use this data to relate the time-of-arrival of the received transmissions from that satellite to GPS time.

All of this means that during normal operation, the source of the timing information being transmitted from each of the satellites is directly traceable to UTC. Due to the nature of the GPS spread-spectrum modulation scheme, this timing information may be extracted by a well-designed receiver with a precision of a few nanoseconds. The GPS Subsystem in the Sonoma does just that.

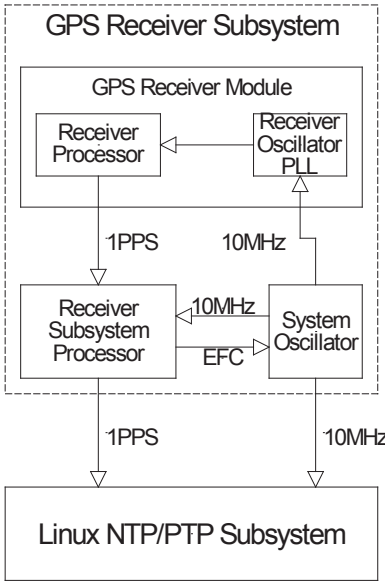
GPS Receivers

GPS-based timing systems supporting critical infrastructure could be vulnerable to malfunction due to weak signals, jamming, spoofing or accidental GPS control system errors. Proprietary algorithms in Sonoma perform advanced integrity checks to filter random and persistent errors to the GPS subframe data.

EndRun developed a timing optimized GPS receiver for additional resiliency, accuracy, and reliability. The EndRun GPS Receiver strictly complies to the IS-GPS-200 specification. GPS receiver specifications are listed in ***Appendix H - Specifications***.

Time Synchronization Components

The Sonoma is composed of a Global Positioning System (GPS) Subsystem containing the EndRun GPS Receiver and system oscillator. The GPS Subsystem is integrated with a fan less, convection-cooled *1.2 GHz CPU with two integrated Ethernet ports that provide NTP (and optionally PTP). This is called the Linux/NTP Subsystem. The drawing below shows Sonoma's time synchronization components.



SONOMA GPS SUBSYSTEM

Where to Use It

Since signals from the GPS satellites are available at all locations on the globe, you may deploy the Sonoma virtually anywhere. However, you must be able to install an antenna either on the rooftop or in a window so that satellite transmissions may be received at least several times during the day. For more information see ***Appendix E - Installing the GPS Antenna***.

Once synchronized, the Sonoma can maintain acceptable network synchronization accuracy for about a day without GPS reception, by flywheeling on its standard temperature compensated crystal oscillator (TCXO). The TCXO ensures a 24-hour holdover period without a GPS signal. For longer holdover periods of 35 days or more, an oscillator upgrade may be installed in your Sonoma.

Client/Slave Software

The Sonoma has been designed to operate in conjunction with existing public domain NTP/SNTP client software and may be used in any network environment that is using TCP/IP protocols. Although client software is available for all platforms, for the most precise applications, the Unix-like operating systems are best supported. For more information see ***Chapter 3 - NTP, Setting Up NTP Clients on Unix-like Platforms*** and ***Setting Up NTP Clients on Windows***. There is additional information about NTP Client software at this link:

endruntechnologies.com/products/ntp-time-servers/ntp-client-software

For PTP/IEEE-1588 applications, the Sonoma can inter operate with a variety of Slave software and hardware. For more information on PTP Slave Software go to this link:

endruntechnologies.com/products/grandmaster-clocks/ptp-slaves

This page intentionally left blank.

Chapter *Two*

Basic Installation

This chapter will guide you through the most basic checkout and physical installation of your Sonoma Time Server. See ***Chapter 3 - NTP*** *for instructions on how to configure your unit as an NTP Server. See* ***Chapter 4 - PTP/IEEE-1588*** *for instructions on how to configure your unit as an optional PTP Grandmaster. Other chapters and appendices will give you the information needed to configure your installation for the maximum performance in your operating environment.*

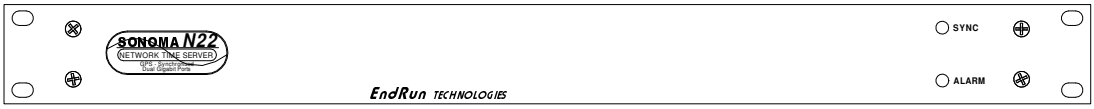
Basic familiarity with TCP/IP networking protocols is required. Though some familiarity with Linux or other Unix-like operating systems would be helpful, it is not essential. If you satisfy these conditions, the instructions provided herein should guide you to a successful installation. For a brief description of some helpful Linux commands and utilities see ***Appendix C - Helpful Linux Information****.*

Checking and Identifying the Hardware

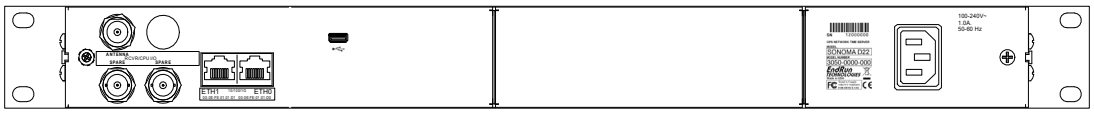
Unpack and check all the items using the shipment packing list. Contact the factory if anything is missing or damaged. The Sonoma N22 Time Server (GPS) shipment typically contains:

- Sonoma N22 (part # 3052-0001-000 or #3052- variant)
- Sonoma N22 Quick Start Guide (part # USM3052-0000-001).
- IEC 320 AC Power Cord (part #0501-0003-000)
  (This part will not be present if using the DC power option.)
- USB 2.0 A Male to Micro B Male Cable (part #0501-0037-000).
- RJ-45 to RJ-45 CAT-5 patch cable, 2 meters (part #0501-0000-000)
- GPS Antenna Kit (part #0610-0009-001). (Optional)
- GPS Anti-Jam Antenna Kit (part #0610-0009-012). (Optional)

Sonoma Physical Description



Sync LED	This amber LED flashes to indicate synchronization status.
Alarm LED	This red LED illuminates briefly at power-up, and thereafter whenever a serious fault condition exists.



The drawing above shows the Sonoma rear-panel in its most common configuration - with no optional outputs. However, there are a wide variety of optional outputs available. For more information on options see ***Chapter 10 - Options***. (For a dimensional drawing of the Sonoma chassis see ***Appendix H - Specifications***.) Descriptions below briefly describe the standard I/O connectors:

Antenna Jack	This TNC connector mates with the download cable from the external antenna.
USB Connector	This Micro B USB connector provides the serial I/O console interface to the Sonoma. This console allows you to initialize and maintain the Sonoma. See ***Chapter 9 - Console Port Control and Status.***
100/1000 Base-T Jacks	These two RJ-45 connectors mate with the Ethernet twisted pair cable from the network. They are labeled with the corresponding MAC address and either “ETH0” or “ETH1”. Integrated LEDs indicate link activity (green). The green LED will pulse with activity. Both ports provide a console interface to the Sonoma. See ***Chapter 9 - Console Port Control and Status*** for more information.
Spare Jacks (Unused)	These unused BNC connectors are usually labeled “SPARE”. When used, they will be labeled with their connector identifier (A, B, or C) and provide optional signals. Label examples are: “A-AMCODE”, “B-1PPS”, or “C-PPO”. For more information on Sonoma options see ***Chapter 10 - Options***.
AC Power Input Jack	This IEC 320 standard three-prong connector provides AC power. Other power supplies are available. See ***Chapter 10 - Options*** for more information.

Performing a Site Survey

Using the front panel status LED indicators, it's easy to find out if your Sonoma will work in your desired location:

1. Screw the TNC plug on the end of the antenna cable onto the TNC antenna input jack on the chassis rear panel of the Sonoma.

2. Apply power.

3. Plug the other end into the AC input connector on the chassis rear panel of the Sonoma.
Place the antenna in a window, or for best performance, mount it on the roof using the supplied mounting hardware. For detailed information on GPS antenna installation see ***Appendix E - Installing the GPS Antenna***.

Initially upon power up:

1. The unit will light the Alarm LED for about 10 seconds.

2. Then it will continuously light the Sync LED.

3. When the unit locks onto a GPS signal and begins to decode the timing data and adjust the system oscillator, the Sync LED will flash very rapidly (about a 6 Hz rate) until the data is fully decoded and the system oscillator is fully locked to the GPS frequency.

4. Then the Sync LED will pulse at precisely a 1 Hz rate, synchronized to UTC seconds.

At this point, the GPS Subsystem is fully synchronized, and you may proceed to permanently mounting the chassis and antenna in their desired locations.

If this sequence has not occurred within twenty-four hours, and you have mounted your antenna in a window or your rooftop installation has poor sky visibility, you may need to provide an accurate reference position to the unit so that it can operate with only one satellite in view. If you have mounted the antenna in a window and can easily move it to the rooftop, you should do that first. Should you need to provide a reference position to the unit, refer to ***Appendix E - GPS Reference Position*** and the `setgpsrefpos` command for details.

If you are unable to achieve GPS lock after trying all of these suggestions, then contact EndRun Customer Support for assistance.

NOTE TO PRECISION TIME PROTOCOL (PTP) USERS

If you want to maximize timing accuracy, see ***Appendix E - Installing the GPS Antenna, Calibrate Your Receiver***.

Installing the Sonoma

FCC NOTICE

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmul interference in which case the user will be required to correct the interference at his own expense.

Using standard 19" rack mounting hardware, mount the unit in the desired location. After mounting the unit and connecting the antenna cable, verify that it still acquires and tracks a GPS signal.

CAUTION

Ground the unit properly with the supplied power cord.

The socket outlet should be installed near the equipment and be easily accessible.

Power cord is used as a disconnection device. To de-energize equipment, disconnect the power cord. If your Sonoma has dual power supplies, then multiple power cords may be installed. To de-energize this equipment, disconnect all power cords from the device.

Le cordon d'alimentation sert de dispositif de déconnexion. Pour mettre l'appareil hors tension, débranchez-le. Si votre Sonoma est équipé de deux alimentations, plusieurs cordons d'alimentation peuvent être installés. Pour mettre cet appareil hors tension, débranchez tous les cordons d'alimentation de l'appareil.

Do not install the Sonoma N12 where the operating ambient temperature might exceed 122°F (50°C).

Connecting the Optional DC Power

The DC Power Input is an option. For installation instructions see ***Chapter 10 - Options, Connecting the DC Power***.

Connecting and Configuring Ethernet

Connect one end of the CAT-5 patch cable supplied with your Sonoma to either of the rear panel mounted RJ-45 connector labeled 100/1000 Base-T. Connect the other end of the patch cable to your network through a 'straight' port on your switch. Do not connect it to a 'crossover' port on your switch.

By factory default, the Sonoma will attempt to configure the ethernet interfaces automatically via the Dynamic Host Configuration Protocol (DHCP). The Sonoma will attempt to set the netmask, its IP address, the IP address of the default gateway, the domain name and the IP addresses of any nameservers, if the DHCP server is configured to provide them. You may optionally configure the Sonoma to also set its hostname via DHCP, if your DHCP server is configured to provide it. You can do this by running a simple script called `netconfig` after your unit is up on the network.

If your network *does* use DHCP for host configuration, and you are in a hurry to get your Sonoma up and running, you may proceed to ***Verifying Network Configuration*** to make sure that the network parameters were set up correctly. Otherwise, it is recommended that you read the following sections on the use of the USB port now, since they will help you in debugging any problems that you may encounter with the automatic configuration via DHCP.

If your network *does not* use DHCP, you will need to configure your Ethernet interfaces using either the front-panel keypad or the USB port. The following sections contain brief descriptions on how to do that.

Configuring Ethernet with the USB Port

To configure your Ethernet interfaces with the USB port, after logging in as the *root* user, you must run a simple script called `netconfig`. This script will prompt you for the needed information and perform some syntax checking on your inputs. Then it will create or modify the appropriate files needed to configure the Ethernet interface. The following sections will guide you in setting up communications with the Sonoma using its USB port.

Connect the USB Port

To test USB communications with the Sonoma you will need a terminal emulation program running on your computer. We will refer to either of these as "terminal" for the remainder of this instruction.

1. Disconnect power from the Sonoma.

2. Connect one end of the USB cable to the USB connector on the Sonoma.

3. Connect the other end of the USB cable to the terminal

Test the USB Port

You must configure your terminal to use the USB port. You must also configure your terminal as shown below:

- Baud Rate: 115200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Handshaking / Flow Control: X ON/ X OFF
- Information on USB to Serial Converter FTDI Driver: FT234XD

After configuring these parameters in your terminal, apply power to the Sonoma. After about 20 seconds, your terminal should display something similar to this:

```
Default Root File System: FACTORY
To override and boot the FACTORY version of the Root File System, type FACTORY within
5 seconds
.....
Booting FACTORY FIT image
```

These lines are the Linux bootloader boot prompts. These prompts will time out after five seconds and the factory default Linux kernel and the factory default Sonoma root file system will be loaded. When the Linux kernel is loaded from FLASH memory into RAM a long list of kernel-generated, informational messages is displayed as the kernel begins execution and the various device drivers are initialized. When the boot process completes, the Sonoma login prompt is displayed:

login as:

```
*******************************************************************************
*         Welcome to Sonoma_N22 GPS console on:  SonomaII.example.net.(none)
*         Tue Aug 26  2025 20:27:02 UTC
*******************************************************************************
```

Here you may log in as “ntpuser” with password “Praecis” or you may log in as the “root” user with password “endrun_1”. When logged in as “ntpuser”, you may check status information and view log files but you will not be able to modify any system settings or view secure files. In order to perform system setup procedures, which includes configuring the IP network settings, you must log in as the “root” user. After correctly entering the password at this prompt,

```
password:
```

the sign on message is shown. It identifies the host system as Sonoma N22 GPS and shows the software part number, version and build date. The out-of-the-box hostname is set to “Sonoma-N22”, and the domainname is set to “your.domain”.

```
Sonoma_N22 GPS 6010-0090-000 v 4.0x - Tue Aug 26 00:51:59 UTC 2025
root@SonomaII:~#
```

This last line is the standard Sonoma N22 GPS prompt. After configuring the unit, you should change the passwords using the Linux **`passwd`** command issued from the prompt.

If you do not see characters displayed by your terminal program within 30 seconds after the unit is powered up, you must troubleshoot your setup. An incorrectly wired cable or incorrect port setting in your terminal emulation program are the most common problems. Refer to ***Appendix H - Specifications*** for the signal connections for the Sonoma.

Once you have successfully established communications with the Sonoma, you may proceed to configure the network parameters using **`netconfig`** (see below). Then you can communicate with Sonoma over the network using **`ssh`** and synchronize your network computers to UTC using NTP.

Set Up Your IP

Set up the IP using the Classless Inter-Domain Routing (CIDR) format. The CIDR format allows you to allocate the IP address and routing.
The CIDR address uses slash notation to specify the number of bits in the network prefix. An IPv4 address is a 32-bit address. An IP address of 192.168.1.0 with a prefix length of 24 bits would be rep-

resented as 192.168.1.0/24. This would indicate that the first 24 bits of the IP address are the network prefix and the remaining 8 bits are the host identifier.
When setting up the IP address it is necessary that each Ethernet port gets assigned to a unique subnet. For example, setting subnet 1 and subnet 2:
eth0 IP address 192.168.1.0/24
eth1 IP address 192.168.2.0/24
Use netconfig to Set Up Your IP

Using netconfig to Set Up Your IP

NOTE

When setting up the IP addresses on both network port 0 (eth0) and 1 (eth1):

1. Be sure that they are NOT on the same subnet.

2. Configure a default gateway on either port 0 (eth0) or port 1 (eth1), BUT NOT BOTH.

https://endruntechnologies.com/pdf/StaticRoutesSetup.pdf

Editing the Network Configuration file

The netconfig utility allows you to setup the basic network configuration. It works by modifying the configuration file in /etc/rc.d/rc.inet1.conf. Advanced network configuration will require changes made in the configuration file.
You must edit the following configuration file: (See Appendix C – Helpful Linux Information for information on a simple editor.)

- `/etc/rc.d/rc.inet1.conf`

After making the changes, you must copy the edited file and copy it to the non-volatile FLASH partition and reboot the unit with the following commands:

```
cp -p /etc/rc.d/rc.inet1.conf /boot/etc/rc.d
reboot
```

The following shows the beginning of the `netconfig` interactive script:

```
*******************************************************************************
Network configuration utility for Sonoma_N22 GPS.
*******************************************************************************

Your Sonoma_N22 has 2 ports that can be assigned either an IPv4 address
and/or IPv6 address. Additionally this script can setup your hostname and
nameservers.

This script is for basic network configurations only.

Changes will not take effect until you reboot your Sonoma_N22, so if you
make a mistake just rerun this script.

What would you like to configure?
1) eth0
2) eth1
5) IPv4 Gateway
6) IPv6 Gateway
7) Hostname and Domain
8) Nameserver
```

```
9) Review settings

Please select a number (1 - 9), (s) save & quit, (q) quit without saving:
```

After configuring your ethernet interfaces, you should shutdown the Sonoma and reboot it by issuing this command at the prompt:

```
root@SonomaII:~#  reboot
```

Verify Network Configuration

If you are using the USB port to communicate with the Sonoma, you will be able to see the kernel-generated boot messages when the unit reboots. You should note the lines

```
Configuring eth0 as 192.168.1.120...
Configuring eth1 as 192.168.5.1...
```

if you have set up a static IP address, or these lines

```
Attempting to configure eth0 by contacting a DHCP server...
Attempting to configure eth1 by contacting a DHCP server...
```

if you are using DHCP. These appear near the end of the kernel generated boot messages.

If you are using DHCP and are not using the USB port, you will have to check the DHCP configuration information maintained by your DHCP server to determine the expected IP address and log in to the Sonoma using **`ssh`** to verify successful DHCP configuration. Refer to the subsequent topics in this section ***Using SSH***, for details on logging in to the Sonoma that way. Once you have logged in, you may perform the following checks.

If you are not using DHCP, the IP address shown should match the static IP address which you entered during the **`netconfig`** procedure. If so, log in as "root" at the login prompt and check the other configuration parameters using **`ifconfig`**:

```
root@SonomaII:~#  ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.141  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20e:feff:fe04:276  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:fe:04:02:76  txqueuelen 1000  (Ethernet)
        RX packets 7005  bytes 420138 (410.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 181  bytes 24791 (24.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x1ae4000-1ae4fff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 792  bytes 133169 (130.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 792  bytes 133169 (130.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Pay particular attention to the settings shown for **`eth0`** and **`eth1`**, in particular the **`netmask`**: setting,

which should match that which is appropriate for your network. Now check the remaining configuration parameters using **route**:

```
root@SonomaII:~# route

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
loopback        0.0.0.0         255.0.0.0       U     0      0        0 lo
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Here you are interested in the default gateway address. It should match the appropriate one for your network. If so, then the Ethernet interface of your Sonoma has been successfully configured to operate on your network and you are ready to check operation of the Sonoma over the network. If not, you should recheck your configuration and/or repeat the **netconfig** procedure.

If you have configured a nameserver(s) for your network, you may check that by issuing this command:

```
root@SonomaII:~#  cat /etc/resolv.conf
search your.domain
nameserver 192.168.1.1
nameserver 192.168.1.2
```

Which displays the contents of the */etc/resolv.conf* file containing the domain name you entered previously using **netconfig**, and the nameserver IP address(es) to use for that domain.

Check Network Operation

With your Sonoma network parameters properly configured, you are ready to test the setup using **ping** from a server or workstation that is able to access the network connected to the Sonoma. Alternatively, you could **ping** one of your servers or workstations from the Sonoma prompt to test the setup.

Once you have successfully established network communications with the Sonoma, you may perform all maintenance and monitoring activities. You may also monitor the Sonoma via the HTTPS interface (see ***Chapter 7 - HTTPS***).

Using HTTPS

If you want to use HTTPS you must first enable it. See ***Chapter 5 - Security, Enable/Disable Protocols*** for instructions. You may monitor the status of the Sonoma via the HTTPS interface. For security reasons, you may not change any settings. See ***Chapter 4 - HTTP/HTTPS*** for more information.

IMPORTANT

SSH and SNMP are all enabled with default passwords. To ensure security, change the passwords or disable the protocols.

To change the passwords for SSH use the Linux `passwd` command. To change the passwords/community strings for SNMP see ***Chapter 6 - SNMP***.

To disable SSH and SNMP see ***Chapter 5 - Security, Disable Protocols***.

Security conscious users will want to use **ssh**, as the login means. The companion utility, **scp** provides a secure replacement for **ftp** as a means of transferring files to and from the Sonoma. Both of these protocols are supported in the Sonoma via the OpenSSH implementations for Linux. Refer to ***Chapter 5 - Security, Open SSH*** for more information about the secure shell protocol.

Using SSH

When establishing a **ssh** connection with your Sonoma, logging in directly as *root* is permitted. When you log in as *root* via a **ssh** session with the Sonoma, this banner will be displayed:

```
*******************************************************************************
*    Welcome to the Sonoma_N22 GPS SSH console on:  SonomaII.example.net
*******************************************************************************

Password:
```

Here you may log in as “root” with password “endrun_1”. After correctly entering the password the sign on message is shown. It identifies the host system as Sonoma and shows the software part number, version and build date:

```
Sonoma_N22 GPS 6010-0090-000 v 4.0x - Tue Aug 26 00:51:59 UTC 2025
root@SonomaII:~#
```

This last line is the standard Sonoma N22 GPS prompt. After configuring the unit, you should change the passwords using the Linux **passwd** command issued from the prompt.

Issuing **exit** will close the **ssh** session.

Chapter *Three*

Network Time Protocol (NTP)

This chapter describes how to configure the Sonoma NTP Server. It also includes brief instruction for setting up NTP Clients on your Unix-like or Windows platform. This manual is not a 'How-To' on installing and using NTP. Only basic approaches to NTP client configuration for operation with Sonoma will be described. If you have never used NTP, then you should spend some time reading the on-line documents, especially the Distribution Notes, FAQ and Configuration subject matter, which are available at:

For Linux:
nwtime.org/documentationandlinks/
or for Windows:
docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-top

A simple introduction to NTP is here:
endruntechnologies.com/pdf/NTP-Intro.pdf

Configuring the NTP Server

Configuring the Sonoma as a Stratum 1 Server

To configure your Sonoma as a Stratum 1 NTP Server you must have successfully completed the Basic Installation procedures in Chapter 2. By default, Sonoma is configured to respond to NTP requests from clients that may or may not be using MD5 or SHA1 authentication. If the clients are using MD5 authentication, they must be configured properly with the same MD5 authentication keys as Sonoma. If you need to modify the factory default Sonoma MD5 or SHA1 keys (recommended) or set up broadcast/multicast operation, then you will need to reconfigure the NTP subsystem. You may perform the configuration from a `ssh` session, the front-panel keypad or the local USB console.

NOTE

If you would like to configure your server for multicast operation, configure it as you would for broadcast operation, with the exception that you must enter this specific NTP IPV4 multicast address: 224.0.1.1, or this specific IPV6 multicast address ff05::101, when you are prompted to enter the broadcast address.

Configuring NTP Using the Network Interface or Serial Port

The following shows the question and answer configuration utility called `ntpconfig`. The user-entered responses are shown in a larger font size.

```
root@SonomaII:~# ntpconfig

*******************************************************************************
**********************Network Time Protocol Configuration**********************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure the ntp.conf and ntp.keys files   *
*   that control Sonoma_N22 NTP daemon operation.                             *
*                                                                             *
*   You will be able to create new MD5 or SHA1 authentication keys which      *
*   are stored in the ntp.keys file.                                          *
*                                                                             *
*   You will be able to update the authentication related commands in the     *
*   ntp.conf file.                                                            *
*                                                                             *
*   You will be able to configure the "broadcast" mode of operation, with     *
*   or without authentication.  If you supply the multicast address instead   *
*   of your network broadcast address, then you will be able to configure     *
*   the time-to-live of the multicast packets.                                *
*                                                                             *
*   The changes you make now will not take effect until you re-boot the       *
*   Sonoma_N22.  If you make a mistake, just re-run ntpconfig prior to        *
*   re-booting.                                                               *
*                                                                             *
*   You will now be prompted for the necessary set up parameters.             *
*                                                                             *
*******************************************************************************
*******************************************************************************

---MD5 Keyfile Configuration


Would you like to create a new ntp.keys file? ([y]es, [n]o)  y


You will be prompted for a key number (1 - 65534), then the actual key.
When you have entered all of the keys that you need, enter zero at the next
prompt for a key number.

MD5 keys may contain from 1 to 31 ASCII characters.  They may not contain
contain SPACE, TAB, LF, NULL, or # characters!  If the key is longer than
20 characters, then only the valid hexadecimal characters
(0 - 9, a, b, c, d, e, f) may be used.


Enter a key number (1-65534) or 0 to quit:  1

Enter the key (1-31 ASCII characters):  EndRun_Technologies

Writing key number: 1 and Key: EndRun_Technologies to ntp.keys

Enter a key number (1-65534) or 0 to quit:  2

Enter the key (1-31 ASCII characters):  Sonoma

Writing key number: 2 and Key: Sonoma to ntp.keys

Enter a key number (1-65534) or 0 to quit:  0

---NTP Authentication Configuration
```

```
Do you want authentication enabled using some or all of the keys in
the ntp.keys file? ([y]es, [n]o)  y

You will be prompted for the key numbers (1 - 65534), that you want NTP to
"trust".  The key numbers you enter must exist in your ntp.keys file.  If you
do not want to use some of the keys in your ntp.keys file, do not enter them
here.  NTP will treat those keys as "not trusted".

Clients that use any of the "trusted" keys in their NTP polling packets will
receive authenticated replies from the Sonoma_N22.  When you have entered
all of the "trusted keys" that you need, enter zero at the next prompt for a
key number.

Enter a trusted key number (1-65534) or 0 to quit:  1

Enter a trusted key number (1-65534) or 0 to quit:  2

Enter a trusted key number (1-65534) or 0 to quit:  0

---NTP Broadcast/Multicast Configuration


Would you like to enable broadcast/multicast server operation? ([y]es, [n]o)  y

Set the network broadcast/multicast address for the Sonoma_N22
to use.  For broadcast mode on IPV4 networks, this address is
the all 1's address on the sub-net.

Example: 111.112.113.255

On IPV6 networks, there is more than one way to
define a range of multicast addresses:

Example: ff05::1 (all nodes on the local site)
Example: ff02::1 (all nodes on the local link)

There are specific multicast addresses assigned for NTP Operation:

For IPV4 multicast operation, it is this specific address-> 224.0.1.1
For IPV6 multicast operation, it is this specific site scope address-> ff05::101

Enter IP address for NTP broadcast/multicast operation
(aaa.bbb.ccc.ddd or aaaa::bbbb ):  224.0.1.1

You have selected multicast operation.  Enter the TTL value that is
needed for multicast packets on your network (1, 32, 64, 96, 128, 160, 192, 224):  32

It is highly recommended that authentication be used if you are using NTP
in broadcast/multicast mode.  Otherwise clients may easily be "spoofed" by
a fake NTP server.  You can specify an MD5 key number that the Sonoma_N22
will use in its broadcast/multicast packets.  The clients on your network must
be configured to use the same key.

Would you like to specify an MD5 key number to use with
broadcast/multicast mode? ([y]es, [n]o)  y

Enter the MD5 key number to use (1-65534):  2
```

```
*******************************************************************************
*******************************************************************************
*                                                                             *
*  The Sonoma_N22 Network Time Protocol configuration has been updated.       *
*                                                                             *
*             Please re-boot now for the changes to take effect.              *
*                                                                             *
*******************************************************************************
*******************************************************************************
*******************************************************************************
```

Configuring the Sonoma as a Stratum 2 Server

Operating Sonoma as a Stratum 1 Server is the recommended mode. However, there are times when Stratum 2 operation is a good strategy:

1. When you want a backup source of time. In this case, Sonoma will operate as a Stratum 1 Server as long as it is locked to the GPS signal. If it loses the signal, then Sonoma will start to drift away from "perfect" time. Eventually, when it has drifted 10 milliseconds, it reach the unlocked condition and stop serving time on your network. If you have Sonoma configured for Stratum 2 operation, then it will continue serving time, using another Time Server as its reference. If Sonoma is later able to acquire lock on the GPS signal again, it will switch back to Stratum 1 operation.

2. When you want your Sonoma to serve accurate time, but you don't want to use the antenna (for some reason). In this case, Sonoma can operate solely as a Stratum 2 server, with no antenna connected.

Since there are innumerable ways to configure your network with Stratum 2 servers, specific instructions for how to do that are beyond the scope of this manual. General instructions on how to edit the *ntp.conf* file are below.

Edit ntp.conf File

You must edit the ntp.conf file in order to point your Stratum 2 server at a Stratum 1 server. Edit */etc/ntp.conf* and add your server line(s). (See ***Appendix C - Helpful Linux Information*** for information on a simple editor.) Here is an example:

```
server 192.168.1.1
```

Or, if you have set up a domain name server via `netconfig`, here is another example:

```
server your.timeserver.com
```

IMPORTANT

Do not remove the server lines for the refclock. Even if your Time Server is not connected to an antenna, the refclock server lines must remain.

Now save the edited file and copy it to the non-volatile flash partition with this command:

```
cp -p /etc/ntp.conf /boot/etc
```

Mask Alarm

In Stratum 1 operation an alarm will be indicated when there is a loss of signal or if the antenna is not connected. For Stratum 2 operation you may not want to see these alarms. You can mask them (prevent them from showing) by using the console port (serial/network) commands **`setsigfltmask`** and **`setantfltmask`**. Or, on the front-panel keypad/display go to the Faults submenu. Look for SigFltMask and AntFltMask and set them appropriately.

Setting Up NTP Clients on Unix-like Platforms

To configure your Unix-like computer to use your Sonoma, you must have successfully completed the NTP Server basic installation procedure described above. It is expected that you are, or have access to, a capable Unix/Linux system administrator and know more than a little about installing distributions from source code. Installation must be performed by a user with root privileges on the system.

If you have access to a usenet news server, many problems may be solved by the helpful people who participate in the Internet news group devoted to NTP at *comp.protocols.time.ntp*.

Three methods of using Sonoma with NTP clients on Unix-like platforms will be described:

Basic: This is the simplest, and will operate without MD5 authentication. **NTP beginners should always perform this setup first**.

MD5: This method is trickier only because MD5 keys must be set up and distributed accurately to the NTP clients in a secure way. Sonoma is factory configured to authenticate its replies to NTP MD5 or clients using its default set of keys.

SHA1: This method is also trickier only because SHA1 keys must be set up and distributed accurately to the NTP clients in a secure way. Sonoma is factory configured to authenticate its replies to NTP SHA1 or clients using its default set of keys.

https://endruntechnologies.com/pdf/SHA1-Authentication-Configuration.pdf

Broadcast/Multicast: This method simplifies configuration of the clients on large networks since specific server addresses need not be configured in each client's */etc/ntp.conf* file. It can be configured either with or without MD5 authentication. However, it is highly recommended that authentication be configured when using broadcast/multicast mode due to the relative ease with which a fake NTP server can take over the clock setting of the broadcast/multicast clients on the network.

Unix-like Platforms: Basic NTP Client Setup

Basic setup is relatively simple, if:

- You have been able to successfully communicate with Sonoma on your network.

- You have installed NTP on your client computer.

Configure NTP

You must edit the *ntp.conf* file which **ntpd**, the NTP daemon, looks for by default in the */etc* directory. Add this line to the ntp.conf file:

```
server 192.168.1.120
```

This line tells **ntpd** to use the NTP server at address 192.168.1.120 in addition to any other servers which might also be configured in the client's *ntp.conf* file.

Restart **ntpd** to have it begin using Sonoma. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with Sonoma. After issuing the command

```
ntpq
```

you will see the **ntpq** command prompt:

```
ntpq>
```

Use the command

```
peers
```

to display the NTP peers which your computer is using. One of them should be the Sonoma server which you have just configured. You should verify that it is being 'reached'. (You may have to continue issuing the peers command for a minute or two before you will see the 'reach' count increment.) If you have other peers configured, verify that the offset information for the Sonoma server peer and your other peers is in agreement to within a few milliseconds, assuming that the other peers are synchronized to that level of accuracy.

It may also be useful to start the NTP daemon in 'debug' mode (**ntpd -d**) to confirm successful configuration. Refer to the NTP documentation for detailed usage of these debug utilities.

Unix-like Platforms: MD5 Authenticated NTP Client Setup

MD5 authenticated setup is relatively simple, if:

- You have been able to successfully communicate with Sonoma on your network.

- Your Sonoma has been configured to perform authentication either by factory default, or by running the **ntpconfig** shell script. The example Sonoma authentication configuration shown in ***Configuring NTP Using the Network Interface or USB Port*** above, will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.

- You have successfully performed the ***Unix-like Platforms: Basic NTP Client Setup*** on your client computer.

Create the ntp.keys File

You must create a file named *ntp.keys* in the */etc* directory. It must be a copy of the one residing in the */etc* directory of your Sonoma. Use secure copy utility SCP to send the Sonoma's */etc/ntp.keys* file to your client computer. You can just use a text editor on your client computer to create an equivalent file.

IMPORTANT

Handling of the ***/etc/ntp.keys*** file is the weak link in the MD5 authentication scheme. It is very important that it is owned by ***root*** and not readable by anyone other than ***root***.

After transferring the file using `SCP`, and placing it in the */etc* directory on the client computer, issue these two commands at the shell prompt:

```
chown root.root /etc/ntp.keys
chmod 600 /etc/ntp.keys
```

Configure NTP

You must edit the *ntp.conf* file which `ntpd`, the NTP daemon, looks for by default in the */etc* directory. Assuming that you have created two trusted keys as shown in ***Configuring the NTP Server Using the Network Interface or USB Port*** above, add these lines to the end of the *ntp.conf* file:

```
keys /etc/ntp.keys
trustedkey 1 2
```

Modify the line added previously in ***Unix-like Platforms: Basic NTP Client Setup*** so that authentication will be used with the Sonoma server using one of the trusted keys, in this example, key # 1:

```
server 192.168.1.120 key 1
```

Restart `ntpd` to have it begin using the Sonoma server with MD5 authentication. Use the NTP utility `ntpq` to check that `ntpd` is able to communicate with Sonoma. After issuing the command

```
ntpq
```

you will see the `ntpq` command prompt:

```
ntpq>
```

Use the command

```
peers
```

to display the NTP peers which your computer is using. One of them should be the Sonoma server which you have just configured. You should verify that it is being 'reached'. (You may have to continue issuing the peers command for a minute or two before you will see the 'reach' count increment.) You can verify that authentication is being used by issuing the command

```
associations
```

to display the characteristics of the client server associations. In the "auth" column of the display, you should see "OK" for the row corresponding to the Sonoma server. If you see "bad", you should wait a few minutes to be sure that there is a problem since "bad" is the initial state of this setting. If the "bad" indication persists then you must check your configuration for errors. Typically this is due to a typing error in creating the */etc/ntp.keys* file on the client that causes a mismatch between the keys being used by the server and client. (If you transfer the file by `scp`, this shouldn't be a problem.) It is also possible to have a typing error in the */etc/ntp.conf* file that causes the needed key to not be included in the "trustedkey" list.

Unix-like Platforms: Broadcast/Multicast NTP Client Setup

Broadcast/multicast client setup is relatively simple, if:

- You have been able to successfully communicate with Sonoma on your network.

- Your Sonoma has been configured to perform broadcasts or multicasts by running the `ntpconfig` shell script. (This is not the factory default configuration, so be sure to run `ntpconfig`.) If you are going to use MD5 or SHA1 authentication, your Sonoma must have been configured to operate with authentication in the broadcast/multicast mode, and you must know which of the trusted keys it is using for broadcast/multicast operation. The example Sonoma configuration shown in ***Configuring the NTP Server*** above will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.

- You have successfully performed the ***Unix-like Platforms: MD5 or SHA1 Authenticated NTP Client Setup*** on your client computer, if you plan to use MD5 or SHA1 authentication.

Configure NTP Client for Broadcast

You must edit the *ntp.conf* file which `ntpd`, the NTP daemon, looks for by default in the */etc* directory. Assuming that your Sonoma server has been configured to use key 2 for broadcast authentication as shown in the example in ***Configuring the NTP Server*** above, make sure that key 2 is included in the `trustedkey` line, and add this line to the end of the *ntp.conf* file:

```
broadcastclient
```

If you are not using MD5 or SHA1 authentication, you would add these lines:

```
disable auth
broadcastclient
```

You may remove the line added previously in ***Unix-like Platforms: Basic NTP Client Setup***:

```
server 192.168.1.120
```

or the authenticated version added in ***Unix-like Platforms: MD5 Authenticated NTP Client Setup***:

```
server 192.168.1.120 key 1
```

Configure NTP Client for Multicast

You must edit the *ntp.conf* file which `ntpd`, the NTP daemon, looks for by default in the */etc* directory. And add these lines for multicast:

```
multicastclient 224.0.1.1
```

or for IPv6:

```
multicastclient ff05::101
```

If you are not using MD5 or SHA1 authentication, you would add these lines:

```
disable auth
multicastclient 224.0.1.1
```

or for IPv6:

```
disable auth
multicastclient ff05::101
```

You may remove the line added previously in ***Unix-like Platforms: Basic NTP Client Setup***:

```
server 192.168.1.120
```

or the authenticated version added in ***Unix-like Platforms: MD5 or SHA1 Authenticated NTP Client Setup***:

```
server 192.168.1.120 key 1
```

Test Broadcast/Multicast

Restart `ntpd` to have it begin using Sonoma as a broadcast or multicast server. Use the NTP utility `ntpq` to check that `ntpd` is able to communicate with Sonoma. After issuing the command

```
ntpq
```

you will see the `ntpq` command prompt:

```
ntpq>
```

Use the command

```
peers
```

to display the NTP peers which your computer is using. One of them should be the Sonoma server which you have just configured. You should verify that it is being 'reached'. (You may have to continue issuing the peers command for a minute or two before you will see the 'reach' count increment.)

If you are using authentication, you can verify that authentication is being used by issuing the command

```
associations
```

to display the characteristics of the client server associations. In the "auth" column of the display, you should see "OK" for the row corresponding to the Sonoma server. If you see "bad", you should wait a few minutes to be sure that there is a problem since "bad" is the initial state of this setting. If the "bad" indication persists then you must check your configuration for errors. Typically this is due to a typing error in creating the */etc/ntp.keys* file on the client that causes a mismatch between the keys being used by the server and client. (If you transfer the file by `scp`, this shouldn't be a problem.) It is also possible to have a typing error in the */etc/ntp.conf* file that causes the needed key to not be included in the "trustedkey" list.

Setting Up NTP Clients on Windows

To configure your Windows computer to use your Sonoma, you must have successfully completed the procedures in ***Configuring the NTP Server*** above. Client installation must be performed by a user with administrative privileges.

If you have access to a usenet news server, many problems may be solved by the helpful people who participate in the Internet news group devoted to NTP at *comp.protocols.time.ntp*.

The most common NTP client on Windows platforms is described below. Information on other NTP Client software is available at:

endruntechnologies.com/products/ntp-time-servers/ntp-client-software

Windows: W32Time

Windows uses a time service called W32Time which is automatically enabled by default during Windows installation. `w32tm.exe` synchronizes time in different ways, depending on the network implementation used. When peer-to-peer networking is used, then each individual workstation synchronizes to the NTP Server. For details, copy and paste this into your browser:

docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings

However, the most common method is with Windows Domain Networking. In this case, you must configure the Primary Domain Controller (PDC) to synchronize to the NTP Server. All other servers and workstations in the domain synchronize to the PDC. The default Windows installation procedure automatically configures workstations and servers to synchronize to the controlling PDC. So, only the PDC needs to be configured to synchronize to the NTP Server.

Security

For Unix-like platforms you can configure your NTP clients for secure MD5 authentication. See ***Unix-like Platforms: MD5 Authenticated NTP Client Setup***. You can also restrict NTP query access - see below.

Restrict NTP Query Access

The Network Time Protocol (NTP) implementation in Sonoma is built from the reference distribution at:

nwtime.org/downloads/

By factory default, remote control and query of the NTP daemon `ntpd` is disabled. Query-only operation is supported only from processes running on Sonoma itself, i.e. from the *localhost*. This restricts access to `ntpd` from remote hosts using either of the two NTP companion utilities `ntpq` and `ntpdc`.

Control via these two utilities is disabled in the */etc/ntp.conf* file in two ways. First, MD5 authentication keys are not defined for control operation via a *requestkey* or *controlkey* declaration. Second, this default address restriction line is present in the file:

```
restrict default nomodify noquery nopeer
restrict 127.0.0.1 nomodify
restrict 0::1 nomodify
```

The first line eliminates control and query access from ALL hosts. The second and third lines disable the localhost from making any modifications to the `ntpd` daemon, but query access is not affected by this restriction. These lines must not be removed, as they are necessary for various monitoring processes running on Sonoma to function properly.

Knowledgable NTP users who would like to customize the security aspects of the configuration of the NTP daemon in Sonoma should edit the */etc/ntp.conf* file directly and then copy it to the */boot/etc* directory. Be sure to retain the ownership and permissions of the original file by using `cp -p` when performing the copy.

CAUTION

If you are planning to make changes to the ***/etc/ntp.conf*** file, you must NOT restrict query access from the local host to the NTP daemon. Various system monitoring processes running on the system require this access.

An example follows which shows how to allow query access from a specific remote host with IP address 192.168.1.10 while also allowing processes running on Sonoma to have query access as well:

```
restrict default noquery nomodify nopeer
restrict 127.0.0.1 nomodify
restrict 0::1 nomodify
restrict 192.168.1.10 nomodify
```

This page intentionally left blank.

Chapter *Four*

Optional Precision Time Protocol (PTP/IEEE-1588)

This chapter contains the configuration and status information for the optional Precision Time Protocol. PTP version 2 is supported. The PTP protocol running on the Sonoma is a full Grandmaster Clock (default profile) implementation of the IEEE-1588-2008 standard.

Option

The PTP/IEEE-1588 protocol is an optional feature in the Sonoma Time Server. Read ***Chapter 10 - Options, Software Options*** if you need information on how to install a software option. To see whether this option is installed on your Sonoma, use the `installed_sw_opts` command:

Command: `installed_sw_opts`
Sonoma reply: <no reply>

In this case, there is no PTP option installed. Contact EndRun Technologies if you would like to obtain PTP for one or both ports. In the case below, PTP is installed on both ports.

```
Command:       installed_sw_opts
Sonoma reply:  The PTP0 Daemon Option is Installed.
               The PTP1 Daemon Option is Installed.
```

About PTP

The PTP implementation in the Sonoma is based on the distribution at the PTPd website:

ptpd.sourceforge.net

For more information about the `ptpd` daemon and to obtain PTP Slave software, refer to the PTPd website. When downloading PTP Slave software from the PTPd website, be sure to obtain this version: *ptpd-2.2.2.tar.gz*.

An excellent book which describes the PTP Master and Slave operation is:

Measurement, Control, and Communication using IEEE 1588,
John C. Eidson, Springer, November 2006.

More information on IEEE-1588 PTP can be found at the NIST National Institute of Standards and Technology IEEE 1588 website:

https://www.nist.gov/el/intelligent-systems-division-73500/ieee-1588

Two Gigabit Ports

The PTP daemon status and configuration is supported from two PTP companion utilities **`ptpstatx`** and **`ptpconfigx`**, where x is network port 0 (**`eth0`**) or 1 (**`eth1`**). The following table shows the Sonoma utilities that pertain to PTP:

	Daemon	Status	Configuration
PTP	`ptpd0` `ptpd1`	`ptpstat0` `ptpstat1`	`ptpconfig0` `ptpconfig1`

PTP can be enabled on one or both network ports (**`eth0`** and **`eth1`**). If PTP is enabled on only one port, then **`eth0`** is the network port identifier and you would use **`ptpstat0`** and **`ptpconfig0`** for PTP status and configuration. If PTP is enabled on both ports, then both **`eth0`** and **`eth1`** will be used.

PTP Configuration and Status

The default PTP configuration settings in the Sonoma are shown below. If you need to modify these settings then you will need to reconfigure the PTP Subsystem. You may perform the configuration from a **`ssh`** session, or the local USB console. Default PTP settings are:

	Port 0 (eth0)	Port 1 (eth1)
Sync Interval	1 second	1 second
Announce Inverval	2 seconds	2 seconds
Priority 1	128	128
Priority 2	128	128
Delay Mechanism	E2E	E2E
Domain	0	1
PTP Time Mode	PTP	PTP
PTP TTL	1	1
Transmission Mode	Multicast	Multicast

PTP Configuration Using the Network or USB Port

The **`ptpconfig0`** or **`ptpconfig1`** command starts an interactive shell script that will allow you to configure the PTP Subsystem of the Sonoma. You will be prompted to set PTP parameters as follows:

ETH Port: 0 or 1
Sync Interval (Per Second): 1, 2, 4, 8, 16, 32, 64, 128
Announce Interval (Seconds): 1, 2, 4, 8, or 16
Priority1: 0-255
Priority2: 0-255
Delay Mechanism: E2E or P2P
Domain: 0-255
PTP Time Mode: UTC or PTP
PTP TTL: 1-255
Transmission Mode: Multicast or Hybrid

One file is modified for each port. Either */etc/ptp0.conf* for `eth0` or */etc/ptp1.conf* for `eth1`. These are non-volatile files stored in the FLASH disk */boot/etc* directory. You must reboot the Sonoma after running this script for the changes to take effect.

The following is a transcript of the question and answer configuration utility provided by `ptpconfig0 or ptpconfig1`. The user-entered parameters are underlined:

```
Sonoma(root@gntp)-> ptpconfig0
*********************************************************************************
************Precision Time Protocol IEEE-1588 V2 Configuration*****************
*********************************************************************************
*                                                                               *
*   This interactive utility will guide you in configuring the ptp daemon       *
*   configuration file that controls its operation on port 0.                   *
*                                                                               *
*   You will be able to configure the PTP sync interval, announce interval,     *
*   priority1, priority2, delay mechanism , ptp domain, time mode and           *
*   time-to-live (TTL).                                                         *
*                                                                               *
*   The changes you make now will not take effect until you re-boot.            *
*   If you make a mistake, just re-run ptpconfig0 prior to                      *
*   re-booting.                                                                 *
*                                                                               *
*   You will now be prompted for the necessary set up parameters.               *
*                                                                               *
*********************************************************************************
*********************************************************************************

---PTP Sync Interval Configuration

Set the PTP Sync Interval in packets per second (1, 2, 4, 8, 16, 32, 64, 128) 1

---PTP announce interval Configuration

Set the PTP Announce Interval in seconds (1, 2, 4, 8, 16) 2

---PTP Priority1 Configuration

Set the PTP Priority1 value (0-255) 128

---PTP Priority2 Configuration

Set the PTP Priority2 value (0-255) 128

---PTP Delay Mechanism E2E or P2P

Set the PTP Delay Mechanism (E2E or P2P) E2E

---PTP Domain Configuration

Set the PTP Domain value (0-255) 1

---PTP Time Mode Configuration

Set the PTP Time Mode (UTC or PTP) PTP

---PTP TTL Configuration

Set the PTP TTL value (1-255) 1

Set the PTP Transmission Mode (Multicast or Hybrid) Multicast
```

```
*******************************************************************************
*******************************************************************************
*                                                                             *
*  The Precision Time Protocol IEEE-1588 V2 configuration has been updated.   *
*                                                                             *
*             Please re-boot now for the changes to take effect.              *
*                                                                             *
*******************************************************************************
*******************************************************************************
*******************************************************************************
```

Now reboot the system by issuing this command at the shell prompt:

```
reboot
```

PTP Status Using the Network or USB Port

The `ptpstat0` or `ptpstat1` command allows you to query the status of the PTP Subsystem. Following is the response to this command:

```
V  SI  AI  P1  P2  DM  DOM  MODE  TTL  CLASS  SCALE  STATE  CLKID  UTC UTCV  CA  L59  L61  TT  FT TM
```

Where:

V is the IEEE-1588 version 2 for the 2008 standard.

SI is the PTP sync interval either 1, 1/2, 1/4, 1/8, 1/16, 1/32, 1/64, or 1/128 seconds.

AI is the PTP announce interval, either 1, 2, 4, 8, or 16 seconds.

P1 is the PTP priority 1 in a range from 0 to 255.

P2 is the PTP priority 2 in a range from 0 to 255.

DM is the PTP delay mechanism , either E2E or P2P.

DOM is the PTP domain, in a range from 0 to 255.

MODE is the PTP time mode, either UTC or PTP.

TTL is the PTP multicast time-to-live in a range from 1 to 255.

CLASS is the PTP clock class one of SYNCHRONIZED, HOLDOVER, or UNLOCKED.

SCALE is the PTP timescale either PTP or ARB.

STATE is the PTP port state one of MASTER, PASSIVE, LISTENING or INITIALIZING.

CLKID is the PTP clock source either GPS or OSC.

UTC is the PTP utc offset in seconds from TAI.

UTCV is the PTP utc offset valid, either TRUE or FALSE.

CA is the PTP clock accuracy one of 25ns, 100ns, 250ns, 1us, 2.5us, 10us, 25us, 100us, 250us, 1ms, 2.5ms, 10ms, or Unknown.

L59 is the PTP leap 59 second indicator, either TRUE or FALSE.

L61 is the PTP leap 61 second indicator, either TRUE or FALSE.

TT is the PTP time traceable indicator, either TRUE or FALSE.

FTis the PTP frequency traceable indicator, either TRUE or FALSE.

TM is the PTP transmission mode, either MULTICAST or HYBRID

PTP Operation

The Sonoma is configured as an IEEE-1588 Grandmaster Clock (default profile). Verify that the network settings have been configured and tested using `netconfig`. Once the network has been configured the Sonoma will begin to transmit PTP Sync messages after it is locked.

The PTP Sync Interval is user configured. 1, 2, 4, 8, 16, 32, 64, or 128 packets per second are transmitted as a multicast. The packets are only transmitted when the clock is fully synchronized or in holdover with a known clock accuracy.

The PTP Announce Interval is user configured. Packets are transmitted every 1, 2, 4, 8, or 16 seconds as a multicast. The packets are only transmitted when the clock is fully synchronized or in holdover with a known clock accuracy.

The Delay Request Interval is not user-configurable. It is set to 32 seconds.

The PTP Priority 1 is user configured in a range from 0 to 255.

The PTP Priority 2 is user configured in a range from 0 to 255.

The PTP Delay Mechanism is user configured to either E2E or P2P. E2E uses the delay request-response mechanism and P2P uses the peer delay mechanism.

The PTP Domain is user configured in a range from 0 to 255.

The PTP Time Mode is user configured to either UTC or PTP. When UTC Time mode is configured the clock transmits the UTC epoch and sets the PTP Scale to ARB. When the Time mode is PTP the clock transmits the PTP epoch (TAI) and sets the PTP Scale to PTP. See ***About the PTP Second and UTC Time*** at the end of this chapter for more information.

The PTP Multicast TTL is user configured in a range from 1 to 255. For a local area network the TTL should be configured to 1.

PTP Clock Class one of SYNCHRONIZED, HOLDOVER, or UNLOCKED. The Clock Class is SYNCHRONIZED when the GPS Subsystem TFOM level is 3 or 4 (see ***Appendix A - TFOM***). The Clock Class is HOLDOVER when the GPS Subsystem TFOM level is greater than 4 and less than 9. The Clock Class is UNLOCKED when the GPS Subsystem TFOM level is 9.

The PTP Timescale either PTP or ARB. When Time Mode is configured to PTP the clock transmits the Timescale as PTP. When the Time mode is UTC the clock transmits the Timescale as ARB.
The PTP Port State is one of MASTER, PASSIVE or LISTENING. The PTP Port State is selected as MASTER by the best master clock algorithm, otherwise it is PASSIVE or LISTENING.

The PTP Clock Source is either GPS or OSC. The Clock Source is GPS if the Clock Class is Synchronized, otherwise it is OSC based on the system oscillator.

The PTP UTC Offset is the offset between TAI and UTC in units of seconds.

The PTP UTC Offset Valid is either TRUE or FALSE. The UTC Offset Valid is TRUE if the current UTC Offset is known to be correct, otherwise it is FALSE.

The PTP Clock Accuracy is transmitted when the time is accurate to within the following:

25ns	Clock is synchronized or in holdover, PTP clock < 25 nanoseconds
100ns	Clock is synchronized or in holdover, PTP clock < 100 nanoseconds
250ns	Clock is synchronized or in holdover, PTP clock < 250 nanoseconds
1us	Clock is synchronized or in holdover, PTP clock < 1 microsecond
2.5us	Clock is synchronized or in holdover, PTP clock < 2.5 microseconds
10us	Clock is synchronized or in holdover, PTP clock < 10 microseconds
25us	Clock is synchronized or in holdover, PTP clock < 25 microseconds
100us	Clock is synchronized or in holdover, PTP clock < 100 microseconds
250us	Clock is synchronized or in holdover, PTP clock < 250 microseconds
1ms	Clock is synchronized or in holdover, PTP clock < 1 millisecond
2.5ms	Clock is synchronized or in holdover, PTP clock < 2.5 milliseconds
10ms	Clock is synchronized or in holdover, PTP clock < 10 milliseconds
Unknown	Clock is unsynchronized, TFOM = 9

The PTP Leap 59 second indicator is either TRUE or FALSE. The Leap 59 is TRUE if the PTP Timescale is PTP and the last minute of the current UTC day contains 59 seconds, otherwise it is FALSE.

The PTP Leap 61 second indicator is either TRUE or FALSE. The Leap 61 is TRUE if the PTP Timescale is PTP and the last minute of the current UTC day contains 61 seconds, otherwise it is FALSE.

The PTP Time Traceable indicator is either TRUE or FALSE. The Time Traceable is TRUE if the Time Scale is PTP and the Clock Class is Synchronized or Holdover, otherwise it is FALSE.

The PTP Frequency Traceable indicator is either TRUE or FALSE. The Frequency Traceable is TRUE if the Time Traceable is TRUE, otherwise it is FALSE.

The PTP Transmission Mode is either Multicast or Hybrid. Multicast Mode is the default and is defined in the IEEE-1588 standard. All packets sent from the Grandmaster are Multicast. Hybrid Mode

uses Multicast and Unicast. In this mode, delay response messages are sent Unicast in response to the slave delay request. NOTE: Unicast messages are only sent when the Delay Mechanism is configured to E2E.

About the PTP Second and UTC Time

The PTP Time Mode selections are PTP and UTC. The IEEE-1588 standard defines the PTP epoch beginning at 0 hours on 1 January 1970. The time measured since this epoch is designated in the standard as PTP seconds. The PTP second is monotonic so does not include leap seconds.

Unlike PTP, the UTC second is not monotonic, that is, from time-to-time there will be leap second insertions. The last second of a leap insertion day is 23:59:60 making the day one second longer than a normal day ending at 23:59:59.

PTP Second

When the PTP Time Mode is set to PTP, the slave clocks must utilize the current leap second and leap second pending flags (leap_59 or leap_61) to convert the PTP second to UTC.

UTC Time

When the PTP Time Mode is set to UTC, then there will be a one second jump in time when a leap second insertion occurs. If the PTP slave does not account for this, it will also jump. Avoid this by using PTP Time Mode.

Multiport PTP

When only one PTP option is enabled it will be configured for `eth0` PTP Domain 0. If a second PTP option is enabled then it will be configured for `eth1` PTP Domain 1. This configuration will allow PTP to run as master on both ports.

If the PTP Domain is configured as the same value for both ports (for example, PTP Domain 0 on `eth0` and PTP Domain 0 on `eth1`) then `eth0` Port State will be master and `eth1` Port State will be listening.

Disable the PTP Protocol

The instructions below assume that the PTP Option has been installed on Port 0 (`eth0`) of your Sonoma. To check, see the section titled ***Option*** at the beginning of this chapter.

To disable the Precision Time Protocol on Port 0 issue the following command:

```
chmod -x /etc/rc.d/rc.ptpd0
```

Copy the *rc.ptpd0* file to the non-volatile FLASH area like this:

```
cp -p /etc/rc.d/rc.ptpd0 /boot/etc/rc.d
```

Then:

```
reboot
```

Once PTP has been disabled, the user interface will no longer show the existence of PTP.

Re-Enable PTP

To re-enable PTP on Port 0, remove the *rc.ptpd0* file from the */etc/rc.d* directory as shown below:

```
rm /boot/etc/rc.d/rc.ptpd0
```

Then:

```
reboot
```

NOTE

If PTP is also installed on Port 1, then follow the instructions above using ***rc.ptpd1***.

Chapter *Five*

Security

Your Sonoma incorporates several important security features to prevent unauthorized tampering with its operation. Many of these are standard multiple-user access control features of the underlying Linux operating system which controls the Sonoma. Others are provided by the additional protocol servers selected for inclusion in your Sonoma, and the way that they are configured.
https://endruntechnologies.com/pdf/Time-Server-Security-Best-Practices.pdf

Secure user authentication and session privacy while performing routine monitoring and maintenance tasks are provided by the OpenSSH implementations of the "secure shell" daemon, `sshd` and its companion "secure copy" utility, `scp`. The Apache implementation of the Hyper Text Transport Protocol (HTTP) with Transport Layer Security (TLS) daemon (`httpd`) provides for a secure, encrypted session with a digital certificate. The NET-SNMP implementation of the Simple Network Management Protocol (SNMP) daemon, `snmpd` conforms to the latest Internet standard, known as SNMPv3, which also supports secure user authentication and session privacy. In addition, the Network Time Protocol daemon, `ntpd` supports client-server authentication security measures to deter spoofing of NTP clients by rogue NTP servers. This chapter describes these security measures and gives the advanced network administrator information that will allow custom configuration to fit specific security needs, including RADIUS, TACACS+, LDAP.

IMPORTANT

SSH and SNMP are enabled with default passwords. To ensure security, change the passwords or disable the protocols. To change the passwords for SSH and HTTP use the `passwd` command. To change the passwords/community strings for SNMP see ***Chapter 6 - SNMP***.

By default all hosts are allowed access via SSH and SNMP. To restrict access via these protocols to specific hosts, see ***Restrict Access - SSH and SNMP*** below. All hosts are allowed access via HTTP as well. To restrict access via HTTP, see ***Restrict Access - HTTP*** below.

To completely disable any or all of these protocols see ***Disable Protocols*** below.

Linux Operating System

The Linux operating system versions are shown in ***Appendix H - Specifications***. Linux supports a complete set of security provisions:

- System passwords are kept in an encrypted file, */etc/shadow* which is not accessible by users other than *root*.

- Direct *root* logins are only permitted on the local USB port or via SSH.

- The secure copy utility, **scp**, is used for transferring program updates to the Sonoma.

- HTTPS access, (when enabled) is supported for system monitoring, is allowed only via TLS, so passwords and session data are encrypted on the wire. Access via HTTPS is disabled by default. See ***Restrict Access - HTTPS*** and ***Disable SNMP, SSH and enable HTTPS*** below.

- SNMP access for system monitoring only, is configurable to provide the security of the latest version 3 Internet standard which supports both view-based access control and user-based security using modern encryption techniques. Previous versions v1 and v2c supported access control essentially via passwords transmitted over the network in plain text. Refer to ***Chapter 6 - SNMP*** and ***Restrict Access -SSH and SNMP*** (below) for details. SNMP may also be completely disabled. See ***Disable SNMP, SSH and HTTPS*** below.

- Individual host access to protocol server daemons **snmpd** or **sshd** are controlled by directives contained in the files */etc/hosts.allow* and */etc/hosts.deny*, which are configured using the interactive script **accessconfig.** See ***Restrict Access - SSH and SNMP*** below.

Restrict Access

The following paragraphs describe how to restrict SNMP, SSH, and HTTPS access to specific hosts. Also described is how to restrict NTP query access.

Restrict Access - SSH and SNMP

By default, the Sonoma is configured to allow access by all users via SSH and SNMP. To ensure security and to protect against denial-of-service attacks, you should restrict access by using the **accessconfig** command.

accessconfig modifies two files, */etc/hosts.allow* and */etc/hosts.deny*, which are used by **tcpd** and the standalone daemons, **snmpd** and **sshd**, to determine whether or not to grant access to a requesting host. These two files may contain configuration information for a number of protocol servers, but in the Sonoma only access control to the protocol server daemons **sshd** and **snmpd** is configured.

As shipped from the factory, these two files are empty. When you run **accessconfig**, these lines are added to the */etc/hosts.deny* file:

```
sshd:  ALL
snmpd:  ALL
```

This tells **tcpd** to deny access to **sshd** and **snmpd** to all hosts not listed in the */etc/hosts.allow* file. The **snmpd** and **sshd** daemons also parse this file directly prior to granting access to a requesting host.

Next you will be prompted to enter a list of hosts that will be granted access to **sshd** and **snmpd**. These appear in the */etc/hosts.allow* as lines like this:

```
sshd:  192.168.1.2, 192.168.1.3
snmpd:  192.168.1.2, 192.168.1.3
```

This simple shell script handles the needs of most users, however the syntax of these two files supports elaborate configuration possibilities which are beyond the capabilites of this simple shell script. Advanced users who need these capabilities will need to edit these two files directly and then copy them to the */boot/etc* directory. (See ***Appendix C - Helpful Linux Information, Using Editors***.) Be careful to maintain the proper ownership and access permissions by using **cp -p** when copying the files.

Restrict Access - HTTPS

To control access via HTTPS, you must edit the */etc/httpd/httpd.conf* file and add the equivalent deny followed by allow directives. For example, the default file contains these lines:

```
<Directory "srv/httpd/cgi-bin">
  AllowOverride None
  Options None
  Require all granted
</Directory>
```

To complete the configuration steps to restrict access and allow a specific host with IP address xxx.xxx.xxx.xxx, you would modify the directives as follows:

```
<Directory "srv/httpd/cgi-bin">
  AllowOverride None
  Options None
  Require ip xxx.xxx.xxx.xxx
# Require all granted
</Directory>
```

After making and saving your changes, you must copy the edited file to the non-volatile FLASH area and reboot the unit:

```
cp -p /etc/httpd/httpd.conf /boot/etc/httpd
reboot
```

Restrict Query Access - NTP

The Network Time Protocol (NTP) implementation in the Sonoma is built from the reference distribution from:

ntp.org

By factory default, remote control and query of the NTP daemon `ntpd` is disabled. Query-only operation is supported only from processes running on the Sonoma itself, i.e. from the *localhost*. This restricts access to `ntpd` from remote hosts using either of the two NTP companion utilities `ntpq` and `ntpdc`.

Control via these two utilities is disabled in the */etc/ntp.conf* file in two ways. First, MD5 authentication keys are not defined for control operation via a *requestkey* or *controlkey* declaration. Second, this default address restriction line is present in the file:

```
restrict default nomodify noquery nopeer
restrict 127.0.0.1 nomodify
restrict 0::1 nomodify
```

The first line eliminates control and query access from ALL hosts. The second and third lines disable the localhost from making any modifications to the `ntpd` daemon, but query access is not affected by this restriction. These lines must not be removed, as they are necessary for various monitoring processes running on the Sonoma to function properly.

Knowledgable NTP users who would like to customize the security aspects of the configuration of the NTP daemon in the Sonoma should edit the */etc/ntp.conf* file directly and then copy it to the */boot/etc* directory. Be sure to retain the ownership and permissions of the original file by using `cp -p` when performing the copy.

CAUTION

If you are planning to make changes to the ***/etc/ntp.conf*** file, you must NOT restrict query access from the local host to the NTP daemon. Various system monitoring processes running on the system require this access.

An example follows which shows how to allow query access from a specific remote host with IP address 192.168.1.10 while also allowing processes running on the Sonoma to have query access as well:

```
restrict default noquery nomodify nopeer
restrict 127.0.0.1 nomodify
restrict 0::1 nomodify
restrict 192.168.1.10 nomodify
```

Enabling and Disabling Protocols

See below for instructions on how to completely disable the following protocols: SSH, SNMP, and how to enable HTTPS. See ***Chapter 4 - PTP/IEEE-1588 Option*** for how to disable PTP. The Network Time Protocol (NTP) cannot be disabled.

Disable SNMP and SSH

To disable SNMP, SSH, you only have to modify the file mode of the scripts that control their execution. These are located in the */etc/rc.d* directory. To disable any of these daemons, issue one or more of these commands:

```
chmod -x /etc/rc.d/rc.snmpd
chmod -x /etc/rc.d/rc.sshd
```

After issuing these commands, you must copy the modified file(s) to the non-volatile FLASH area using one or more of these commands:

```
cp -p /etc/rc.d/rc.snmpd /boot/etc/rc.d
cp -p /etc/rc.d/rc.sshd /boot/etc/rc.d
cp -p /etc/rc.d/rc.httpd /boot/etc/rc.d
```

Enable HTTPS

Since the factory default for HTTPS is disabled, you will need to execute these commands to enable it:

```
chmod +x /etc/rc.d/rc.httpd
cp -p /etc/rc.d/rc.httpd /boot/etc/rc.d
```

Re-boot the Sonoma when done for the changes to take effect.

Enable LDAP

Since the factory default for LDAP is disabled, you will need to execute these commands to enable it:

```
chmod +x /etc/rc.d/rc.nss-pam-ldap
cp -p /etc/rc.d/rc.nss-pam-ldap  /boot/etc/rc.d
```

Re-boot the Sonoma when done for the changes to take effect.

IMPORTANT

After modifying ***/etc/rc.d/rc.snmpd, rc.sshd or rc.httpd***, you must copy them to the ***/boot/etc/rc.d*** directory and reboot the system. It is very important to use the `-p` when performing the copy. During the boot process, the files contained in the ***/boot/etc/rc.d*** directory are copied to the working ***/etc/rc.d*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Re-Enable SNMP, SSH

If you have disabled SNMP, SSH and you want to re-enable it, all you need to do is remove the *rc* file from the */boot/etc/rc.d* directory using one or more of these commands:

```
rm /boot/etc/rc.d/rc.snmpd
rm /boot/etc/rc.d/rc.sshd
```

Re-boot the Sonoma when done for the changes to take effect.

Disable HTTPS

To disable HTTPS after it was enabled issue this commands:

```
rm /boot/etc/rc.d/ rc.httpd
```

Re-boot the Sonoma when done for the changes to take effect.

Disable LDAP

To disable LDAP after it was enabled issue this commands:

```
rm /boot/etc/rc.d /rc.nss-pam-ldap
```

Re-boot the Sonoma when done for the changes to take effect.

Is the Protocol Disabled?

SNMP, SSH and HTTPS: To determine if one of these protocols is disabled or enabled, issue the following command:

```
ls -l /boot/etc/rc.d
```

If you see one of the following files listed, and there is NOT an '*' after the file name, then the corresponding protocol is disabled:

```
-rw-r--r-- 1 root root 1144 Feb 19 01:52 rc.httpd
-rw-r--r-- 1 root root 1168 Oct 26 2012  rc.snmpd
-rw-r--r-- 1 root root 2684 Feb 18 02:16 rc.sshd
```

If rc.httpd, rc.snmp, or rc.ssh is not listed, or it is listed and there is an '*' after the file name, then the protocol is enabled. Here is an example:

```
-rwxr-xr-x 1 root root 1168 Oct 26 2012  rc.snmpd*
```

OpenSSH

The secure shell protocol server running in the Sonoma is based on the portable OpenSSH for Linux. As such it supports both SSH1 and SSH2 protocol versions. By default, only SSH2 is enabled in the Sonoma due to security issues with SSH1. For more information about OpenSSH, and to obtain client software, refer to the OpenSSH website:

openssh.com

An excellent book which describes operation and configuration of the various SSH implementations, including OpenSSH is:

SSH, The Secure Shell, Barrett & Silverman, O'Reilley & Associates, 2001.

NOTE: To disable the SSH protocol see ***Disable SNMP, SSH and HTTPS*** above. To restrict access see ***Restrict Access, SSH and SNMP*** above.

Configure Keys

On initial boot-up from out-of-the-box, the SSH start-up script, */etc/rc.d/rc.sshd*, will detect that no keys are present in the */etc/ssh* directory. It will call **`ssh-keygen`** to generate a set of host keys and then it will copy them to the */boot/etc/ssh* directory. These will be copied to */etc/ssh* during each boot up. A complete set of security keys for both SSH1 and SSH2 versions of the protocol are generated. RSA keys are supported by both versions, and DSA keys are supported when using the SSH2 version. Should you need to replace your keys at any time, you can just remove the keys from the */boot/etc/ssh* directory and then reboot the Sonoma. A new set of host keys will automatically be generated.

To configure root logins to your Sonoma via passwordless, public key authentication, you must generate a public/private pair of SSH2 keys using your own ssh key generating utility, or you can use the **`ssh-keygen`** that is resident on the Sonoma file system. You must then append the public key to the

/boot/root/.ssh/authorized_keys file in the non-volatile FLASH area on your Sonoma. At boot time, the Sonoma will copy these to the actual working */root/.ssh* directory of the system ramdisk. To use this capability, the corresponding private key must reside in the */root/.ssh* directory of your remote computer as *id_rsa* or *id_dsa*. If you are unfamiliar with this process, refer to the man page for the **`ssh-keygen`** utility for details (issue **`man ssh-keygen`** at the prompt). (Be careful to maintain the proper ownership and access permissions of the private key by using **`cp -p`** when copying the file. It MUST be readable only by *root*.)

Advanced users wishing to modify the overall configuration of the **`sshd`** daemon should edit the */etc/ssh/sshd_config* file and then copy it to the */boot/etc/ssh* directory of the Sonoma. Be careful to maintain the proper ownership and access permissions by using **`cp -p`** when copying the file. At boot time, it will be copied to the */etc/ssh* directory of the system ramdisk, thereby replacing the factory default configuration file.

HTTPS

The HTTPS server in the Sonoma is built from the standard Apache version 2.4.62 distribution from:

httpd.apache.org

It uses HTTPS (HTTP over TLS) with mod_ssl (the Apache interface to OpenSSL). For more information about this protocol, refer to:

modssl.org

NOTE: To enable the HTTPS protocol see ***Enabling and Disabling Protocols*** above. To restrict access see ***Restrict Access - HTTPS*** above.

HTTP and TLS use files for the default configuration located in */etc/httpd*. Of these, you will typically only need to modify *httpd.conf*. Advanced users who need to modify the default configuration will need to edit the file and copy it to the */boot/etc/httpd* directory. Do not attempt to change the directives unless you have a real need to do so. (See ***Appendix C - Helpful Linux Information, Text Editors***.)

Configure Certificate and Key

For TLS it is recommended, but not required, that new certificates and keys are generated and installed on the Apache web server with mod_ssl. The factory configured, self-signed certificate is located in */etc/httpd/server.crt*, and the key in*/etc/httpd/server.key*. After creating new certificates and private keys, they will need to be saved in */boot/etc/httpd/server.crt* and */boot/etc/httpd/server.key*. To generate a new certificate and key, issue these commands:

```
cd /boot/etc/httpd
openssl req -new -x509 -nodes -out server.crt -keyout server.key
```

The two files will be created in the */boot/etc/httpd* directory. You must reboot the Sonoma for them to take effect. An excellent book which describes operation and configuration of the various HTTPS directives and TLS configuration is:

Professional Apache, Wainwright, Wrox Press, 1999.

NTP

You can configure your NTP clients for secure MD5 authentication. See ***Chapter 3 - NTP, Unix-like Platforms: MD5 or SHA1 Authenticated NTP Client Setup*** or ***Chapter 3 - NTP, Windows: MD5 or SHA1 Authenticated NTP Client Setup***. You can also restrict NTP query access. See ***Restrict Query Access - NTP*** in this chapter.

PAM (Pluggable Authentication Modules)

The /etc/pam.d/sshd is the configuration file checked by PAM for all incoming ssh connections, it is where a user sets the order and rules for checking credentials for LDAP, TACACS+, RADIUS.

Remote Access Dial In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are two security protocols in Sonoma that provide centralized access. RADIUS and TACACS+ are used to authenticate and log remote network users to Sonoma. Both protocols provide centralized Authentication, Authorization, and Accounting (AAA) management for Sonoma.
The Radius implementation in the Sonoma is based on the distribution at this website:
Radius (PAM module via this source: https://github.com/FreeRADIUS/pam_radius)

The TACACS+ implementation in the Sonoma is based on the distribution at this website:
TACACS+ (PAM module via this source: https://github.com/kravietz/pam_tacplus)

Lightweight Directory Access Protocol (LDAP) is used to access and manage directory information on Sonoma. It reads and edits directory information on your Sonoma , such as user names, passwords, public keys, and configuration.
The LDAP implementation in the Sonoma is built into the current Slackware Linux root file system.

RADIUS

The PAM to RADIUS authentication module allows the Sonoma to become a RADIUS client for authentication. You will need to supply your own RADIUS server to perform the actual authentication.
Edit RADIUS Files
You must edit the following configuration files: (See Appendix C – Helpful Linux Information for information on a simple editor.)

- */etc/radius_auth.conf*
- */etc/pam.d/sshd*

After making the changes, you must copy the edited files and copy it to the non-volatile FLASH partition and reboot the unit with the following commands:

```
cp -p /etc/radius_auth.conf /boot/etc
cp -p /etc/pam.d/sshd /boot/etc/pam.d
reboot
```

TACACS+

The TACACS+ authentication module allows the Sonoma to become a TACACS+ client for authentication. You will need to supply your own TACACS+ server to perform the actual authentication.

Edit TACACS+ Files
You must edit the following configuration file: (See Appendix C – Helpful Linux Information for information on a simple editor.)

- */etc/pam.d/sshd*

After making the changes, you must copy the edited file and copy it to the non-volatile FLASH partition and reboot the unit with the following commands:

```
cp -p /etc/pam.d/sshd /boot/etc/pam.d

reboot
```

LDAP

The LDAP module allows the Sonoma to become a LDAP client. You will need to supply your own LDAP server.

Edit LDAP Files
You must edit the following configuration files: (See Appendix C – Helpful Linux Information for information on a simple editor.)

```
/etc/nsswitch.conf
/etc/nscd.conf
/etc/nslcd.conf
/etc/rc.d/rc.nss-pam-ldap
/etc/pam.d/sshd
```

Enable LDAP

Since the factory default for LDAP is disabled, see **Enabling and Disabling Protocols**.

After making the changes, you must copy the edited files and copy it to the non-volatile FLASH partition and reboot the unit with the following commands.

```
cp -p /etc/nsswitch.conf  /boot/etc/
cp -p /etc/nscd.conf /boot/etc/
cp -p /etc/nslcd.conf  /boot/etc/
cp -p /etc/pam.d/sshd/ /boot/pam.d

reboot
```

Network Security Vulnerabilities

EndRun addresses major network security vulnerabilities that affect Sonoma at the top of this webpage:

endruntechnologies.com/fsb.htm

This Application Note describes best practices to secure your time server and mitigate many network security vulnerabilities:

endruntechnologies.com/pdf/A

This page intentionally left blank.

Chapter *Six*

Simple Network Management Protocol (SNMP)

Your Sonoma includes the NET-SNMP version 5.9.4 implementation of an SNMP agent, `snmpd`*, and a SNMP notification/trap generation utility,* `snmptrap`*. It supports all versions of the protocol in use today: SNMPv1 (the original Internet standard), SNMPv2c (never reached standard status, often called "community SNMP") and SNMPv3 (the latest Internet standard).*

The NET-SNMP project has its roots in the Carnegie-Mellon University SNMP implementation. For more detailed information about the NET-SNMP project and to obtain management software and detailed configuration information, you can visit this website:

net-snmp.org

An excellent book which describes operation and configuration of various SNMP managers and agents, including the NET-SNMP implementations, is available from O'Reilley & Associates:

Essential SNMP, Mauro & Schmidt, O'Reilley & Associates, 2001

If you are planning to operate with SNMPv3, it is highly recommended that you make use of both of these resources to familiarize yourself with the agent configuration concepts.

SNMPv3 Security

Prior to SNMPv3, SNMP had definite security inadequacies due to using two community names in a manner analogous to passwords that were transmitted over the network as clear text. In addition, since no mechanism existed for authenticating or encrypting session data, any number of man-in-the-middle data corruption/replacement exploits were possible in addition to plain old snooping to learn the community names. SNMPv3 implements the User-based Security Model (USM) defined in RFC-2274 which employs modern cryptographic technologies to both authenticate multiple users and to encrypt their session data for privacy, much in the same way that SSH does for remote login shell users.

In addition, it implements the View-based Access Control Model (VACM) defined in RFC-2275. This RFC defines mechanisms for limiting the access of multiple users having various security levels (no authentication, authentication or authentication plus privacy) to specific "views" of the Structure of Management Information (SMI) object tree.

Enterprise Management Information Base (MIB)

In addition to providing the SNMP variables contained in MIB-II as described in RFC-1213, EndRun Technologies has implemented an enterprise MIB using the syntax of the SMI version 2 (SMIv2) as described in RFC-2578. Your Sonoma will have one of the two MIBs listed below:

SONOMA2-MIB

Which is located on your Sonoma in this ASCII file:

/usr/local/share/snmp/mibs/SONOMA2-MIB.txt

In addition to a complete set of NTP and GPS Receiver status objects, the MIB defines four SMIv2 notification objects:

- NTP Leap Indicator Bits status change
- NTP Stratum change
- Receiver Fault Status change
- Receiver Time Figure of Merit change

Invocation of the SNMP daemon

The SNMP daemon, **`snmpd`** is started from the */etc/rc.d/rc.snmpd* system start-up script. By default, it will listen on port 161 for SNMP queries from the network management system. If you would like to have it listen on another port, you could edit the file and change the port number in the argument list being passed to **`snmpd`** when it is started.

IMPORTANT

After modifying ***/etc/rc.d/rc.snmpd***, you must copy it to the ***/boot/etc/rc.d*** directory and reboot the system. It is very important to retain the access mode for the file, so be sure to use `cp -p` when performing the copy. During the boot process, the files contained in the ***/boot/etc/rc.d*** directory are copied to the working ***/etc/rc.d*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Quick Start Configuration -- SNMPv1/v2c

You should be able to compile the MIB file on your SNMP management system and access the variables defined therein. The factory default community names are “Sonoma” for the read-only community and “endrun_1” for the read-write community. This is all that is required for operation under v1 and v2c of SNMP.

Change Default Community Strings (Passwords)

You can, and should, change the default community names by editing */etc/snmpd.conf* and modifying these two lines:

```
rwcommunity  endrun_1
rocommunity  Sonoma
```

Configuring SNMPv1 Trap Generation

To have your Sonoma send SNMPv1 traps (RFC-1215) you must configure the community and desnation for SNMPv1 traps by uncommenting and editing this line in */etc/snmpd.conf*:

```
trapsink    xxx.xxx.xxx.xxx trapcommunity trapport
```

where **`trapcommunity`** should be replaced by your community, and **`xxx.xxx.xxx.xxx`** is the IP address or hostname of the destination host for receiving the traps generated by the Sonoma. By default, the trap will be sent to port 162. You may optionally add another parameter, **`trapport`** to the end of the above line to override the default port setting. Otherwise leave it blank.

Note: Though the agent will recognize multiple **`trapsink`** lines within */etc/snmpd.conf* and send the generic SNMP coldStart or authenticationFailure traps to multiple destinations, the Sonoma enterprise MIB trap generation mechanism will only send a trap to the last declared **`trapsink`** in the file.

Configuring SNMPv2c Notifications and Informs

To have your Sonoma send SNMPv2c notifications (SMIv2, RFC-2578) or informs, you must config ure the communities and destinations by uncommenting and editing one or both of these lines in */etc/snmpd.conf*:

```
trap2sink    xxx.xxx.xxx.xxx trap2community trap2port
informsink   xxx.xxx.xxx.xxx informcommunity informport
```

where **`trap2community`** and **`informcommunity`** should be replaced by your communities, and **`xxx.xxx.xxx.xxx`** is the IP address or hostname of the destination host for receiving the notifications or informs generated by the Sonoma. By default, the v2c trap or inform will be sent to port 162. You may optionally add another parameter, **`trap2port`** or **`informport`** to the ends of the above lines to override the default port setting. Otherwise leave it blank.

Note: Though the **`snmpd`** agent will recognize multiple **`trap2sink`** or **`informsink`** lines within */etc/snmpd.conf* and send the generic SNMP coldStart or authenticationFailure notifications and informs to multiple destinations, the Sonoma enterprise MIB notification/inform generation mechanism will only send a notification to the last declared **`trap2sink,`** and an inform to the last declared **`informsink`** in the file.

IMPORTANT

After editing ***/etc/snmpd.conf***, you must copy it to the ***/boot/etc*** directory and reboot the system. It is very important to retain the access mode for the file (readable only by ***root***), so be sure to use `cp -p` when performing the copy. During the boot process, the files contained in the ***/boot/etc*** directory are copied to the working ***/etc*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Configuration of SNMPv3

If you are planning to use SNMPv3, you should definitely make use of the two resources mentioned previously (NET-SNMP website and *Essential SNMP*) and study them carefully. There are rather elaborate configuration options available when you are using v3. The instruction presented here will give you the flavor of the configuration but definitely not the full scope of possibilities. To access your Sonoma via v3 of SNMP, you will have to configure two files:

/etc/snmpd.conf
/boot/net-snmp/snmpd.conf

The first file contains static configuration parameters that the agent uses to control access and to determine where to send notifications/traps. Other aspects of the agent's operation are also configurable in this file, but you should not need to modify those. To use the SNMPv3 capabilities of the Sonoma, you must first set up user information and access limits for those users in */etc/snmpd.conf*. Uncomment and edit these two lines to define your v3 users and their access parameters:

```
rwuser root    priv .1
rouser ntpuser auth .1.3.6.1.4.1.13827
```

The first line defines a SNMPv3 read-write user *root* whose minimum security level will be authenticated and encrypted for privacy (choices are noauth, auth and priv), and who will have read-write access to the entire *iso(1)* branch of the SMI object tree. The second line defines a SNMPv3 read-only user *ntpuser* whose minimum security level will be authenticated but not encrypted, and who will have read-only access to the entire *iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).endRunTechnologiesMIB(13827)* branch of the SMI object tree. After adding the user lines to */etc/snmpd.conf*, copy it to the */boot/etc* directory using `cp -p`.

The second file is located on the non-volatile FLASH disk and is used by the SNMP agent to store "persistent data" that may be dynamic in nature. This may include the values of the MIB-II variables sysLocation, sysContact and sysName as well as any configured SNMPv3 user crypto keys. In order to use SNMPv3, you must configure user keys in this file for each SNMPv3 user that you have set up in */etc/snmpd.conf*. To do this, you must add lines to */boot/net-snmp/snmpd.conf* like these for each user:

```
createUser root    MD5 endrun_1 DES endrun_1
createUser ntpuser SHA Sonoma_0
```

The first line will cause the agent, `snmpd` to create a user *root* who may be authenticated via Message Digest Algorithm 5 (MD5) with password *endrun_1* and may use the Data Encryption Standard (DES) to encrypt the session data with passphrase *endrun_1*. The second line will cause a user *ntpuser* to be created who may be authenticated using the Secure Hash Algorithm (SHA) with password *Sonoma_0*. Passwords and passphrases must have a *minimum* of 8 characters, or you will not be able to be authenticated.

IMPORTANT

You must kill the `snmpd` daemon prior to editing, ***/boot/net-snmp/snmpd.conf***. Otherwise, the secret key creation may not complete properly. Issue the command `/etc/rc.d/rc.snmpd stop` to kill the `snmpd` daemon. You can verify that the `snmpd` daemon has been killed by issuing the `ps -e` command and verifying that it is not present.

After rebooting, the agent will read the */boot/net-snmp/snmpd.conf* configuration file and compute secret key(s) for each of the users and delete the `createUser` lines from the file. It will then write the secret key(s) to the file. These lines begin with the string, `usmUser`. In this way, un-encrypted passwords are not stored on the system.

IMPORTANT

To generate new keys, stop the `snmpd` process, delete the existing `usmUser` key lines from the file ***/boot/net-snmp/snmpd.conf*** and then add new `createUser` lines. Then reboot the system.

This example gives the simplest configuration to begin using SNMPv3 but doesn't make use of the full capabilities of the VACM in defining groups and views for fine-grained access control. The factory default */etc/snmpd.conf* file contains commented blocks of lines that can be uncommented to give you a basic configuration that uses the User-based Security Model (USM) described in RFC-2274 and the View-based Access Control Model (VACM) described in RFC-2275. The comments included in the file should help you in modifying it for your specific requirements.

Configuring SNMPv3 Notifications and Informs

If you have followed the steps in ***Configuration of SNMPv3*** (above), then you are almost ready to use SNMPv3 notifications and informs.

SNMPv3 uses the same `trap2sink` and `informsink` directives in */etc/snmpd.conf* as SNMPv2c. The difference being that `snmptrap` requires authorization and authentication information be provided to it when sending SNMPv3 notifications and/or informs. This additional information comes from the usmUser records in */boot/net-snmp/snmp.conf*. A usmUser record is a space delimited record on one line with the following fields:

Field#	Field Name	Field Value
1	usmUser	usmUser
2	usmStatus	[a number (most likely 1)]
3	userStorageType	[a number (most likely 3)]

4 engineID [0x followed by a number string/hash]
5 name [0x followed by a number string/hash]
6 secName [0x followed by a number string/hash]
7 cloneFrom [NULL, unless user was created from a clone]
8 authProtocol [a dotted number representing: MD5, SHA, ““]
9 authKey [0x followed by a number string/hash]
10 privProtocol [a dotted number representing: DES, AES, “ “]
11 privKey [0x followed by a number string/hash]
12 userPublicString [0x followed by a number string/hash]

`snmptrap` requires (depending on the level of security) the use of fields 4, 5, 8, 9, 10, and 11. Your SNMP management station(s) will need to be configured to handle these hashed values.

Additionally, in */etc/snmptraps.conf* you will need to change the setting for V3 to ON. Copy *snmptraps.conf* to */boot/etc/* after you have made those changes so settings will be saved through reboots with *cp -a snmptraps.conf /boot/etc/snmptraps.conf*.

You should leave V1V2C set to ON until you verify that you can receive SNMPv3 notifications/informs. Then you can change the value to OFF.

Example of usmUser Record

1	2	3	4	5	6	7	8
usmUser	userStatus	userStorageType	engineID	name	secName	cloneFrom	authProtocol
usmUser	1	3	0x80001f8880f06ffc1df80b5960	0x726f6f7400	0x726f6f7400	NULL	.1.3.6.1.6.3.10.1.1.2

9	10	11	12
authKey	privProtocol	privKey	userPublicString
0xea5285876964b7fc8bbef3e6c380f63f	.1.3.6.1.6.3.10.1.2.2	0xea5285876964b7fc8bbef3e6c380f63f	0x

The image above shows an example of a usmUser record, where the fields are:

Field# Example Field Value
5 & 6 hashed from the value *root*
8 MD5
9 hashed from the value *endrun_1*
10 DES
11 hashed from the value *endrun_1*

Disable or Restrict Access

To disable SNMP, see ***Chapter 5 - Security, Enable or Disable SNMP, SSH and HTTPS***. To restrict access to specific hosts see ***Chapter 5 - Security, Restrict Access - SSH and SNMP***.

Chapter *Seven*

Hyper Text Transport Protocol Secure (HTTPS)

This chapter briefly describes the HTTPS interface that resides on the Sonoma GPS Time Server. The HTTPS interface to the Sonoma is a fast and easy-to-use graphical interface that is compatible with your standard web browser. Simply point your browser to the IP address of the Sonoma and log in securely with HTTP over the Transport Layer Security (TLS). The HTTPS interface is disabled by default to strengthen security (to enable see the end of this chapter for instructions).

The HTTPS implementation in the Sonoma uses HTTP over TLS. TLS is a sublayer under standard HTTP. HTTPS enhances security because it encrypts and decrypts the requested and returned pages from the server, including any passwords which are transmitted.

The HTTPS implementation is built from the standard Apache/2.4.62 distribution from:

httpd.apache.org

See ***Chapter 5 - Security, HTTPS*** for information on changing the default HTTPS configuration and TLS certificate and key.

IMPORTANT

A domain name server IP address is required by the Apache web server. When using `netconfig` (see ***Chapter 9 - Console Port Control and Status***) to configure the TCP/IP parameters, be sure to configure a name server. Only one name server is required but two gives some redundancy. The HTTPS Interface will not operate properly if this is configured incorrectly.

HTTPS Interface Description

For security reasons the web pages on the Sonoma show status and configuration information only. You cannot change any operational settings, however you can perform upgrades to the Sonoma firmware, which is done with several security measures in place. To make other changes to the Sonoma you will need to use the command line interfact via either a network or USB port.

NOTE

When Sonoma is shipped from the factory, HTTPS is disabled. If you want to enable, see Chapter 5 -***Security, Enable or Disable Protocols***. We also recommend that you restrict access to specific IP addresses. See ***Restrict Access*** in this Chapter.

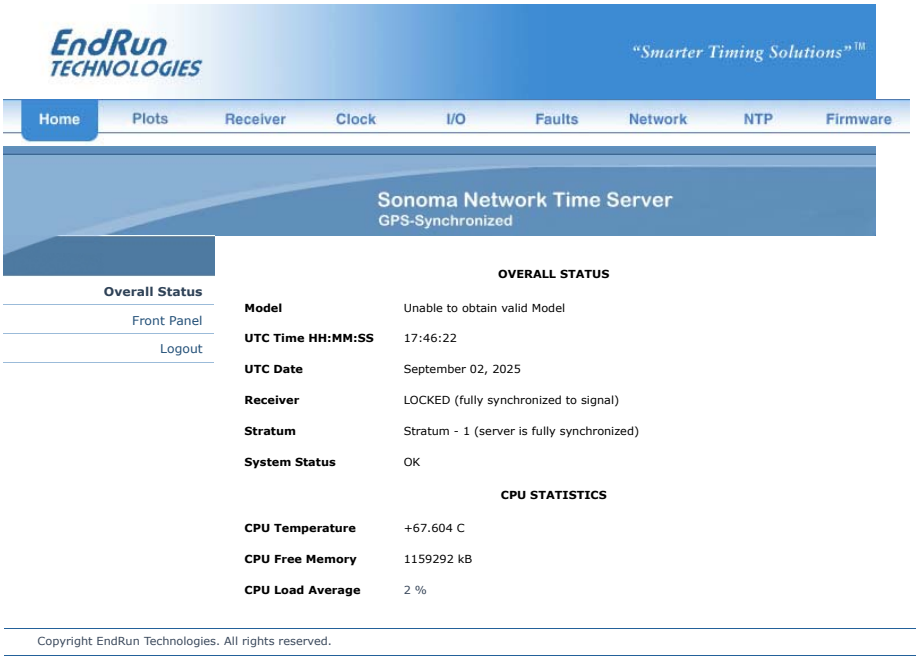
For proper operation, your web browser must be configured to allow pop-up windows.

To get started with the web interface simply point your browser to the IP address of the Sonoma and log in securely with HTTPS. Following are examples for IPv4 and IPv6:

IPv4: https://192.168.1.1
IPv6: https://[fe80:0:0:0:20e:f3ff:fe01:1f] Do not forget the brackets [].

A warning dialog page will be presented for the certificate. Acknowledge the dialog page and the server will continue to load, protected by TLS. To maximize security you should replace the TLS Certificate. See ***Chapter 5 - Security, HTTPS*** for details.

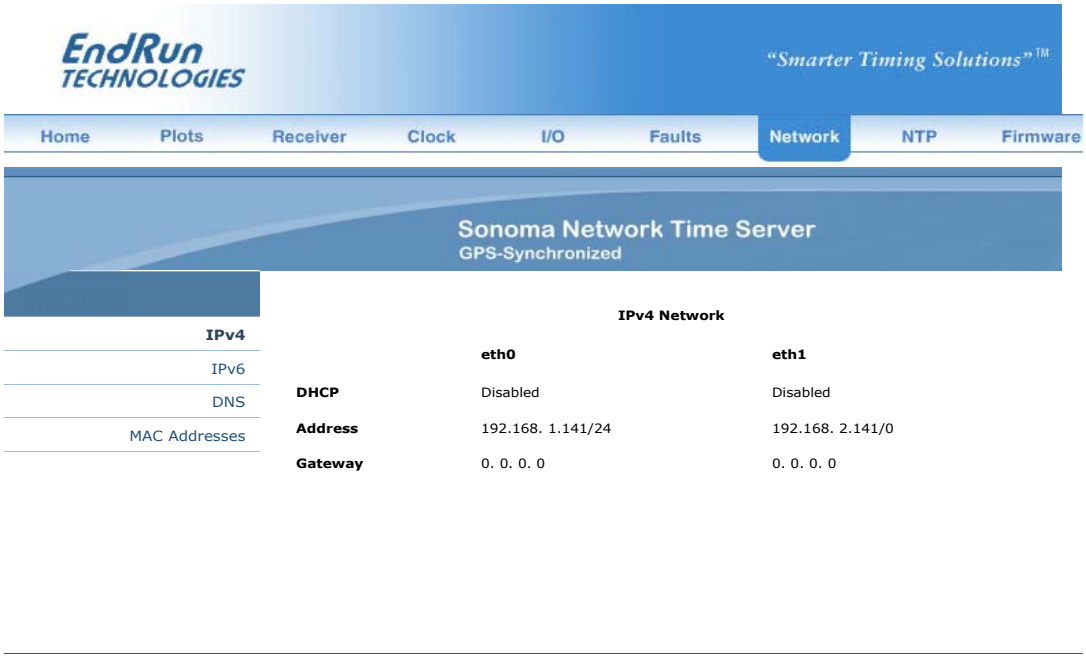
Below is a picture of the login page:



Navigation

The main menu tabs across the top of each webpage allow you to navigate through the status infomation in the Sonoma while links on the left side of each webpage provide subcategory navigation.

For example, in the page below the main menu tabs are: Home, Receiver, Plots, Clock, I/O, Faults, Network, NTP, PTP and Firmware. The subcategory links on this particular page are: IPv4, IPv6, DNS and MAC Address. IPv4 is selected. The tabs across the top and the left-side links are logically arranged for easy navigation.



Page Descriptions

Home: Overall Status Page

Data fields for this page are described below.

Overall Status

Model	Sonoma N22
Serial Number	Serial number of the Sonoma N22.
UTC Time, UTC Date	The current UTC date and time is shown. This date will show year 1980 if the time has not yet been acquired.
Receiver	This is the locked status of the GPS Subsystem/Receiver as follows: WRM: Warm up period for units with oscillator upgrades. ACQ: Acquiring. Searching for a signal. LKG: Locking to the GPS signal. LKD: Locked. Fully synchronized to signal.
Stratum	The NTP stratum field has these possible values: Stratum 1: The server is fully synchronized and accurate. Stratum 2: The server is synchronized to a Stratum 1 server. Stratum x: The server is synchronized to a Stratum x-1 server. Stratum 16: The server is unsynchronized. NTP clients will not use a Stratum 16 server.
System Status	This field indicates whether a system fault exists. Possible values are OK and FAULT. If it shows FAULT then go to the Faults Page to see which particular fault is the problem.

CPU Statistics

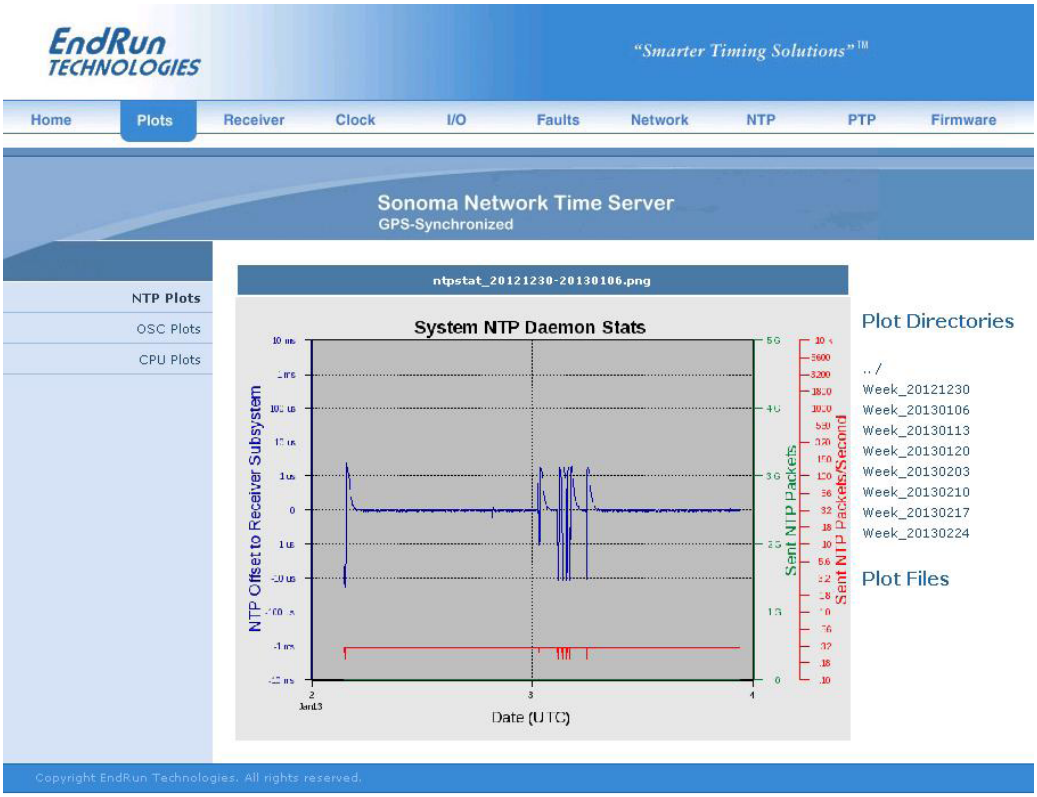
Current CPU temperature, CPU free memory and CPU load average are all shown.

Home: Logout

Clicking on this link will immediately log you out of the Sonoma HTTPS Interface.

Plots Page

Information available on this page are performance statistics related to NTP. Links on the right give access to the daily plot files - going back up to 10 years. Links on the left give access to performance statistics for CPU and Oscillator. A sample data plot is shown below:



There are four types of data plots available for viewing: CPU, NTP, Oscillator and Receiver. The large data plot shown on any of the plot pages is the last data plot viewed. This could be from any one of the four data types.

All plot files are kept in directories. There is one directory for each week. To choose a new plot to view, use the selections on the right side of the page. First, click to select a directory. Then you can either click to select one of the listed plot files, or you can use your mouse to hover over one of the plot files. Hovering over a plot file will display a small plot next to the large main plot. In this way you can compare plots from different types to correlate data. For example, you can compare an NTP data plot with a CPU data plot.

Plots files can also be downloaded from the Sonoma as .PNG files. They can be found in the directory */logs/png*.

Receiver: Receiver Page

This page contains information related to the GPS Subsystem/Receiver. Data fields are described below.

GPS Receiver Status

State — Shows the current state of the GPS Subsystem/Receiver:
- WRM: Warm up period for units with oscillator upgrades.
- ACQ: Acquiring. Searching for a signal.
- LKG: Locking to the GPS signal.
- LKD: Locked. Fully synchronized to signal.

TFOM — Shows the current TFOM value. See ***Appendix A - TFOM*** for more information.

Satellite ID — This field lists the satellites that are currently being tracked. Up to 12 may be tracked at a time. Click on the Satellite-Info link for details.

Average C/No — The carrier-to-noise ratio is an indicator of the GPS signal quality. This number typically ranges from 30 to 45 dB when the Sonoma is locked.

GPS Dynamic Mode — This field shows whether the dynamic mode is set or not. Dynamic mode should be OFF when the Sonoma is in a static (not moving) position. To change the dynamic mode setting use the **`gpsdynmode`** command.

WGS-84 Reference Position

Position Source — The source of the reference position can be:
- UNK: Unknown position.
- DYN: Dynamic. Position determined while in Dynamic Mode.
- USR: User-entered reference position.
- AVG: Average is a 24-hour average of GPS fixes.

To change the reference position source use the **`gpsrefpos`** command.

Latitude, Longitude, Height — The WGS-84 latitude and longitude in degrees, minutes and seconds format, and the height above the WGS-84 reference ellipsoid in meters is shown. Refer to ***Appendix D - Installing the GPS Antenna, About WGS-84***.

WGS-84 Last Position Fix

Latitude, Longitude, Height — These fields show information for the most recent position fix. The WGS-84 latitude and longitude in degrees, minutes, seconds format and the height above the WGS-84 reference ellipsoid in meters is shown. Refer to ***Appendix D - Installing the GPS Antenna, About WGS-84***.

GPS-UTC Almanac Info

These fields show the IS-GPS-200 almanac parameters which are used to relate GPS time to UTC.

LS, LSF — These fields contain the current leap second and future leap second values.

WNLSF, DN	These fields show the GPS week number and day number of week at the end of which the future leap second will take effect. This could be in the past if a leap second insertion has recently taken place. Leap second events typically occur every few years on either June 30 or December 31.
A0, A1, WNt, tot	These fields show the parameters for calculating the small residual offset between the GPS master clock ensemble and UTC-USNO. This is typically less than 10 nanoseconds.
Current (GPS-UTC)	This is the current value of the GPS-UTC offset, which includes leap seconds plus the small residual offset explained above. Time and date of most recently received satellite transmission containing this data is also shown.
Configuration	
Clock Calibration	Clock calibration is used to advance or retard the clock in order to correct for GPS Receiver delay and any propagation delay due to GPS antenna cable. It may also be used to compensate for the inherent time offsets that may exist with external hardware such as distribution amplifiers, etc. Calibration range is ±500,000 nanoseconds.

Receiver: Oscillator Page

This page shows system oscillator control information such as:

Oscillator Status	
Oscillator Type	This field shows the system oscillator type that is installed in the Sonoma. It will be either TCXO (standard), OCXO (option) or Rubidium (option).
DAC	The system oscillator control DAC value indicates the frequency control setting. The system automatically sets this value to remove frequency errors. Values may range from 0 to 1,048,575. Values close to the minimum or maximum will set the DAC fault flag.
Measured Time Error	This field shows the last measured time offset of the GPS Subsystem relative to GPS while locked, in second.
Time Deviation	This field shows the time deviation (TDEV) of the offset measurements in seconds. The tau associated with this measurement is one second, which is the update interval of the position fixes received from the GPS Receiver.
Oscillator Ageing Rate	This field shows the regression-computed system oscillator ageing rate per day (several-hours delay before the first measurements are displayed).
Control Loop TAU	This field shows the system oscillator control loop averaging time constant, in seconds. It's value is automatically adjusted to maintain optimum offset and stability.

Coast Duration	This shows the number of seconds the GPS Subsystem has been in coast mode, while the Sonoma is unlocked to GPS. Coast mode is another term for holdover mode.
Estimated Time Error	This is the estimated time error of the GPS Subsystem when in coast/holdover mode, in seconds.
Internal Chassis Temperature	Internal chassis temperature in °C. Available with OCXO or Rubidium oscillator.

Clock Page

This page shows the configuration of the Sonoma Time Server except for any optional I/O which is listed on the I/O page.

Clock Configuration

Time Mode This field shows the current time mode setting. Possible settings are UTC, GPS and Local. Since NTP always uses UTC, this setting only affects any optional Time Code or Serial Time outputs. To change the time mode setting use the `systimemodeconfig` command via the console port.

Time Zone Offset	This field shows the offset from UTC and is only valid when the Time Mode is Local. A positive Time Zone Offset implies a longitude east of the Greenwich meridian. To change the time zone use the `systimemodeconfig` command.
Daylight Savings Time	This field will show whether DST control is enabled or not. DST fields are only used when the Time Mode is Local.
DST Start, DST End	These fields will only display if the Daylight Savings Time field above shows enabled. If enabled, then these fields show when DST starts and ends during the year. For example, in most of the U.S.A. the DST Start Time is the 2nd Sunday in March at 2 a.m. The DST End Time is the 1st Sunday in November at 2 a.m. DST settings are used when the time mode is Local. To change the DST settings use the `systimemodeconfig` command.

I/O Page

This page shows any installed CPU Options and their settings. These are optional outputs that are generated from the CPU Module in the Sonoma. A basic Sonoma Time Server has no CPU Options installed. Use commands `cpuioconfig` and `sysioconfig` via the console port to change the settings of the CPU Options. See ***Chapter 10 - Options*** for information on the various options.

Faults: System Faults Page

This page lists all possible fault conditions of the Sonoma. For details on each fault see ***Appendix G - System Faults***.

Faults: Fault Mask Page

This page shows the fault masks available.

Fault Masks

Signal Fault	This field shows the current mask setting for the Signal Fault, either Masked or Enabled. When the signal fault is Masked it will prevent a Signal Loss Fault from occurring. Some installations may need to mask this fault when operating the Sonoma with no GPS signal. (An example of this would be when configured as a Stratum 2 NTP Server.) To change the Signal Fault Mask use the `setsigfltmask` command.
Antenna Fault	This field shows the current mask setting for the Antenna Fault. When the antenna fault is Masked it will prevent an Antenna Fault from occurring. Some installations may need to mask this fault due to special antenna situations like splitters. To change the Antenna Fault Mask use the `setantfltmask` command.
Primary and Secondary Power Fault Alarms	These fields will display ONLY if your Sonoma has the Dual Power Supply option installed. See ***Chapter 10 - Options, Masking Dual Power Supply Fault Alarms*** for more information.

Network: IPv4 Page

This page shows the IPv4 network configuration.

IPv4 Network Status

DHCP	By default, the Sonoma will configure itself using the Dynamic Host Configuration Protocol (DHCP). If you need to set up static IP configuration, you must use the `netconfig` command via the console port. The field will show whether DHCP is enabled or disabled.
Address, Gateway	These fields show the settings for the IP address in CIDR format and gateway.

Network: IPv6 Page

This page shows information related to the IPv6 network parameters. For more information on IPv6 see ***Chapter 8 - IPv6 Information***.

Network: DNS Page

This page shows the IP addresses of the primary and secondary domain name servers.

Network: MAC Address Page

This page shows the media-access-control (MAC) address for both ethernet ports (`eth0` and `eth1`).

NTP Page

The NTP Status page shows all information related to NTP operation.

NTP Status

Status	The stratum field has several possible values: Stratum 1: The server is fully synchronized and accurate. Stratum 2: The server is synchronized to a Stratum 1 server. Stratum x: The server is synchronized to a Stratum x-1 server. Stratum 16: The server is unsynchronized. NTP clients will not use a Stratum 16 server.
Source	This field will show the source of time which is usually GPS. If the Sonoma is configured as a Stratum 2 server then it will show the IP address of the upstream Stratum 1 server.
Offset	This field shows the offset in seconds between the NTP system clock and the GPS Subsystem clock. Positive implies that the NTP system clock is ahead of the GPS Subsystem clock.
Leap Indicator Bits	This field shows whether a leap second is pending. Leap seconds occur about every 1½ to 3 years. Possible indicator values are: 00: Normal, locked operation. 01: Leap second insertion will occur after 23:59:59 UTC. 11: Fault. Unsynchronized state.

I/O Statistics

Time Since Reset, Packets Sent/Received, Packets Sent Rate, Packets Dropped	These fields show statistics accumulated since the last reboot of the system.

PTP: Status and Configuration Pages

The fields on these pages show the status and the configuration for the optional PTP/IEEE-1588 protocol. If your Sonoma does not have PTP enabled then there will be no fields shown. For more information on PTP and an explanation of the data fields on this page see ***Chapter 4 - PTP/IEEE-1588***.

Firmware: Firmware Status Page

The firmware status page shows part numbers and revisions for Sonoma firmware.

Firmware Status

GPS Subsystem Firmware	This field shows the GPS Subsystem firmware version.
GPS Subsystem FPGA	This field shows the GPS Subsystem Field Programmable Gate Array (FPGA) version.

Firmware: GPS Subsystem Upgrade Page

This page is used for upgrading the firmware. You must be logged in as "root" in order to have access to these pages. The latest released versions of Sonoma firmware are freely available on the EndRun Technologies website. For detailed information on how to perform the upgrade either via the network port, the serial port, or the HTTPS interface see ***Appendix B - Upgrading The Firmware***.

Firmware: Reboot Page

This page will allow you to perform a software reboot of both the Linux Subsystem and the GPS Subsystem. This is normally used after a firmware upgrade but can be done anytime you wish to reset the Sonoma.

Disable or Restrict Access

To disable HTTPS, see ***Chapter 5 - Security, Enable or Disable SNMP, SSH and HTTPS***. To restrict access to specific hosts see ***Chapter 5 - Security, Restrict Access - HTTPS***.

This page left intentionally blank.

Chapter *Eight*

IPv6

The Sonoma Time Servers support IPv6 out-of-the-box. During network configuration, you have the option to disable IPv6 on either or both Ethernet ports. The IPv6 addressing scheme will see expanding deployment in the near future due to the fact that there are no longer any IPV4 addresses to be allocated in many regions of the world.

IPv6 Capabilities

The presence of an IPv6-capable kernel will automatically enable most of the IPv6 capabilities. By default, autoconfiguration of the Ethernet interfaces via IPv6 Router Advertisements is enabled. To disable acceptance of Router Advertisements, or to configure a static IPv6 address and default IPv6 gateway, and to configure IPv6 domain name servers, you must run the interactive **`netconfig`** script. Either method will allow you to configure your Ethernet interface for both IPv4 and IPv6 operation. Using the **`netconfig`** script has the advantage that you can also configure the hostname and domainname for the unit.

OpenSSH

By default, **`sshd`** is factory-configured to listen on both IPv4 and IPv6 addresses. It may be forced to listen on either IPv4 only, or IPv6 only by editing the */etc/ssh/sshd_config* file and modifying the **`AddressFamily`** directive, and then copying it to */boot/etc/ssh*. Refer to the *sshd_config* man page for detailed information (**`man sshd_config`**).

Apache HTTP

By default, **`httpd`** is factory-configured to listen on both IPv4 and IPv6 addresses. It may be forced to listen on either IPv4 only, or IPv6 only by editing the */etc/httpd/httpd.conf* configuration file and adding a **`Listen`** directive, and then copying it to */boot/etc/httpd*. Refer to the Apache HTTP documentation for details.

Net-SNMP

By default, **`snmpd`** is factory-configured to listen on both IPv4 and IPv6 addresses. This may be changed by editing */etc/rc.d/rc.snmpd* and modifying the agent address argument passed to **`snmpd`** at start-up, and then copying it to */boot/etc/rc.d*.

NTP

By default, `ntpd` is factory-configured to listen on both IPv4 and IPv6 addresses on all interfaces. This may be changed by editing */etc/ntp.conf* and adding the desired `interface` directives to achieve the desired behavior, and then copying it to */boot/etc*. For example, adding this line:

```
interface ignore ipv6
```

will cause ntpd to not bind to any IPv6 addresses. Refer to the NTP documentation for details on the `interface` directive.

IPv4-Only Protocols

There are several protocols running on the Sonoma which are not IPv6 capable: The Optional PTP/IEEE-1588 and `dhcpcd`. The address autoconfiguration capabilities of IPv6 along with the Neighbor Discovery Protocol (NDP) make the DHCP protocol less important in IPv6 networks.

Chapter *Nine*

Console Port Control and Status

This chapter describes the Sonoma control and status commands used via the Linux console. The console is accessed via any of the Ethernet ports or the USB port. The Sonoma supports several application-specific commands for configuration and for monitoring the performance and status of the Linux and GPS Subsystems.

You do not need knowledge of Linux commands in order to operate the Sonoma. However, the Sonoma does support a subset of the standard Linux commands and utilities and it uses the `bash` *shell, which is the Linux standard, full-featured shell. A wealth of information is available from a variety of other sources on Linux.*

The Sonoma-specific commands will be described in this chapter. For a brief description of some of the most useful Unix/Linux commands, see ***Appendix C - Helpful Linux Information****.*

Console Ports

Three interface ports are available on the Sonoma D22. Two are 100/1000Base-T Ethernet ports and one is a USB port. Network cables and a USB cable are provided with each Sonoma shipment. The USB cable can be used to connect the Sonoma to the USB port on your computer. Detailed specifications on the ports, including the USB port, are in ***Appendix H - Specifications***.

General Linux Operation

You do not need to know Linux in order to operate the Sonoma. However, for those interested, the command shell used by the Sonoma is the Linux standard: `bash`. All commands and file names are case sensitive, which is standard for Unix-like operating systems. For a brief description of some of the most useful Unix/Linux commands, see ***Appendix C - Helpful Linux Information***.

If you are unfamiliar with Unix-like operating systems, and you would like to be able to more closely monitor or optimize the performance of your Sonoma then you should consult good Linux reference books or the Linux Documentation Project at::

tldp.org

Available User Commands

COMMAND	FUNCTION
accessconfig	Interactive script that guides you in configuring `ssh` and `snmpd` access to the Sonoma that is limited to specific hosts. The resulting */etc/hosts.allow* and */etc/hosts.deny* files are saved to the non-volatile FLASH disk. Factory default configuration allows access by all hosts.
antfltmask	Prints the current setting for the Antenna Fault Mask. See the `setantfltmask` command.
caldelay	Prints the calibration delay. See the `setcaldelay` command.
cpuio *(optional)*	Returns the current settings for any installed, user-selectable, CPU Module options. See ***Chapter 10 - Options, CPU Module Options*** for more information.
cpuioconfig *(optional)*	An interactive utility that allows you to modify the settings for the CPU Module options. See ***Chapter 10 - Options, CPU Module Options*** for more information.
cpustat	Prints the current Linux CPU core temperature, system load as percent of maximum and free memory available.
faultstat	Prints the summary of all system fault states in a user-friendly format.
fitversion	Prints the FIT Image version.
get_sw_opts	Returns the current software options enabled in your Sonoma. See ***Chapter 10 - Options, Software Options*** for more information.
gpsdynmode	Prints the GPS dynamic mode currently in effect. See the `setgpsdynmode` command.
gpslastfix	Prints the last computed GPS position fix.
gpsrefpos	Prints the GPS reference position. See the `setgpsrefpos` command.
gpsstat	Prints the GPS Subsystem status information.
gpstrkstat	Prints the GPS satellite tracking status. Azimuth, elevation and signal level (C/No) are shown for each satellite.
gpsutcinfo	Prints the GPS UTC Almanac parameters per the GPS-IS-200. Also shows the current calculated GPS-UTC offset, which includes leap seconds and a small sub-second offset.
gpsversion	Prints the GPS Subsystem firmware and FPGA version information.
help help command	Prints help for all Sonoma-specific (not Linux) commands. Prints command-specific help. For example: `help gpsstat`.
inetdconfig	Interactive script that allows you to configure the list of protocol servers which are started by the `inetd` server daemon running in the Sonoma.
installed_sw_opts	Command to show which software options are enabled. See ***Chapter 10 - Options, Software Options*** for information.

kernelversion	Prints the Linux operating system kernel version.
netconfig	Interactive script that allows you to configure the IP network subsystem of the Sonoma.
ntpconfig	Interactive script that guides you in configuring the NTP Subsystem. Allows configuration of MD5 authentication and broadcast/multicast mode. All parameters are retained in non-volatile FLASH disk storage.
ntpstat	Prints the values of several key parameters indicating the status of the NTP daemon. These include the current offset between the NTP-steered system clock and the GPS Subsystem clock, and the current counts of received packets, sent packets and dropped packets. In addition the current sent packet rate is shown.
oscctrlstat	Prints the system oscillator disciplining parameters.
passwd	Used to change the password for the user that you are logged in as.
ptpconfig0 ptpconfig1 *(optional)*	Interactive script that guides you in configuring parameters for the optional PTP/IEEE-1588 protocol. See ***Chapter 4 - PTP/IEEE-1588*** for more information.
ptpstat0 ptpstat1 *(optional)*	Prints the status of the optional PTP/IEEE-1588 Subsystem. See ***Chapter 4 - PTP/IEEE-1588*** for more information.
pwrfltmask *(optional)*	Prints the current settings of the optional Dual Power Supply Input Fault Alarm Masks. See ***Chapter 10 - Options, Masking Dual Power Supply Fault Alarms*** for more information.
rcvrserialnumber	Prints the serial number of the GPS Receiver.
rcvrstat	Prints the status of the GPS Receiver.
rcvrversion	Prints the GPS Receiver firmware and FPGA version information.
resetlastgpswn	For use with a GPS simulator.
resetleaphistory	For use with a GPS simulator.
rcvrserialnumber	Prints the serial number of the GPS Receiver.
rcvrstat	Prints the status of the GPS Receiver.
rcvrversion	Prints the GPS Receiver firmware and FPGA version information.
resetlastgpswn	For use with a GPS simulator.
resetleaphistory	For use with a GPS simulator.
serialnumber	Prints the serial number of the Sonoma. *The serial number is not available using this command in units shipped before August 2015.*
setantfltmask	Command to enable or mask the Antenna Fault. See the `antfltmask` command.
setcaldelay	An interactive utility that allows you to change the clock calibration delay. See the `caldelay` command.

setgpsdynmode	Command to set the dynamic mode of operation of the GPS Subsystem. See the **`gpsdynmode`** command.
setgpsrefpos	Interactive utility that prompts you for an accurate reference position, performs syntax and argument validity checking then passes the position to the GPS Subsystem. See the **`gpsrefpos`** command.
setpwrfltmask *(optional)*	Command to enable or mask the optional Dual Power Supply Input Faults. See ***Chapter 10 - Options, Masking Dual Power Supply Fault Alarms*** for more information.
setsigfltmask	Command to enable or mask the Signal Loss Fault. See the **`sigfltmask`** command.
sigfltmask	Prints the current setting for the Signal Loss Fault mask. See the **`setsigfltmask`** command.
subsysreset	Command that performs a GPS Subsystem reset.
sysosctype	Prints the installed system oscillator type, which is one of TCXO, OCXO or Rubidium.
sysfit	Prints the currently loaded Linux root file system image, either 0 or 1, where 0 is the factory-installed FIT file system, and 1 is the upgraded FIT file system.
sysstat	Prints detailed NTP status information. Included is the offset of the NTP-steered system clock to the GPS Subsystem clock, the NTP daemon leap indicator bit values, the TFOM, the time of the most recent update and the current leap seconds value.
systemio *(optional)*	Returns the current settings for any installed, system options. See ***Chapter 10 - Options, CPU Module Options*** for more information.
systemioconfig *(optional)*	An interactive utility that allows you to modify the settings for the system options. See ***Chapter 10 - Options, CPU Module Options*** for more information.
systimemode	Prints the time mode settings in effect for the any optional Time Code or Serial Time output. See the **`systimemodeconfig`** command.
systimemodeconfig	Interactive utility that guides you in configuring the time mode settings for any optional Time Code or Serial Time output. Allows setting to the LOCAL, GPS or UTC timescale. See the **`systimemode`** command.
sysversion	Prints the Linux root file system version information.
updaterootflag	Command to update the flag stored in FLASH that is read by the Linux bootloader at boot time to select operation with either the factory-installed or upgraded root file system.
upgradefit	Command that performs the FIT Image upgrade process.
upgradercvr	Command that performs the GPS Receiver upgrade process.
upgradercvrfpga	Command that upgrades the FPGA resident on the GPS Receiver.
upgradercvr	Command that performs the GPS Receiver upgrade process.

upgradercvrfpga	Command that upgrades the FPGA resident on the GPS Receiver.
upgradesubsys	Command that performs the GPS Subsystem firmware upgrade process.
wrt_sw_opt	Command to enable a software option. See ***Chapter 10 - Options, Software Options*** for information.

Detailed Command Descriptions

accessconfig

This command starts an interactive script that will allow the root user to configure access limitation via **`ssh`** and **`snmp`** to the Sonoma. By default, the unit is configured to allow access by all users. If you need to limit **`ssh`** or **`snmp`** access, e.g. for security reasons, you must run this script as root from either the USB port or from a **`ssh`** session.

This script modifies these files: */etc/hosts.allow* and */etc/hosts.deny*. These are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot the Sonoma after running this script for the changes to take effect.

Command: **`accessconfig`**
Sonoma reply: Interactive script is started.

antfltmask

This command displays the current setting for the Antenna Fault Mask.

Command: **`antfltmask`**
Sonoma reply: **`Antenna Fault is ENABLED`**

caldelay

This command displays the current calibration delay setting. The allowable calibration delay range is ±500,000 nanoseconds.

Command: **`caldelay`**
Sonoma reply: **`+0 nanoseconds`**

cpuio (Optional)

See ***Chapter 10 - Options, CPU Module Options*** for information on this command.

cpuioconfig (Optional)

See ***Chapter 10 - Options, CPU Module Options*** for information on this command.

cpustat

This command shows a group of key values for monitoring the health of the Linux CPU and operating system status. The format is:

```
YYYYMMDD.HH:MM:SS LLL% FREEkB +TT.TC
```

Where:
YYYY is the year of the UTC timestamp of the most recent update.
MMDD is the month and day-of-month of the UTC timestamp of the most recent update.
HH:MM:SS is the hour, minute and second of the UTC timestamp of the most recent update.
LLL% is the percentage of maximum load as returned using the Linux **vmstat** command.
FREEkB is the available free memory in kilobytes as returned using the Linux **vmstat** command.
+TT.TC is the temperature in degrees centigrade of the Linux CPU die temperature.

Command: **cpustat**
Sonoma reply: **20170116.22:24:00 23% 320056kB +67.9C**

faultstat

This command returns the summary of all system fault states in a user-friendly format. It decodes the fault status word (FLTS) returned in the **gpsstat** command and displays the result in a tabular form with verbose descriptions. For details on the various faults see ***Appendix G - System Faults***.

Command: **faultstat**
Sonoma reply:

```
System Fault Status:
System Oscillator DAC --------------------------> OK
GPS Signal -------------------------------------> OK
FPGA Configuration -----------------------------> OK
FLASH Writes -----------------------------------> OK
GPS Receiver Communication --------------------> OK
GPS Reference Time -----------------------------> OK
Subsystem Communication ------------------------> OK
GPS Antenna ------------------------------------> OK
System Oscillator PLL Unlocked-----------------> OK
System Power/Configuration --------------------> OK
```

FITversion

This command displays FIT version and build date.

Command: **fitversion**
Sonoma reply: **6010-1009-000 v 4.0x - Wed Aug 20 04:57:28: UTC 2025**

get_sw_opts

See ***Chapter 10 - Options, Software Options*** for information on this command.

gpsdynmode

This command displays the current GPS Subsystem dynamic mode of operation. It has two possible settings: ON or OFF. When it is ON, it is assumed that the Sonoma is installed on a moving platform (shipboard only). When it is OFF, it is assumed that the Sonoma is installed in a stationary location.

When the dynamic mode is OFF, the Sonoma will use its accurate reference position to implement Timing Receiver Autonomous Integrity Monitoring (TRAIM) for the utmost in reliability during any GPS system faults. In addition, single satellite operation is possible once an initial accurate position has been determined.

When the dynamic mode is ON, only a very minimal TRAIM algorithm is in effect because the accurate reference position is not static. In addition, a minimum of four satellites must be visible and only 3-D position fixes are used. When the dynamic mode is ON, the source reported for the accurate reference position by **gpsrefpos** is set to DYN.

Command: **gpsdynmode**
Sonoma reply: **OFF**

gpslastfix

This command provides the last computed GPS position. When tracking four or more satellites, the GPS Receiver provides a 3D-position fix. When only three satellites are in view, this will drop to a 2D-position fix. The last-fix position is unaveraged and typically less accurate than the reference position, but it does provide a good indication that the receiver is working properly. Position is provided in latitude, longitude and height above the WGS-84 ellipsoid.

Command: `gpslastfix`

Sonoma reply: `LAST POSITION FIX = N38d24m54.28s W122d45m10.89s +00010.9 meters`

gpsrefpos

This command displays the current GPS Subsystem reference position. The source of the position, which is one of UNK (unknown), DYN (dynamic), USR (user entered) or AVG (24 hour average of GPS fixes) is displayed first. The WGS-84 latitude and longitude in degrees, minutes, seconds format and the height above the WGS-84 reference ellipsoid in meters follow.

Command: `gpsrefpos`

Sonoma reply:

```
CURRENT REFERENCE POSITION = AVG N38d26m36.11s W122d42m56.50s +00032.5 meters
```

gpsstat

This command allows you to query the status of the GPS Subsystem. During normal operation, the NTP daemon polls the GPS Subsystem every 16 seconds. The results of this poll are used to steer the system clock and are saved to a log file. This command parses and formats the data contained therein and prints this fixed-length string having these fields:

```
LKSTAT TFOM = ? YEAR DOY HH:MM:SS LS LF S NN EFCDAC C/No FLTS
```

or

```
LKSTAT TFOM = ? YEAR DOY HH:MM:SS LS LF S NN AGC EFCDAC C/No FLTR FLTS
```

Where:

LKSTAT is the tracking status of the GPS Subsystem, either LOCKED or NOTLKD.

TFOM = ? is a value between 3 and 9 and indicates clock accuracy. A detailed explanation of TFOM is in ***Appendix A - TFOM***.

YEAR is the year of the UTC timestamp of the most recent update.

DOY is the day-of-year of the UTC timestamp of the most recent update.

HH:MM:SS is the hour, minute and second of the UTC timestamp of the most recent update.

LS is the current number of leap seconds difference between the UTC and GPS timescales (18 at the time of this writing).

LF is the future (at the next UTC midnight) number of leap seconds difference between the UTC and GPS timescales (18 at the time of this writing).

S is the Signal Processor State, one of 0 (Acquiring), 1 (GPS Locking), 2 (GPS Locked), 9 (Warming Up).

NN is the number of GPS satellites being tracked, 0 to 12.

AGC is the current receiver Automatic Gain Control DAC word, 0 to 255.

EFCDAC is the system oscillator Electronic Frequency Control 20-bit DAC value, 0 to 1048575 with larger numbers implying higher oscillator frequency. Typical range is 320000 to 680000.

C/No is the received GPS Carrier Signal-to-Noise Ratio, 0.00 to 99.9, measured in dB in a 1Hz bandwidth. Typical range is 30 to 45.

FLTR is the fault status for the GPS Receiver. This is a numeric value consisting of four hexa decimal characters where each bit indicates a particular fault. Assertion of any of these bits will light the Alarm LED. Bit definitions are shown below. Decoding the bits can be difficult for non-programmers. For a more user-friendly method of reading the fault status use the `faultstat` command. For details on each receiver fault see ***Appendix G - System Faults***.

	Bit 3	Bit 2	Bit 1	Bit 0
Char 0	FLASH Writes	FPGA Configuration	GPS Signal	GPS Receiver Oscillator DAC
Char 1	GPS Receiver Oscillator	GPS Reference Time	Local Oscillator Synthesizer	Local Oscillator Synthesizer Tuning
Char 2	N/A	GPS Receiver Oscillator PLL	GPS Antenna Open	GPS Antenna Short
Char 3	N/A	N/A	N/A	N/A

FLTS is the fault status for the GPS Subsystem. This is a numeric value consisting of four hexadecimal characters where each bit indicates a particular system fault. Assertion of any of these bits will light the Alarm LED. Bit definitions are shown below. Decoding the bits can be difficult for non-programmers. For a more user-friendly method of reading the fault status use the `faultstat` command. For details on each system fault see ***Appendix G - System Faults***.

	Bit 3	Bit 2	Bit 1	Bit 0
Char 0	FLASH Writes	FPGA Configuration	GPS Signal	System Oscillator DAC
Char 1	GPS Receiver	Subsystem Communication	GPS Reference Time	GPS Receiver Communication
Char 2	GPS Antenna	System Osc PLL	Secondary Power Supply	Primary Power Supply
Char 3	System Power/ Configuration	N/A	N/A	N/A

The Primary and Secondary Power Supply bits are only used if your Sonoma has the Dual-Redundant

Power Supply option.

The example reply below indicates that there has been a period without tracking a GPS signal that exceeded the time-out period, that there was a FLASH Write Fault and that there is an Antenna Fault.

Command: **gpsstat**
Sonoma reply:

```
LOCKED TFOM = 4 2025 092 04:48:56 18 18 2  7 181 328605 41.6 0100 008A
```

gpstrkstat

This command displays the current GPS Subsystem satellite tracking status. A list of twelve satellite numbers along with azimuth, elevation and C/No is displayed for each receiver channel. Satellite number 0 is an invalid number and indicates that no satellite is being tracked on that channel. Valid satellite numbers range from 1 to 32. Azimuth and elevation are in degrees and C/No is in dB.

Command: **gpstrkstat**
Sonoma reply:

```
Ch SV Azimuth   Elev C/No
 1 23 -108.41 +15.70 41.7
 2 11 -118.21 +45.58 46.9
 3 22 +107.41 +21.04 37.9
 4 14  +52.10 +29.76 40.4
 5 32  -40.36 +58.18 45.2
 6  1  -79.14 +55.53 46.6
 7 31 +127.87 +62.60 47.3
 8  0   +0.00  +0.00  0.0
 9  0   +0.00  +0.00  0.0
10  0   +0.00  +0.00  0.0
11  0   +0.00  +0.00  0.0
12  0   +0.00  +0.00  0.0
```

gpsutcinfo

This command displays the IS-GPS-200 almanac parameters which are used to relate GPS time to UTC. The first line of output contains the current (LS) and future (LSF) leap second values and the GPS week number (WN_lsf) and day of week (DN) at the end of which the future leap second will take effect. This could be in the past if a leap second insertion has recently taken place. Leap second events occur every few years on either June 30 or December 31.

The second line of output contains the parameters for calculating the small residual offset between the GPS master clock ensemble and UTC-USNO. This is typically less than 10 nanoseconds. The remaining output shows the current value of the GPS-UTC offset.

Command: **gpsutcinfo**
Sonoma reply:

```
GPS UTC Almanac Parameters:
LS = 16  LSF = 16  WN_lsf = 1694  DN = 7
a0 = +9.313226e-10  a1 = -1.243450e-14  WN_t = 1727  t_ot =  61440
Current (GPS - UTC) Offset:
GPS - UTC = (16 + 3.810e-09) s @ WN = 1726, TOW = 434757
```

gpsversion

This command displays the firmware and hardware versions of the GPS Subsystem.

Command: `gpsversion`
Sonoma reply:

```
F/W 6010-0071-000 Ver 1.00 - FPGA 6020-0012-000 Ver 01 - JAN 15 17:03:27 2013
```

help

This command displays a list of the Sonoma commands (not Linux commands). To get help on a particular command you would type `help`, followed by the command.

Command: `help`
Sonoma reply: Sonoma commands are displayed.

Command: `help gpsstat`
Sonoma reply: Information specific to the `gpsstat` command is displayed.

installed_sw_opts

See ***Chapter 10 - Options, Software Options*** for information on this command.

kernelversion

This command prints the current Linux operating system kernel firmware version.

Command: `kernelversion`
Sonoma reply:

```
6010-0091-000_v1.00 Linux Kernel 6.1.55-Sonoma #16 Jul 30 19:35:55 2025
```

netconfig

This command starts an interactive script that allows you to configure the IP network subsystem of the Sonoma. By default, the unit is configured to configure itself using the Dynamic Host Configuration Protocol (DHCP). If you need to set up static IP configuration, you must run this script as *root* from the USB port during the installation process. Refer to ***Chapter 2 - Basic Installation, Using netconfig to Set Up Your IP*** for details on the use of the command.

This script creates or modifies these files: */etc/HOSTNAME*, */etc/hosts*, */etc/networks, /etc/resolv.conf* and */etc/rc.d/rc.inet1.conf*. All of these are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot the Sonoma after running this script for the changes to take effect.

Command: `netconfig`
Sonoma reply: Interactive script is started.

ntpconfig

This command starts an interactive script that allows you to configure the NTP Subsystem of the Sonoma. By default, the unit is configured to authenticate its replies to clients using its default MD5 keys in the */etc/ntp.keys* file. If you need to create your own MD5 keys (recommended) or set up broadcast/multicast operation, you must run this script as root. Refer to ***Chapter 3 - Configure the NTP Server*** for details on the use of this command.

The two files that are modified are */etc/ntp.keys* and */etc/ntp.conf*. Both of these are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot the Sonoma after running this script for the changes to take effect.

Command:	`ntpconfig`
Sonoma reply:	Interactive script is started.

ntpstat

This command provides some key information regarding the operation of the NTP daemon. It shows the current offset between the NTP-steered system clock and the GPS Subsystem, the counts of received, sent and dropped packets, and the sent packet rate. The format of the response is:

```
YYYYMMDD.HH:MM:SS +S.sssssssss RCVDCNT SENTCNT SENT/sec DROPCNT
```

Where:

YYYY is the year of the UTC timestamp of the most recent update received from the GPS Sub system.

MMDD is the month and day-of-month of the UTC timestamp of the most recent update received from the GPS Subsystem.

HH:MM:SS is the hour, minute and second of the UTC timestamp of the most recent update received from the GPS Subsystem.

+S.sssssssss is the offset in seconds between the NTP system clock and the GPS Subsystem clock. Positive implies that the system clock is ahead of the GPS Subsystem clock.

RCVDCNT is a count of the number of NTP packets received since startup of the NTP daemon. This is a 32-bit counter so it will wrap back to zero after 4,294,967,295 packets.

SENTCNT is a count of the number of NTP packets sent since startup of the NTP daemon. This is a 32-bit counter so it will wrap back to zero after 4,294,967,295 packets.

SENT/sec is the current rate of NTP packets being sent per second.

DROPCNT is a count of the number of NTP packets dropped since startup of the NTP daemon. This is a 32-bit counter so it will wrap back to zero after 4,294,967,295 packets.

Below is an example of a typical response to this command:

Command: `ntpstat`
Sonoma reply:

```
20170117.00:02:40 -0.000000051 129127988 129015079  1594.4/sec      15
```

oscctrlstat

This command displays the current values of the system oscillator control parameters. These parameters are related to the disciplined system oscillator. The command formats the data and prints this fixed-length string having these fields:

```
YYYYMMDD.HH:MM:SS LKSTAT COAST ESTERR MEASERR TIMEDEV AGERATE TAU EFCDAC TEMP
```

Where:

YYYY is the year of the UTC timestamp of the most recent update received from the GPS Subsystem.

MMDD is the month and day-of-month of the UTC timestamp of the most recent update received from the GPS Subsystem.

HH:MM:SS is the hour, minute and second of the UTC timestamp of the most recent update received from the GPS Subsystem.

LKSTAT is the GPS Subsystem control status, either WRM (warming up), ACQ (acquiring), LKG (locking) or LKD (locked).

COAST is the number of seconds the GPS Subsystem has been in coast mode (unlocked to GPS).

ESTERR is the estimated time error of the GPS Subsystem when in coast mode, in seconds.

MEASERR is the last measured time offset of the GPS Subsystem to GPS while locked, in seconds.

TIMEDEV is the time deviation (TDEV) of the offset measurements in seconds. The tau associated with this measurement is one second, which is the update interval of the position fixes received from the GPS Receiver.

AGERATE is the regression-computed system oscillator ageing rate per day (several-hour delay before the first measurements are displayed).

TAU is the system oscillator control loop averaging time constant, in seconds. It's value is automatically adjusted to maintain optimum offset and stability.

EFCDAC is the system oscillator Electronic Frequency Control 20-bit DAC value. The system automatically sets this value to remove frequency errors. Values may

range from 0 to 1048575. Values close to the maximum or minimum will set the DAC fault flag that will appear in the fault status display. The Time/Status display will also indicate a fault condition.

TEMP is the chassis internal temperature in °C.

Below is an example of a typical response to this command:

Command: `oscctrlstat`
Sonoma reply:

```
20170117.00:23:10 LKD     0 6.26e-09 -6.26000e-09 1.25e-09 -6.93e-13  1955.3
524281          +50.750
```

passwd

This command is used to change the password for the user that you are logged in as. It affects the serial port, SSH and HTTP. `passwd` is a Linux command that is also described in ***Appendix C - Helpful Linux Information***.

Command: `passwd`
Sonoma reply: Interactive script is started.

ptpconfig0 and ptpconfig1 (Optional)

These commands are only available if the Precision Time Protocol (PTP) option has been installed. Refer to ***Chapter 4 - PTP/IEEE-1588*** for more information.

ptpstat0 and ptpstat1 (Optional)

These commands are only available if the Precision Time Protocol (PTP) option has been installed. Refer to ***Chapter 4 - PTP/IEEE-1588*** for more information.

pwrfltmask (Optional)

See ***Chapter 10 - Options, Masking Dual Power Supply Fault Alarms*** for information on this command.

rcvrserialnumber

It shows the serial number of the EndRun GPS Receiver inside Sonoma. See ***Chapter 1 - Introduction, GPS Receivers*** for information on EndRun's GPS Receiver.

Command: `rcvrserialnumber`
Sonoma reply: `17080056`

rcvrstat

It shows three critical status parameters of the GPS Receiver: the number of satellites currently being tracked, the automatic gain control DAC value for the receiver front end, and the average Carrier-to-

Noise ratio of the tracked satellites. See ***Chapter 1 - Introduction, GPS Receivers*** for information on EndRun's GPS Receiver.

Command: `rcvrstat`
Sonoma reply: `20150622.23:35:50 8 125 45.0`

rcvrversion

It displays the firmware and hardware versions of the EndRun GPS Receiver. See ***Chapter 1 - Introduction, GPS Receivers*** for information on EndRun's GPS Receiver.

Command: `rcvrversion`
Sonoma reply:

```
F/W 6010-0081-000 Ver 1.00 - FPGA 6020-0014-000 Ver 01 - MAR 24 15:05:36 2015
```

or

```
rcvrversion: command not found
```

If the command is not found then your Sonoma does not have an EndRun GPS Receiver.

resetlastgpswn

It is for use with a GPS simulator. Not for general use - contact EndRun for details.

resetleaphistory

It is for use with a GPS simulator. Not for general use - contact EndRun for details.

serialnumber

This command shows the serial number of the Sonoma.

Command: `serialnumber`
Sonoma reply: `15080056`

setantfltmask

This command allows you to enable or mask the GPS antenna fault. Parameter for this command is either MASKED or ENABLED. Setting this command to MASKED will prevent the antenna fault from creating an alarm condition. Some installations may need to mask this fault due to special antenna situations like splitters or DC blocks that confuse the antenna detection circuit. The factory default setting is ENABLED.

Command: `setantfltmask MASKED`
Sonoma reply: `Antenna Fault Mask set to MASKED`

setcaldelay

This command starts an interactive utility that allows you to change the clock calibration delay. This setting is used to advance or retard the clock in order to compensate for antenna cable length or other external hardware or cabling. Allowable range is ±500,000 nanoseconds.

Command: `setcaldelay`
Sonoma reply: Interactive utility is started.

setgpsdynmode

This command accepts a single argument: ON or OFF to allow you to set the dynamic mode of operation of the GPS Subsystem. By default, the unit is configured for static operation, so this setting is OFF. If Sonoma will be mounted on a ship, then this setting must be changed to ON. The change takes place immediately and is stored non-volatilely.

It is important that the dynamic mode be set OFF when the instrument is in a static installation. This is the factory-default setting. *Set the dynamic mode to ON only if the instrument is installed on a moving platform such as a ship. Dynamic mode is intended for shipboard applications only. Dynamic mode is intended for shipboard applications only, for no GPS signal obstruction at speeds less than 60 mph.*

Command: `setgpsdynmode ON`
Sonoma reply: `GPS Dynamic Mode is ON`

setgpsrefpos

This command starts an interactive utility that allows you to set the accurate reference position of Sonoma. This utility must be run as the root user. By default, the unit is configured to locate itself using the GPS satellites. In some situations, visibility of the sky is limited and Sonoma will not be able to determine its position. In this case, you must determine an accurate WGS-84 position by other means and input it using this command. Changes you make to the position take place immediately. Refer to ***Appendix E - Installing the GPS Antenna, GPS Reference Position*** for details. *If the GPS dynamic mode setting is ON (see* `gpsdynmode`/`setgpsdynmode` *commands), then running this utility will have no effect.*

In addition to setting a new reference position, you can also invalidate an existing one. We recommend you do this if Sonoma has an established position and then you move your GPS antenna. You can invalidate an old position by setting the position mode to UNKNOWN. This will speed up the time it takes for Sonoma to acquire a new position and relock to the GPS signal. A cold start in unknown position mode should take about 20 minutes to lock, assuming a decent antenna installation.

Command: `setgpsrefpos`
Sonoma reply: Interactive utility is started.

setpwrfltmask (Optional)

See ***Chapter 10 - Options, Masking Dual Power Supply Fault Alarms*** for information on this command.

setsigfltmask

This command allows you to enable or mask the Signal Loss Fault. Parameter for this command is either MASKED or ENABLED. Setting this command to MASKED will prevent a signal loss fault from creating an alarm condition. Some installations may need to mask this fault when operating the NTP server as a Stratum 2 server. The factory default setting is ENABLED.

Command: `setsigfltmask MASKED`
Sonoma reply: `Signal Loss Fault Mask set to MASKED`

sigfltmask

This command displays the current setting for the Signal Loss Fault Mask.

Command: `sigfltmask`
Sonoma reply: `Signal Loss Fault is ENABLED`

subsysreset

This command performs a GPS Subsystem reset which is similar to cycling the power on the GPS Subsystem. After about 10 seconds, the boot messages from the GPS Subsystem will be displayed.

Command: `subsysreset`
Sonoma reply:

```
Bootloader 6010-0070-000 v 1.00 - Dec 27 2012 14:48:55
FW 6010-0071-000 v  1.00  - Mar 12 2013 16:08:46
FPGA 6020-0012-000 v 01
```

sysfit

This command returns the currently booted Linux kernel, either 0 or 1, where 0 is the factory-installed kernel and 1 is the upgraded kernel.

Command: `sysfit`
Sonoma reply: `BOOTED FIT IMAGE = 1 (Upgrade)`

sysosctype

This command displays the installed system oscillator type. It is either TCXO, OCXO or Rubidium. The standard oscillator type is the TCXO.

Command: `sysosctype`
Sonoma reply: `Installed Oscillator is TCXO.`

sysstat

This command allows you to query the status of the NTP Subsystem. It retrieves information from the NTP daemon to determine the current synchronization status of the NTP Subsystem. It then retrieves the last line in the logfile */var/log/praecis0.monitor* controlled by the NTP daemon reference clock driver that communicates with the GPS Subsystem. This logfile is updated every 16 seconds under normal operation. It parses and formats the data contained therein and prints this fixed-length (generally, since grossly unsynchronized states could cause the floating offset field to overflow momentarily) string having these fields:

```
LKSTAT TO GPS, Offset = +S.sssssssss, LI = ??, TFOM = ? @ YEAR DOY HH:MM:SS LS
```

Where:

LKSTAT is the system peer status of the NTP daemon relative to the GPS Subsystem, either LOCKED or NOTLKD. NOTLKD can imply several things: the system has just started, there is a fault in the GPS Subsystem which has caused NTP to either be unable to obtain timing information from the GPS Subsystem or to reject the timing information that it is obtaining from it.

+S.sssssssss is the offset in seconds between the NTP system clock and the GPS Subsystem clock. Positive implies that the system clock is ahead of the GPS Subsystem.

LI = ?? is the NTP daemon leap indicator bits. Leap seconds occur about every 1½ to 3 years. Possible indicator values are:

00:	Normal, locked operation.
01:	Leap second insertion will occur after 23:59:59 UTC.
11:	Fault. Unsynchronized state.

TFOM = ? is a value between 3 and 9 and indicates clock accuracy. A detailed explanation of TFOM is in ***Appendix A - TFOM.***.

YEAR is the year of the UTC timestamp of the most recent update received from the GPS Sub system.

DOY is the day-of-year of the UTC timestamp of the most recent update received from the GPS Subsystem.

HH:MM:SS is the hour, minute and second ot the UTC timestamp of the most recent update received from the GPS Subsystem.

LSis the current number of leap seconds difference between the UTC and GPS timescales (18 at the time of this writing).

Below is an example of a typical response to this command:

Command: **sysstat**
Sonoma reply:

```
LOCKED TO GPS, Offset = +0.000000024, LI = 00, TFOM = 4 @ 2017 012 06:03:10 18
```

systemio (Optional)

See ***Chapter 10 - Options, CPU Module Options*** for information on this command.

systemioconfig (Optional)

See ***Chapter 10 - Options, CPU Module Options*** for information on this command.

systimemode

This command displays the current time mode for any optional Time Code or Serial Time outputs. Time modes are UTC, GPS and LOCAL. The displayed Local Time Offset from UTC and the DST Start/Stop parameters are only valid when the time mode is LOCAL. A positive Local Time Offset implies a longitude east of the Greenwich meridian and that Local time is ahead of UTC.

Command: **systimemode**
Sonoma reply:

```
Time Mode = LOCAL
Local Time Zone Offset from UTC (Does Not Include DST) = -16 (half hours)
DST Start Month = Mar Sunday = 2nd  Hour = 2
DST Stop  Month = Nov Sunday = 1st  Hour = 2
```

systimemodeconfig

This command starts an interactive utility that allows you to configure the time mode of any optional Time Code outputs, Serial Time output. *These settings have no effect on the operation of the NTP daemon or the underlying Linux operating system time. These ALWAYS operate in UTC.*

By default, the unit is configured to operate in UTC mode. If you need to modify the setting, you must run this utility as root. Settings made using this command are non-volatile.

Command: `systimemodeconfig`
Sonoma reply: Interactive utility is started.

sysversion

This command displays the firmware version and build date of the Linux root file system.

Command: `sysversion`
Sonoma reply: `Sonoma_D22 GPS 6010-0090-000 v 4.0 - Aug 20 04:57:28 2025`

updaterootflag

This command allows you to update the configuration of the Linux bootloader after a new root file system image has been written to the UPGRADE FIT file system partition of the Sonoma FLASH disk. You may also use it to reset the default back to the FACTORY FIT file system partition. Refer to ***Appendix B - Upgrading the Firmware*** for detailed instructions for performing the upgrade procedure. One argument is accepted, whose value is either 0 or 1, which causes a flag to be set that indicates to the bootloader which FIT file system image should be loaded by default. If an argument value of 2 is given, then the currently configured default root file system is shown.

Command: `updatefootflag o`
Sonoma reply: `no reply (sets boot flag to FACTORY partition)`
Command: `updaterootflag 1`
Sonoma reply: `no reply (sets boot flag to UPGRADE partition)`
Command: `updaterrootflag 2`
Sonoma reply: `Default FIT Image (either FACTORY or UPGRADE, whatever is currently set)`

upgradefit

This utility allows you to upgrade the Linux kernel. It is run after the *kernel.gz* file has been copied to the */tmp* directory on the system. It performs an erase of the upgrade kernel partition and then writes the */tmp/kernel.gz* file to it. Refer to ***Appendix B - Upgrading the Firmware, Performing the Linux Kernel Upgrade*** for detailed information.

Command: `upgradefit`
Sonoma reply: Shows progress indicator.

upgradercvr

It allows you to upgrade the EndRun GPS Receiver firmware. See ***Chapter 1 - Introduction, GPS Receivers*** for information on EndRun's GPS Receiver.

Prior to executing this command, you must copy the new binary firmware file to */tmp/rcvr.bin*.

The utility starts the X-modem file transfer, and then displays progress to the console. See ***Appendix B - Upgrading the Firmware, Performing the GPS Receiver Upgrade*** for more information.

Command: `upgradercvr`
Sonoma reply: Upgrade progress is shown.

upgradercvrfpga

It allows you to upgrade the Field-Programmable Gate Array (FPGA) resident on the EndRun GPS Receiver. See ***Chapter 1 - Introduction, GPS Receivers*** for information on EndRun's GPS Receiver.

Prior to executing this command, you must copy the new binary FPGA file to */tmp/rcvrfpga.bin*.

The utility starts the X-modem file transfer, and then displays progress to the console. See ***Appendix B - Upgrading the Firmware, Performing the GPS Receiver FPGA Upgrade*** for more information.

Command: `upgradercvrfpga`
Sonoma reply: Upgrade progress is show

upgraderootfs

This utility allows you to upgrade the Linux root file system. It is run after the *rootfs.gz* file has been copied to the */tmp* directory on the system. It performs an erase of the upgrade root file system partition and then writes the */tmp/rootfs.gz* file to it. Refer to ***Appendix B - Upgrading the Firmware, Performing the Linux RFS Upgrade*** for detailed information..

Command: `upgraderootfs`
Sonoma reply: Shows progress indicator.

upgradesubsys

This utility allows you to upgrade the GPS Subsystem firmware. Prior to executing this command, you must copy the new binary firmware file to */tmp/subsys.bin*.

It issues the commands over the serial port to the GPS Subsystem that are needed to start the X-modem file transfer, and then displays progress to the console. See ***Performing the GPS Subsystem Upgrade*** in ***Appendix B - Upgrading the Firmware*** for more information.

Command: `upgradesubsys`
Sonoma reply: Upgrade progress is shown.

wrt_sw_opt

See ***Chapter 10 - Options, Software Options*** for information on this command.

This page is left intentionally blank.

Chapter *Ten*

Options

Your Sonoma supports many input/output (I/O) options. Several outputs via the CPU Module are available in addition to various power supply input options. Status and user settings for the output signals can be easily viewed and modified via the console port. Methods to do this are described in this chapter. Refer to ***Chapter 4 - PTP/IEEE-1588*** *for details on the Precision Time Protocol. Refer to* ***Appendix H - Specifications*** *for details on signals, connector types, pinouts, etc.*

Software Options

Currently, there are only two software options available in Sonoma. These are for PTP/IEEE-1588 on port 0 and port 1. The Precision Time Protocol is described in detail in ***Chapter 4 - PTP/IEEE-1588***.

Normally, EndRun products are configured from the factory with software options enabled. But software options are also field-installable. In other words, you can enable a software option yourself, after you have received your Sonoma. First you must obtain an 8-digit license key from EndRun Technologies, then you can enable it using the `wrt_sw_opt` command.

wrt_sw_opt

To enable a software option use this console port command. You must be logged in as the root user in order to run this command and you must provide a license key on the command line. If the key is verified, then the option will be enabled.

Command: `wrt_sw_opt [key]`
Sonoma reply: `Option to be enabled is PTP0 Daemon`

installed_sw_opts

This user-friendly command shows which software options are enabled in your Sonoma. Below is an example when PTP is installed on both ports.:

Command: `installed_sw_opts`
Sonoma reply: `The PTP0 Daemon Option is Installed.`
`The PTP1 Daemon Option is Installed.`

Another example is below, no software options are installed:

Command: `installed_sw_opts`
Sonoma reply: <no reply>

get_sw_opts

This command is documented here for completeness. The **`installed_sw_options`** command above is much easier to use. The **`get_sw_opts`** command returns a 32-bit value with each bit identifying a software option. Below is an example when no software options are enabled:

Command: **`get_sw_opts`**
Sonoma reply: **`00000000000000000000000000000000`**

Bit are numbered from 0 to 31, from right to left. The example below shows bit 0 set which identifies that the PTP0 option is enabled.

Command: **`get_sw_opts`**
Sonoma reply: **`00000000000000000000000000000001`**

Software Option Bit Definitions

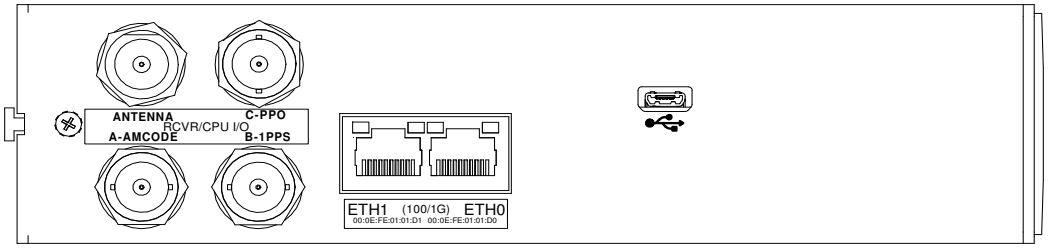
Bits are numbered from 0 to 31, from right to left. Currently, there are only two software options defined in the Sonoma. These are for PTP/IEEE-1588 enabled on port 0 (eth0) or port 1 (eth1). The table below shows the currently defined bits.

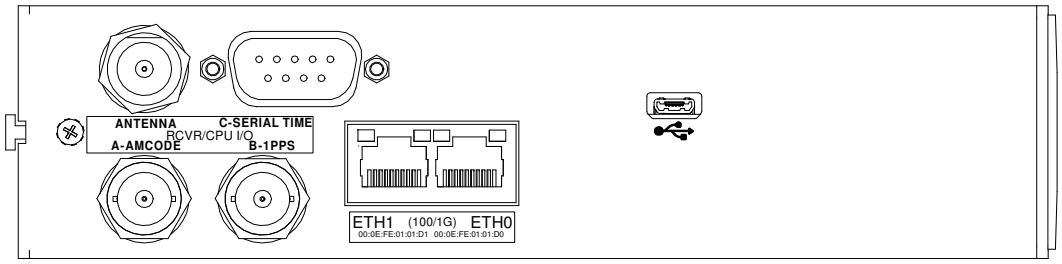
Bit 31	Bit 30	.....	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
								PTP Port 1 (eth1)	PTP Port 0 (eth0)

CPU Module Options

Standard rear-panel configuration for the CPU Module is the Antenna input, the USB connector and two ethernet connectors. Refer to ***Chapter 2 - Basic Installation, Sonoma Physical Description*** for more information on the basic Sonoma rear-panel.

In addition to the standard connectors, the CPU Module can be configured with optional outputs. Some of these optional outputs are a Programmable Pulse Output, a DDS Output, an Alarm Output, various pulse rates at RS-422 levels, and RS-232 serial port with a Serial Time Output. See sample CPU Module configurations below.





Programmable Pulse Output (PPO)

The PPO Option provides user-selectable, on-time pulse rates from 1 PPS to 10 MPPS. Other selections are 1PP60S (pulse per 60 seconds, on the minute), 1PP2S (pulse per 2 seconds, on the even second), and Inverted 1PPS (falling edge on-time). For details on signal definition see ***Appendix H - Specifications***.

View and Change the PPO Configuration

Use the `cpuio` command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C. To change the PPO selection use the `cpuioconfig` command.

Command: `cpuio`
Sonoma reply:
```
PROGRAMMABLE PULSE OUTPUT is Installed
    Current Setting = OFF
```

Command: `cpuioconfig`
Sonoma reply: Interactive script is started so you can change the pulse rate.

1PPS Output

This output provides 1PPS signal. There are several variations of the 1PPS Output signal such as: 1PPS TTL, 1PPS (RS-422), and Inverted 1PPS. The Programmable Pulse Output also has a 1PPS selection.

The 1PPS is a “system signal”. This means that there is one 1PPS signal that affects the whole system. In other words, if your Sonoma has multiple 1PPS outputs and you change the pulse width, then all 1PPS outputs will be affected.

The pulse width is normally 1 millisecond wide when shipped from the factory but can be changed (see below). For details on the 1PPS signal definition see ***Appendix H - Specifications***.

View and Change the 1PPS Configuration

Use the `cpuio` command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C. Use the `systemio` command to view the 1PPS pulse width setting.

Command: `cpuio`
Sonoma reply:
```
CPU I/O B - 1 PPS OUTPUT is Installed
Current Setting = (See systemio command)
```

Command: `systemio`
Sonoma reply:
```
System I/O Signal 1 PPS OUTPUT is Installed
Current Setting = 1 Milliseconds Pulse Width
```

Use the **`systemioconfig`** command to change the 1PPS pulse width. You will be able to choose from among these selections: 20 microseconds, 1 millisecond, 100 milliseconds and 500 milliseconds.

Command: `systemioconfig`
Sonoma reply: Interactive script is started so you can change the pulse width.

Time Code Output

There are two different kinds of Time Code outputs. Either amplitude-modulated (AM) or DC-Shift. Connectors will be labeled as either AMCODE or DCCODE.

The Time Code is a "system signal". This means that there is one Time Code signal that affects the whole system. In other words, if your Sonoma has multiple Time Code outputs (AM or DC) and you change the Time Code format, then all Time Code outputs will be affected.

The Time Code output is normally IRIG-B122 (AM) or B002 (DC) when shipped from the factory but can be changed (see below). For details on signal definition see ***Appendix H - Specifications***.

View and Change the Time Code Configuration

Use the **`cpuio`** command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C. Use the **`systemio`** command to view the current setting for the Time Code format.

Command: `cpuio`
Sonoma reply:
```
CPU I/O A - AM TIME CODE OUTPUT is Installed
Current Setting = (See systemio command)
```

Command: `systemio`
Sonoma reply:
```
System I/O Signal TIME CODE OUTPUT is Installed
Current Setting = IRIG-B122/B002 Format
```

Use the **`systemioconfig`** command to change the Time Code format. You will be able to choose from among several different formats.

Command: `systemioconfig`
Sonoma reply: Interactive script is started so you can change the Time Code format.

Fixed Rate Output (10 MPPS, etc.)

The Fixed Rate Output Option provides a customer-specified fixed rate output ranging from 1 PPS to 10 MPPS. The rear-panel connector will be labeled for the appropriate rate such as “10 MPPS” or “100 PPS”, etc. This signal is specified by the customer when the order is placed, preset at the factory, and cannot be changed. For details on signal definition see ***Appendix H - Specifications***.

View the Fixed Rate Output Connector

Use the `cpuio` command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C.

Command: `cpuio`
Sonoma reply: `CPU I/O C - 10M PPS OUTPUT is Installed`

Alarm Output

The Alarm Output provides an open-collector output that indicates when the GPS Subsystem has lost lock, or when serious hardware faults are detected. For a detailed description of the faults see ***Appendix G - System Faults.***

Care should be taken not to directly connect this open-collector output to a voltage source. A series current-limiting resistor of at least 1K ohms in value should be used. The pull-up voltage must not exceed 40V. The Alarm Output connector can be either a BNC or a terminal block. For more details see ***Appendix H - Specifications***.

View the Alarm Output Connector

Use the `cpuio` command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C.

Command: `cpuio`
Sonoma reply: `CPU I/O C - OPEN COLLECTOR ALARM OUTPUT is Installed`

Direct Digital Synthesizer (DDS)

The DDS Option provides user-selectable pulse rates from 1 Hz to 10 MHz, programmable in 1 PPS steps, including 1.544 MPPS or 2.048 MPPS. The selected pulse rate is phase locked to the system oscillator and is not aligned with system time.

The DDS is a “system signal”. This means that there is one DDS signal that affects the whole system. In other words, if your Sonoma has multiple DDS outputs and you change the pulse rate, then all DDS outputs will be affected.

The pulse rate is 0 Hz when shipped from the factory but can be changed (see below). For details on the DDS signal definition see ***Appendix H - Specifications***.

View and Change the DDS Configuration

Use the `cpuio` command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C. Use the `systemio` command to view the DDS rate.

```
Command:        cpuio
Sonoma reply:   CPU I/O C - DIRECT DIGITAL SYNTHESIZER OUTPUT is Installed
                Current Setting = (See systemio command)

Command:        systemio
Sonoma reply:   System I/O Signal DIRECT DIGITAL SYNTHESIZER OUTPUT Installed
                Current Setting = 0 Hz
```

Use the `systemioconfig` command to change the DDS rate.

```
Command:        systemioconfig
Sonoma reply:   Interactive script is started so you can change the DDS rate.
```

Serial Time Output

This option is provided on an RS-232 (or RS-422) serial port labeled “Serial Time”. It is an output that provides a once-per-second sequence of ASCII characters indicating the current time. The “on-time” character starts transmitting within the first 20 microseconds of each second. The output starts automatically on power-up. See ***Appendix H - Specifications*** for details.

The Serial Time is a “system signal”. This means that there is one Serial Time signal that affects the whole system. In other words, if your Sonoma has multiple Serial Time outputs, and you change the settings, then all Serial Time outputs will be affected.

There are several different formats for this ASCII string. The format, baud rate and parity can all be changed via the console port. Baud rate selections are 57600, 19200, 9600, and 4800. Parity selections are odd, even, and none. Format selections are Sysplex, Truetime, EndRun, EndRunX, NENA and NMEA.

View and Change the Serial Time Configuration

Use the `cpuio` command to view the optional outputs on the CPU Module. This command will list any connector that has an optional I/O signal. Connectors are identified as A, B or C. Use the `systemio` command to view the Serial Time configuration.

```
Command:        cpuio
Sonoma reply:   CPU I/O A - SERIAL TIME OUTPUT is Installed
       Current Setting = (See systemio command)
```

Command: `systemio`
Sonoma reply: `System I/O Signal SERIAL TIME OUTPUT is Installed --`
`Current Serial Time Output Baudrate Setting = 9600`
`Current Serial Time Output Format Setting = SYSPLEX`
`Current Serial Time Output Parity Setting = ODD`
`Current NMEA Sentence 1 Setting = NONE`
`Current NMEA Sentence 2 Setting = NONE`
`Current NMEA Sentence 3 Setting = NONE`

Use the `systemioconfig` command to change the Serial Time settings.

Command: `systemioconfig`
Sonoma reply: Interactive script is started so you can change the Serial Time settings.

Sysplex Format

"Sysplex" means SYStem comPLEX and is a term used to describe computing on clusters of computers. The Sysplex option is designed to provide time synchronization for an IBM Sysplex Timer. It can also be used for precise time synchronization by any computers that do not use NTP and have an available serial port connection. The time contained in this string format is always UTC time. The following string is sent once each second:

<SOH>DDD:HH:MM:SSQ<CR><LF>

<SOH> is the ASCII Start-of-Header character (0x01)
DDD is the day-of-year
: is the colon character (0x3A)
HH is the hour of the day
MM is the minute of the hour
SS is the second of the minute
Q is the time quality indicator and may be either:
<space> ASCII space character (0x20) which indicates locked
? ASCII question mark (0x3F) which indicates the unsynchronized condition
<CR> is the ASCII carriage return character (0x0D) and is the on-time character, transmitted during the first millisecond of each second.
<LF> is the ASCII line feed character (0x0A)

Truetime Format

The format of the Truetime string is identical to the Sysplex format. The only difference between the two is that the Sysplex format always uses UTC time. The time contained in the Truetime format depends on the time mode of the Sonoma. For example, if you want an output with this string format that uses Local Time, then select the Truetime format.

EndRun Format

The time contained in this string depends on the time mode of the Sonoma. For example, if you want the time in this string to be UTC, then set the time mode of the Sonoma to UTC. (You can do this by using the console port (see `systimemodeconfig` in ***Chapter 9 - Console Port Control and Status***). The following string is sent once each second:

T YYYY DDD HH:MM:SS zZZ m<CR><LF>

T	is the Time Figure of Merit character described in ***Appendix A - TFOM***. This is the on-time character, transmitted during the first millisecond of each second.
YYYY	is the year
DDD	is the day-of-year
:	is the colon character (0x3A)
HH	is the hour of the day
MM	is the minute of the hour
SS	is the second of the minute
z	is the sign of the offset to UTC, + implies time is ahead of UTC.
ZZ	is the magnitude of the offset to UTC in units of half-hours. Non-zero only when the Timemode is Local.
m	is the Timemode character and is one of: G = GPS L = Local U = UTC
<CR>	is the ASCII carriage return character (0x0D)
<LF>	is the ASCII line feed character (0x0A)

EndRunX (Extended) Format

The EndRunX format is identical to the EndRun format with the addition of two fields - the current leap second settings and the future leap second settings. The following string is sent once each second:

T YYYY DDD HH:MM:SS zZZ m CC FF<CR><LF>

T	is the Time Figure of Merit character described in ***Appendix A - TFOM***. This is the on-time character, transmitted during the first millisecond of each second.
YYYY	is the year
DDD	is the day-of-year
:	is the colon character (0x3A)
HH	is the hour of the day
MM	is the minute of the hour
SS	is the second of the minute
z	is the sign of the offset to UTC, + implies time is ahead of UTC.
ZZ	is the magnitude of the offset to UTC in units of half-hours. Non-zero only when the Timemode is Local.
m	is the Timemode character and is one of: G = GPS L = Local U = UTC
CC	is the current leap seconds value.
FF	is the future leap seconds which will show a leap second pending 24 hours in advance.
<CR>	is the ASCII carriage return character (0x0D)
<LF>	is the ASCII line feed character (0x0A)

NENA Format

NENA is the National Emergency Number Association. This organization has adopted several ASCII time code formats for use in PSAPs (Public Safety Answering Points) and they are specified in the NENA PSAP Master Clock Standard, Issue 4. These ASCII time code formats are NENA Format 0 (NENA0), NENA Format 1 (NENA1), and NENA Format 8 (NENA8):

NENA0

<CR><LF>Q^^DDD^HH:MM:SS^dTZ=XX<CR><LF>

Q	is the time quality indicator and may be either: <space> ASCII space character (0x20) which indicates locked. ? ASCII question mark (0x3F) which indicates the unsynchronized condition.
^	is the space character (0x20).
DDD	is the day-of-year (001-366)
:	is the colon character (0x3A)
HH	is the hour-of-the-day (00-23)
MM	is the minute-of-the-hour (00-59)
SS	is the second-of-the-minute (00-60)
d	is the DST indicator (S,I,D,O).
TZ=XX	is the time zone where XX is 00 through 23
<CR>	is the ASCII carriage return character (0x0D). The first <CR> is the on-time character.
<LF>	is the ASCII line feed character (0x0A).

NENA1

<CR><LF>Q^WWW^DDMMMYY^HH:MM:SS<CR><LF>

Q	is the time quality indicator and may be either: <space> ASCII space character (0x20) which indicates locked. ? ASCII question mark (0x3F) which indicates the unsynchronized condition.
^	is the space character (0x20).
WWW	is the day-of-week (MON, TUE, WED, THU, FRI, SAT
DD	is the day-of-month (1-31)
MMM	is the month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC)
YY	is the two-digit year
:	is the colon character (0x3A)
HH	is the hour-of-the-day (00-23)
MM	is the minute-of-the-hour (00-59)
SS	is the second-of-the-minute (00-60)
<CR>	is the ASCII carriage return character (0x0D). The first <CR> is the on-time character.
<LF>	is the ASCII line feed character (0x0A)

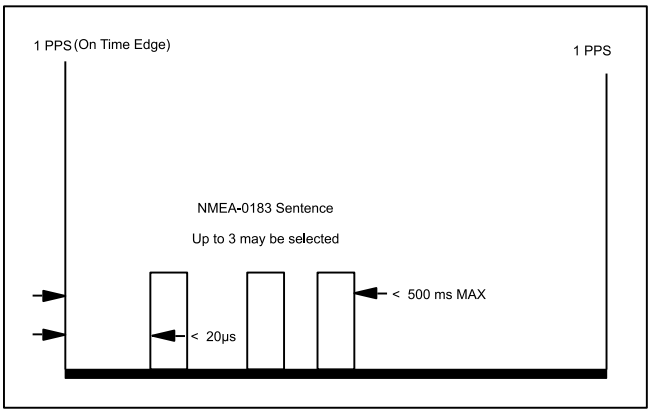
NENA8
<CR><LF>Q^^YYYY^DDD^HH:MM:SS^D+ZZ<CR><LF>

Q	is the time quality indicator and may be either:
	<space> ASCII space character (0x20) which indicates locked.
	? ASCII question mark (0x3F) which indicates the unsynchronized condition.
^	is the space character (0x20).
YYYY	is the four-digit year
DDD	is the day-of-year (001-366)
:	is the colon character (0x3A)
HH	is the hour-of-the-day (00-23)
MM	is the minute-of-the-hour (00-59)
SS	is the second-of-the-minute (00-60)
d	is the DST indicator (S,I,D,O).
+ZZ	+ or - time zone offset relative to UTC (00-12)
<CR>	is the ASCII carriage return character (0x0D).
	The first <CR> is the on-time character.
<LF>	is the ASCII line feed character (0x0A).

NMEA Format

The National Marine Electronics Association (NMEA) has developed a specification that defines the interface between various pieces of marine electronic equipment. This standard defines "sentences" that contain GPS position, navigation, time, and other information. Sentences that have been implemented in the Sonoma conform to NMEA-0183 Specification Version 3.01.

Your Sonoma can output one, two, or three of these sentences per second. The first character ("$") of the first sentence is the "on-time" character. Once the unit is locked to GPS, the "on-time" character starts transmitting within the first 20 microseconds of each second. Each sentence is transmitted within 500 milliseconds after the 1PPS pulse. See diagram below.



*NOTES: If the GPS Receiver is tracking less than 3 satellites then there will be no valid fixes. Therefore, the sentences will be blank. For example: $GPGLL,,,,,,V,N*64.*

If the GPS Receiver is tracking 3 or more satellites then fixes will occur every 3 seconds. Therefore, the content of the once per second NMEA strings will repeat 3 times.

Sonoma NMEA Sentences

Not all information defined in the NMEA sentences is available from the GPS Receiver resident in the Sonoma. Following are the definitions for the NMEA sentences as implemented in this product:

GGA (GPS Fix Data)

The GGA sentence contains the time, position, and fix related data. (EndRun does not calculate mean sea level.) Examples are below:

$GPGGA,,,,,,,0,00,,,M,,,*2B<CR><LF>
$GPGGA,173423.00,3827.030,N,12244.020,W,1,08,1.2,14.5,M,,,,0000*72<CR><LF>

Msg ID	$GPGGA	
Field 1	173423.00	UTC time of fix (hhmmss.ss)
Field 2	3827.030	Latitude in ddmm.mmm
Field 3	N	Direction of latitude (N=north, S=south)
Field 4	12244.020	Longitude in dddmm.mmm
Field 5	W	Direction of longitude (W=west, E=east)
Field 6	1	Fix quality indicator (0=fix not valid, 1=GPS fix)
Field 7	08	Number of SVs in use, 00-08
Field 8	1.2	HDOP (horizontal dilution of precision)
Field 9	14.5	Altitude above WGS84 ellipsoid (we do not calculate mean sea level)
Field 10	M	“M” indicates altitude is in meters
Field 11	empty field	Height of geoid (mean sea level)
Field 12	empty field	Units of geoidal separation
Field 13	empty field	Time in seconds since last DGPS update
Field 14	empty field	DGPS station ID number
Checksum	*72	
Msg End	<CR><LF>	

GLL (Position Data)

The GLL sentence identifies the position fix, time of position fix, and status. Examples are below:

$GPGLL,,,,,,,V,N*64<CR><LF>
$GPGLL,3827.030,N,12244.020,W,173423.00,A,A*34<CR><LF>

Msg ID	$GPGLL	
Field 1	3827.030	Latitude in ddmm.mmm
Field 2	N	Direction of latitude (N=north, S=south)
Field 3	12244.020	Longitude in dddmm.mmm
Field 4	W	Direction of longitude (W=west, E=east)
Field 5	173423.00	UTC time of fix (hhmmss.ss)
Field 6	A	A=data valid, V=data not valid
Field 7	A	A=autonomous mode, N=data not valid
Checksum	*34	
Msg End	<CR><LF>	

GSA (GPS DOP and Active Satellites)

The GSA sentence identifies the GPS position fix mode, the Satellite Vehicles (SVs) used for navigation, and the Dilution of Precision (DOP) values. DOP is an indication of the effect of satellite geometry on the accuracy of the fix. An example is below:

$GPGSA,A,1,,,,,,,,,,,,,,*1E<CR><LF>
$GPGSA,A,3,18,3,22,6,9,14,19,32,17,1,,,2.0,1.2,1.6*10<CR><LF>

Msg ID	$GPGSA	
Field 1	A	Fixed text “A” shows auto selection of 2D or 3D fix
Field 2	3	Fix type (1=fix not available, 2=2D fix, 3=3D fix)
Field 3	18	PRN of SV used for fix on channel 1 (empty if no SV)
Field 4	3	PRN of SV used for fix on channel 2 (empty if no SV)
Field 5	22	PRN of SV used for fix on channel 3 (empty if no SV)
Field 6	6	PRN of SV used for fix on channel 4 (empty if no SV)
Field 7	9	PRN of SV used for fix on channel 5 (empty if no SV)
Field 8	14	PRN of SV used for fix on channel 6 (empty if no SV)
Field 9	19	PRN of SV used for fix on channel 7 (empty if no SV)
Field 10	32	PRN of SV used for fix on channel 8 (empty if no SV)
Field 11	17	PRN of SV used for fix on channel 9 (empty if no SV)
Field 12	1	PRN of SV used for fix on channel 10 (empty if no SV)
Field 13	empty field	PRN of SV used for fix on channel 11 (empty if no SV)
Field 14	empty field	PRN of SV used for fix on channel 12 (empty if no SV)
Field 15	2.0	PDOP (position dilution of precision)
Field 16	1.1	HDOP (horizontal dilution of precision)
Field 17	1.6	VDOP (vertical dilution of precision)
Checksum	*10	
Msg End	<CR><LF>	

RMC (Recommended Minimum Specific GPS Data)

The RMC sentence identifies the UTC time of fix, status, latitude, longitude, and date. Examples are below:

$GPRMC,,V,,,,,,,,,N*53<CR><LF>
$GPRMC,173831.00,A,3827.030,N,12244.020,W,0.08,158.14,200508,,,A*0D<CR><LF>

Msg ID	$GPRMC	
Field 1	173831.00	UTC time of fix (hhmmss.ss)
Field 2	A	GPS receiver warning (A=data valid, V=data not valid)
Field 3	3827.030	Latitude in ddmm.mmm
Field 4	N	Direction of latitude (N=north, S=south)
Field 5	12244.020	Longitude in dddmm.mmm
Field 6	W	Direction of longitude (W=west, E=east)
Field 7	0.08	Speed over ground, knots
Field 8	158.14	Course made good, degrees True
Field 9	200508	Date of fix (ddmmyy)
Field 10	empty field	Magnetic variation
Field 11	empty field	Direction of magnetic variation

Field 12	A	A=autonomous mode, N=data not valid
Checksum	*0D	
Msg End	<CR><LF>	

VTG (Course Over Ground and Ground Speed)

The VTG sentence identifies the actual course and speed relative to the ground. Course over ground degrees Magnetic is not available. Examples are below:

$GPVTG,,T,,,,N,,K,N*61<CR><LF>
$GPVTG,158.14,T,,,0.08,N,0.14,K,A*74<CR><LF>

Msg ID	$GPVTG	
Field 1	158.14	Course over ground
Field 2	T	Fixed text “T” shows degree True
Field 3	empty field	Course over ground (not available)
Field 4	empty field	Degrees Magnetic (not available)
Field 5	0.08	Speed over ground, knots
Field 6	N	Fixed text “N” shows speed over ground is in knots
Field 7	0.14	Speed over ground, km/hr
Field 8	K	Fixed text “K” shows speed over ground is in km/hr
Field 9	A	A=autonomous mode, N=data not valid
Checksum	*74	
Msg End	<CR><LF>	

ZDA (Time and Date)

The ZDA sentence identifies the time associated with the current 1PPS pulse. Each sentence is transmitted within 500 milliseconds after the 1PPS pulse is output and tells the time of the pulse that just occurred. If the Sonoma is unsynchronized then this sentence will be composed of null fields. Examples are below:

$GPZDA,,,,,,*48<CR><LF>
$GPZDA,175658.00,20,05,2008,07,00*69<CR><LF>

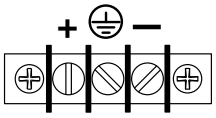
Msg ID	$GPZDA	
Field 1	175658.00	UTC time at 1PPS (hhmmss.ss)
Field 2	20	Day (01 to 31)
Field 3	05	Month (01 to 12)
Field 4	2008	Year (1980 to 2079)
Field 5	07	Local time zone hour, offset from UTC (- for east longitude)
Field 6	00	Local time zone minutes, offset from UTC
Checksum	*69	
Msg End	<CR><LF>	

Power Supply Options

Your Sonoma can be configured with several optional power supply inputs which are listed in ***Appendix H - Specifications***. Dual-redundant power supplies are also available.

DC Power Input

The DC power input uses a a 3-position terminal block and replaces the standard AC power input jack.



Connecting the DC Power

Connect the safety ground terminal to earth ground. Connect the "+" terminal to the positive output of the DC power source. Connect the "-" terminal to the negative output of the DC power source. Note that the Sonoma has a "floating" internal power supply, therefore either the positive or negative output of the DC power source can be referenced to earth ground. This unit will not operate if the +/- connections are reversed; however it will not be damaged by a reverse connection.

SHOCK/ENERGY HAZARD

Install in Restricted Access Location.

Use 10-14 AWG copper wire only.

Terminal block screw torque: 9 lb-in (1 n•M).

Branch circuit must have circuit breaker, 15A or less.

Power must be sourced via two pole disconnect device.

Install terminal block cover after wiring.

Dual-Redundant Power Supplies

Any combination of Universal AC and/or DC supplies is available. Primary and secondary power supplies are connected in a dual-redundant configuration with hitless automatic primary-to-secondary and secondary-to-primary switchover.

A fault detector monitors the status of each redundant power supply. When a fault is detected it will trigger a system alarm. When Sonoma is configured with Dual Power Supplies, an alarm will show if the primary or secondary supply does not have power connected.

Masking Dual Power Supply Fault Alarms

You can mask the Primary and Secondary Faults to prevent them from causing a system alarm. Masking a fault will prevent it from causing the Alarm LED and Alarm Output (if any) from going active. Masking a fault will NOT prevent it from showing in the `gpsstat` command.

To mask the fault you can use the console commands **pwrfltmask** and **setpwrfltmask**. Parameters are either Masked or Enabled. Setting this command to Masked will prevent a power supply fault from creating an alarm condition. The factory default setting is Enabled.

Command: **pwrfltmask**
Sonoma reply:
```
Primary Power Input Fault Alarm is MASKED
Secondary Power Input Fault Alarm is ENABLED
```

Command: **setpwrfltmask MASKED MASKED**
Sonoma reply:
```
Primary Power Input Fault Alarm Mask set to MASKED
Secondary Power Input Fault Alarm Mask set to MASKED
```

This page intentionally left blank.

Appendix *A*

Time Figure of Merit (TFOM)

This appendix describes the Time Figure of Merit number. The TFOM number indicates the level of accuracy that should be included in the interpretation of the time-of-day and ranges from 3 to 9:

3	time error is < 100 nanoseconds
4	time error is < 1 microseconds
5	time error is < 10 microseconds
6	time error is < 100 microseconds
7	time error is < 1 milliseconds
8	time error is < 10 milliseconds
9	time error is > 10 ms, unsynchronized state if never locked to GPS

In all cases, the Sonoma reports this value as accurately as possible, even during periods of GPS signal outage where the Sonoma is unable to directly measure the relationship of its timing outputs to UTC. During these GPS outage periods, assuming that the Sonoma had been synchronized prior to the outage, the Sonoma extrapolates the expected drift of the Sonoma timing signals based on its knowledge of the characteristics of the system oscillator - either the Temperature Compensated Crystal Oscillator (TCXO), Oven Controlled Crystal Oscillator (OCXO) or Rubidium oscillator. The extrapolated TFOM is based on a conservative estimate of the performance of the oscillator and should be considered 'worst case' for a typical benign ambient temperature environment.

Due to this extrapolation behavior, after initial synchronization, brief periods without GPS satellite visibility will not induce an immediate alarm condition. (Removal of the antenna to simulate this will induce an immediate alarm, however.) If the condition persists for long enough periods, you should see the TFOM character change to indicate a gradually deteriorating accuracy of the timing outputs. If the signal loss condition persists longer, then the final, unsynchronized state will eventually be reached. If the Sonoma is unable to re-synchronize within one hour after reaching this state, the Alarm LED will light and the `faultstat` command will show a No Signal Time-Out fault.

If the GPS Subsystem reaches the unsynchronized TFOM state, the NTP daemon will report that it is running at stratum 16 and the leap indicator bits will be set to the fault state. NTP clients will recognize this and cease to use the unsynchronized server.

This page intentionally left blank.

Appendix *B*

Upgrading the Firmware

Periodically, we make bug fixes and enhancements to our Sonoma product line. The Sonoma firmware is freely available on our website at the link shown below. You may securely upgrade your Sonoma firmware via the HTTPS interface or the console port (network/serial).

endruntechnologies.com/support/software-upgrades/sonomaII

NOTE

The Sonoma firmware consists of several different binary files. You may only need one or two of them. The revision history on our website will tell you which files need to be upgraded. The FIT Image containing the Linux RFS(Root File Sysytem), Linux Kernel, and a device-tree, the GPS Subsystem, and the GPS Receiver.

Upgrade via the HTTPS Interface

Software upgrades via the HTTPS interface are simple.
You must first download the appropriate file(s) from the EndRun Technologies website to the computer that you will be using later to access the Sonoma via its HTTPS interface. Use this link to get the file(s) you want:

endruntechnologies.com/support/software-upgrades/sonomaII

After saving the file(s), use the Sonoma HTTPS interface to select one or more for upload to the Sonoma. Then follow the remaining prompts from the HTTPS interface to complete the upgrade(s). (You will need to enter "root" as the user name and enter root's password.)

Upgrade via the Console Port

In order to upgrade via the console port (network or serial) you will need to first download the appropriate firmware image from our website. The Sonoma firmware consists of several different binary files. You may only need one or two of them. The revision history on our website will tell you which files need to be upgraded. The website link is:

endruntechnologies.com/support/software-upgrades/sonomaII

Performing the FIT Image Upgrade

NOTE TO LINUX GEEKS

There are two FLASH disk partitions which hold the compressed FIT Image. These partitions are raw FLASH blocks, have no file system and may not be mounted. They are accessed through low-level device drivers. To protect the factory root file system from accidental erasure or over-writing, the upgrade utilties you will be using will only access the upgrade root file system partiton. When performing an upgrade, you will be erasing and then copying the new image to this device.

First you need to download the FIT Image from the EndRun website to a place on your network which is accessible to the Sonoma. The link to the Sonoma upgrade page is shown above.

Transfer File to Sonoma

You may transfer the file to your Sonoma using **scp**. The FIT image will be named with the software part number and version like: *6010-1009-000_4.00.gz*. When following the instructions below, substitute the name of the actual file image that you are installing for *6010-1009-000_4.00.gz*. Issue these commands from the console of your Sonoma:

Using **scp**, you may open a command window on the remote computer and securely transfer the root file system image from the remote computer to your Sonoma. A command like this should be used:

```
scp -p 6010-1009-000_4.00.fit root@host.your.domain:/tmp/SonomaII.fit
```

Now issue the following command to the Sonoma console to initiate the upload:

```
upgradefit
```

Next, update the default file system partition by issuing this command to your Sonoma console:

```
updaterootflag 1
```

You should see this line displayed:

```
Default FIT File now set to: UPGRADE
```

Finally, reboot the system by issuing this command at the shell prompt:

```
reboot
```

Wait about 90 seconds for the system to shutdown and reboot. Then log in to the Sonoma using **ssh**. If all has gone well, you should be able to log in the usual way. After you have entered your password, the version message will be displayed. You should notice that it now indicates the software version and date of the upgrade that you previously downloaded. You can also check this at any time by issuing

```
fitversion
```

which will cause the FIT version message to be re-displayed.

You can also check to see which FIT image the system is currently booted under by issuing this command at the shell prompt:

```
sysfit
```

Which should cause this to be printed to the console:

```
BOOTED FIT FILE IMAGE = 1 (Upgrade)
```

If so, and your unit seems to be operating normally, you have successfully completed the FIT Image upgrade. If your unit does not boot up successfully, and you are not able to **ssh** into the system after 90 seconds, then there has been some kind of problem with the FIT Image upgrade. It is possible that the file downloaded was corrupt when downloading the file from the EndRun Technologies website.

Recovering from a Failed FIT Image Upgrade

To restore your Sonoma to a bootable state using the factory root file system, you must use the USB port and reboot the Sonoma by cycling the power. Refer to ***Chapter 2 – Basic Installation, Connect the USB Port and Test the USB Port*** for setup details. When you have connected your terminal to the USB port, apply power to the Sonoma.

Pay close attention to the terminal window while the unit is rebooting. After the Linux bootloader displays the message

```
Default FIT: Ok
To override and boot the UPGRADE version of the Fit Image,
type UPGRADE within 5 seconds
.....
Booting with FACTORY FIT
```

you must begin typing “factory” within five seconds to let the bootloader know that you are going to override the default file system. After you hit <enter> the bootloader will boot the factory file system. Watch the rest of the boot process to make sure that you have successfully recovered. If the system boots normally, then you should resolve the problems with the previous file system upgrade and re-perform it.

Wait about 90 seconds for the system to shutdown and reboot. Then log in to the Sonoma using **the USB port** or **ssh**. If all has gone well, you should be able to log in the usual way. You can check the running FIT version at any time by issuing

```
fitversion
```

which will cause the FIT version message to be displayed.

Performing the GPS Subsystem Upgrade

First you need to download the GPS Subsystem firmware from the EndRun website to a place on your network which is accessible to the Sonoma. There are two different versions of the GPS Subsystem firmware.

You may transfer the file to your Sonoma using **scp**. The GPS Subsystem image will be named with the software part number and version like: *6010-0076-000_3.01.bin*. You will be transferring the file to a temporary file, */tmp/subsys.bin* on your Sonoma.

Using SSH to perform the GPS Subsystem upgrade, you may open another command window on the remote computer and securely transfer the GPS Subsystem image to */tmp/subsys.bin* using **scp** from the remote computer. A command like this could be used:

```
scp -p 6010-0076-000_3.01.bin root@host.your.domain:/tmp/subsys.bin
```

Now issue the following command to the Sonoma console to initiate the upload:

```
upgradesubsys
```

This command performs the file transfer to the GPS Subsystem. You will see a file transfer progress message while it is performing the transfer. After it completes, wait about 40 seconds and issue this command to check the GPS Subsystem version:

```
gpsversion
```

You should see a message like this:

```
F/W 6010-0076-000 Ver 3.01 - FPGA 6020-0016-000 Ver 02 - FEB 12 11:59:15 2017
```

The firmware version should match that of the binary file that you uploaded.

Problems with the GPS Subsystem Upgrade

Should you have difficulties with the upgrade due to a corrupt file, power failure during upload, or other accident, do not be alarmed. Even though you may have lost the existing application program, the GPS Subsystem bootloader program will remain intact. Correct any problem with the binary file and retry the upload procedure. If you are still unable to successfully perform the GPS Subsystem upgrade, you should contact Customer Support at EndRun Technologies.

Performing the GPS Receiver Upgrade

This section has instructions for upgrading the EndRun GPS Receiver. If you want to upgrade the GPS Subsystem see the section above called ***Performing the GPS Subsystem Upgrade***.

First you need to download the EndRun GPS Receiver firmware from the EndRun website to a place on your network which is accessible to the Sonoma. The link to the Sonoma upgrade page is shown above. You may transfer the file to your Sonoma using **scp**. The EndRun GPS Receiver image will be named with the software part number and version like: *6010-0081-000_1.04.bin*. You will be transferring the file to a temporary file, */tmp/rcvr.bin* on your Sonoma.

Using SSH to perform the EndRun GPS Receiver upgrade, you may open another command window on the remote computer and securely transfer the GPS Receiver image to */tmp/rcvr.bin* using **scp** from the remote computer. A command like this could be used:

```
scp -p 6010-0081-000_1.04.bin root@host.your.domain:/tmp/rcvr.bin
```

Now issue the following command to the Sonoma console to initiate the upload:

```
upgradercvr
```

This command performs the file transfer to the EndRun GPS Receiver. You will see a file transfer progress message while it is performing the transfer. Next, issue the following command to the Sonoma console to reset the GPS Subsystem (and Receiver):

```
subsysreset
```

After it completes, wait about 60 seconds and issue this command to check the EndRun GPS Receiver version:

```
rcvrversion
```

You should see a message like this:

```
F/W 6010-0081-000 Ver 1.31 - FPGA 6020-0014-000 Ver 0004 - DEC 26 09:10:59 2023
```

The firmware version should match that of the binary file that you uploaded.

Problems with the GPS Receiver Upgrade

Should you have difficulties with the upgrade due to a corrupt file, power failure during upload, or other accident, do not be alarmed. Even though you may have lost the existing application program, the GPS Receiver bootloader program will remain intact. Correct any problem with the binary file and retry the upload procedure. If you are still unable to successfully perform the EndRun GPS Receiver upgrade, you should contact Customer Support at EndRun Technologies.

Performing the GPS Receiver FPGA Upgrade

This section has instructions for upgrading the Field-Programmable Gate Array (FPGA) resident on the EndRun GPS Receiver. This is rarely, if ever, used. Therefore, it's not an option on the HTTPS interface.

First you need to download the FPGA image from the EndRun website to a place on your network which is accessible to the Sonoma. The link to the Sonoma upgrade page is shown above.

You may transfer the file to your Sonoma using **scp**. The FPGA image will be named with the image part number and version like: *6020-0014-000_02.rbf*. When following the instructions below, substitute the name of the actual FPGA image that you are installing for *6020-0014-000_02.rbf*. You will be transferring the file to a temporary file, */tmp/rcvrfpga.rbf* on your Sonoma.

Using SSH to perform the EndRun GPS Receiver upgrade, you may open another command window on the remote computer and securely transfer the FPGA image to */tmp/fpga.bin* using **scp** from the remote computer. A command like this could be used:

```
scp -p 6020-0014-000_02.rbf root@host.your.domain:/tmp/rcvrfpga.rbf
```

Now issue the following command to the Sonoma console to initiate the upload:

```
upgradercvrfpga
```

This command performs the file transfer to the FPGA on the EndRun GPS Receiver. You will see a file transfer progress message while it is performing the transfer. Next, issue the following command to the Sonoma console to reset the GPS Subsystem (and Receiver):

```
subsysreset
```

After it completes, wait about 60 seconds and issue this command to check the FPGA version on the GPS Receiver:

```
rcvrversion
```

You should see a message like this:

```
F/W 6010-0081-000 Ver 1.04 - FPGA 6020-0014-000 Ver 02 - OCT 11 13:08:52 2015
```

The FPGA version should match that of the binary file that you uploaded.

Appendix C

Helpful Linux Information

You do not need knowledge of Linux commands in order to operate the Sonoma. All commands necessary for proper operation are described in ***Chapter 9 - Console Port Control and Status****. However, the Sonoma does support a subset of the standard Linux commands and utilities and it uses the* `bash` *shell, which is the Linux standard, full-featured shell. Very brief descriptions of some of the most useful Linux information is described in this appendix.*

Linux Users

Sonoma is shipped from the factory with two users enabled. The first is the "root" user with password "endrun_1". The root user has access to everything on the system, including the ability to perform system setup procedures.

The other user is "ntpuser" with password "Praecis". When logged in as ntpuser you may check status information and view log files but you will not be able to modify any system settings or view secure files.

For security reasons, we recommend you change the default passwords using the Linux `passwd` command (see ***Change Password*** below).

More user can be added if needed. (see Add Users below)

Linux Commands

Detailed Information Is Available

A very brief description of the most helpful Linux commands and utilities is listed in this appendix. On Linux systems, the system commands are located in the directories with "bin" in their name, e.g. */usr/bin* or */sbin*. You can list the contents of those directories using the `ls` command to see what is installed on your Sonoma. Then you can find out about those commands using the `man` command, which stands for "manual". For example, to read details on the `ps` command type this:

```
man ps
```

A very detailed description, called a "man page", of the `ps` command will be shown. To navigate in the document, press `d' to scroll down, `b' to scroll up, and `q' to quit and return to the command prompt.

To search the database of man pages, use either `apropos` or `whatis`. `apropos` will do partial word searches, while `whatis` will only find matching whole words. For example to find all man pages dealing with ntp:

```
apropos ntp
```

The relevant available man pages are shown:

```
ntp []                (1)  - keygen - Create a NTP host key
ntpd []               (1)  - NTP daemon program
ntpdc []              (1)  - vendor-specific NTP query program
ntpq []               (1)  - standard NTP query program
ntpsnmpd []           (1)  - NTP SNMP MIB agent
sntp []               (1)  - standard SNTP program
```

Now you can issue issue **man** commands on each of these man pages to find what you are looking for.

Add User

The following steps tell you how to add a user to the Sonoma and how to set the password or change the password. You must be logged in as the "root" user in order to perform the following.
There are two commands that will be used, **useradd** and **chpasswd**.
To add a new user type the following where newuser is the name of the user to add:

```
useradd   newuser
```

To assign a password (newpassword) to the newuser type:

```
chpasswd
```

and type the input:

```
newuser:newpassword
```

When done type:

```
Ctrl+D
```

Change Password

This command is used to change the password for the user that you are logged in as. It affects the USB port, SSH and HTTPS.

```
passwd
```

List Active Processes

This command displays all active processes running in the system.

```
ps -e
```

NTP Monitoring and Troubleshooting

The following command displays which NTP clients are reaching the NTP daemon running on the Sonoma. It will not try to look up host names:

```
ntpq -n -c mrulist
```

A useful command for querying NTP status is the following:

```
ntpq -peers
```

To query a remote time server (if the remote timeserver will accept the query) type:

```
ntpq -peers <hostname>
```

A table of information will be displayed. For details on what each of the table columns means type:

```
man ntpq
```

To see what version of the NTP daemon, ntpd, is operating type:

```
ntpd --version
```

Text Editors

There are three text editors resident on the Sonoma file system: **edit**, **joe** and **elvis**. All of these may be useful when needing to edit system configuration files or to view and search within system log files.

edit is a very simple editor with Wordstar key commands that was originally developed for extremely memory-limited environments, such as floppy boot disks and embedded Linux appliances. When EndRun Technologies' first generation Linux-based embedded network time servers were introduced, they fell into this category and the **edit** text editor was appropriate. Now it is included on the Sonoma file system for legacy reasons, since it has been the default editor for all first and second generation EndRun Technologies products. A man page for **edit** is resident on the system. When it is first started, and you did not give it a file name to edit on the command line, it shows a start-up screen with its command syntax, But once you have opened a file to edit, online help is not available. It is started by issuing the command **edit [file-to-edit]**, optionally with a file name to edit.

joe is the modern replacement for **edit** on the Sonoma. It is a full-featured editor with syntax highlighting and is also based on the Wordstar commands. It is user friendly with easy to find help for its key commands, and complete man page documentation. It is the recommended editor for all purpose use in configuring and monitoring the Sonoma time server. It is started by simply issuing the command **joe [file-to-edit]**, optionally with a file name to edit.

elvis is a full-featured **vi** clone which is provided in the Sonoma file system for masochistic Unix diehards. It is not the least bit user friendly to anyone lacking experience with text mode applications. If you don't know what **vi** is, avoid using this editor! It is started by simply issuing the command **vi [file-to-edit]**, optionally with a file name to edit.

Change Log-In Banners

There are three different log-in banners in the Sonoma - the USB port banner and the SSH banner. You must be logged in as the "root" user in order to edit the *rc.local* file and change the log-in banners. Perform the following:

```
edit /etc/rc.d/rc.local
```

Change the banners as appropriate. After saving the file, copy it to */boot/etc* like this:

```
cp -p /etc/rc.d/rc.local /boot/etc/rc.d
```

Then reboot for your changes to take effect.

Query and Change Ethernet Ports

`ethtool` is a Linux utility that allows you to query or change the settings for Port 0 (`eth0`) and Port 1 (`eth1`). For example, to view current settings for Port 0 issue the following command:

```
ethtool eth0
```

Here is an example of one way to set the speed on Port 0 to 1000Base-T:

```
ethtool -s eth0 speed 1000 duplex full autoneg off
```

The command above will immediately change the port speed to 1000Base-T, but it will revert to its factory (100/1000Base-T) at a system reset. If you want to retain the setting after a system reset, then you need to edit the *rc.M* configuration file. Follow this sequence:

1. Edit */etc/rc.d/rc.M* using one of the editors on the previous page.
Insert the desired `ethtool` line (see example above) after the Gatekeeper Daemon is started and before the Precision Time Protocol is started. Exit and save the *rc.M* file.

2. Now you need to copy the *rc.M* file into a location that will ensure your changes persist through a system reset. Copy */etc/rc.d/rc.M* to */boot/etc/rc.d* as shown:

```
cp /etc/rc.d/rc.M /boot/etc/rc.d
```

For more details on `ethtool` and how to use it type:

```
man ethtool
```

Redirect Syslog Files to Remote Host

You can redirect syslog files to a remote host (syslog server) by adding the standard Linux redirect commands to the Sonoma's *syslog.conf* file. Follow this sequence:

1. Edit */etc/syslog.conf* using one of the editors on the previous page. Insert this line:

```
*.* @remote_host
```

Substitute the actual name or IP address of your remote syslog server for "remote_host". The most common log file to be directed to the Syslog Server is the *messages.log* file which contains authenticated user login activity. If you would like to only redirect this log info to the remote host, insert this line instead of the one above:

```
messages.log @remote_host
```

Exit and save the *syslog.conf* file.

2. Now you need to copy the *syslog.conf* file into a location that will ensure your changes persist through a system reset. Copy */etc/syslog.conf* to */boot/etc/syslog.conf* as shown:

```
cp /etc/syslog.conf /boot/etc/syslog.conf
```

Appendix *D*

Third-Party Software

The Sonoma is running several different software products created and/or maintained by open source projects. Open source software comes with its own license. These are printed out for your information below.

The license for the GNU software project requires that we provide you with a copy of all source code covered under the GNU Public License (GPL) at your request. Please contact us with your request and we will mail it to you on a CD. We will charge you a fee for our incurred expenses as allowed for in the license.

The Kravietz / pam_tacplus software license is covered under the following GNU General Public Licence.

GNU General Public License

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

Copyright © 2007 Free Software Foundation, Inc. <https://fsf.org/>

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

NTP Software License

Information about the NTP Project can be found at www.ntp.org. The distribution and usage of the NTP software is allowed, as long as the following copyright notice is included in our documentation. For more information see: https://opensource.org/licenses/ntp-license.php

```
********************************************************************************
*                                                                              *
* Copyright (c) University of Delaware 1992-2015                               *
*                                                                              *
* Permission to use, copy, modify, and distribute this software and            *
* its documentation for any purpose with or without fee is hereby              *
* granted, provided that the above copyright notice appears in all             *
* copies and that both the copyright notice and this permission                *
* notice appear in supporting documentation, and that the name                 *
* University of Delaware not be used in advertising or publicity               *
* pertaining to distribution of the software without specific,                  *
* written prior permission. The University of Delaware makes no                *
* representations about the suitability this software for any                   *
* purpose. It is provided "as is" without express or implied                   *
* warranty.                                                                    *
*                                                                              *
```

Apache Software License

PTP Software License

The PTP/IEEE-1588 option as implemented in the Sonoma is covered by patents and copyrights. For patents that pertain to the Std No 1588, see the IEEE Standards Association.

Information about the PTP Project, led by Kendall Correll, can be found at:
ptpd.sourceforge.net

The distribution and usage of the PTP software is allowed, as long as the following copyright notice is included in our documentation. The copyright notice applies to all files which compose the PTPd. This notice applies as if the text was explicitly included in each file.

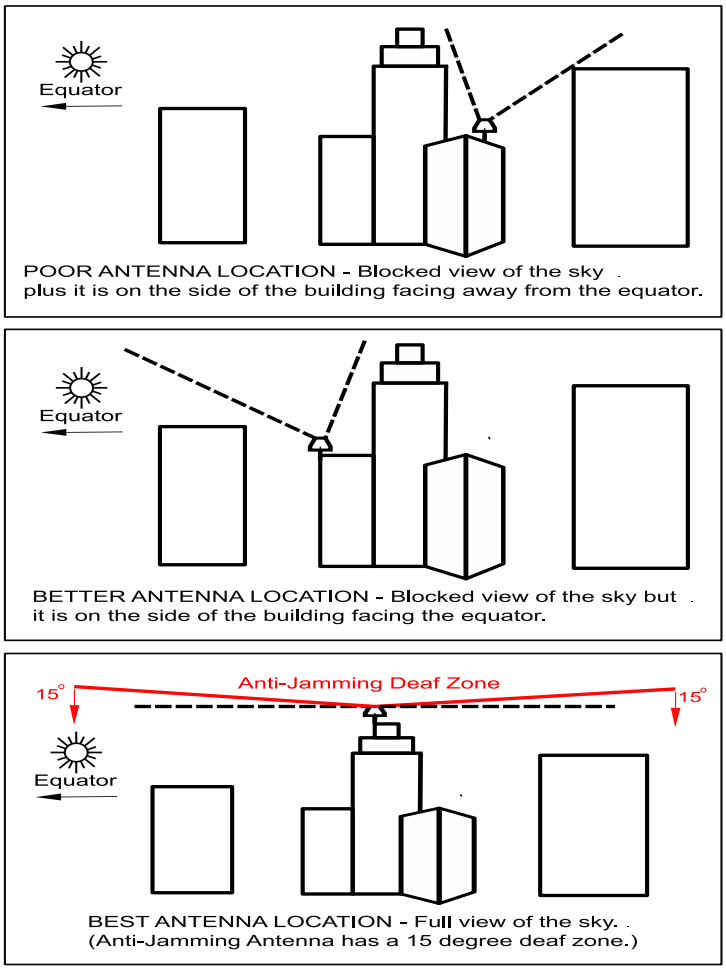
Appendix *E*

Installing the GPS Antenna

This appendix contains guidelines for installing the GPS antenna. The majority of this appendix is devoted to rooftop installations. The last sections contains information on a window-mount installation and on obtaining a GPS reference position.

Antenna Location

The location of the antenna must be chosen based on having as clear a view of the sky as possible. Any obstructions such as buildings, large metal objects or other antennas, and even trees, will limit the performance of the GPS antenna. The antenna should also be located away from overhead power lines or circuits, for safety reasons. The illustration below shows some examples of good and bad antenna mounting locations.



GPS Antenna Kit

The time server typically ships with an optional GPS Antenna Kit which includes 50 feet (15 meters) of antenna cable. This amount of cable is sufficient for the majority of GPS antenna installations. Longer cable runs can also be accommodated. Below is a list of the items in a typical GPS Antenna Kit:

- GPS Antenna
- Mounting Pipe
- Hose Clamps
- 50 feet of RG-59U (Belden 9104) Cable/TNC Male

Complete GPS Roof-Top Installation Guide for both antennas is here:
endruntechnologies.com/pdf/5050-0017-000.pdf

About Coax Cable

The GPS signal frequency is considered to be in the microwave range and is highly affected by impedance mismatches and discontinuities in the transmission cables. All RF coax cables have a minimum bend radius. In order to prevent damage, cable should not be bent into tight curves. It is critically important during installation that kinks are not allowed to form in the cable. If RF coax cable is bent beyond its minimum bend radius. then damage to the inner construction of the cable may result. This can lead to much higher levels of loss and a non-functioning GPS receiver.

Similarly, care should be taken to ensure that the cable is not crushed, or likely to be crushed later. If the RF coax cable does suffer this kind of damage, then the dimensions of the cable will be changed and it will not maintain its characteristic impedance. Again, this can result in a non-functioning GPS receiver.

Please keep the above precautions in mind when you install the GPS cable. It should not be treated like a garden hose or a power extension cord.

Long Cable Runs

Most GPS Time Servers are installed with only 50 feet (15 meters) of antenna cable. However, there are many circumstances where 50 feet is inadequate. EndRun can accommodate a cable length of up to 1000 feet using a combination of low-loss cable and preamplifiers.

Recommended Cable

The factory-supplied GPS cable is an RG-59 type. RG-59 is a broad classification, with wide variation in performance between cables from different manufacturers and for different applications. EndRun supplies two specific cables: Belden 9104 or Belden 1505A. Both cables are double shielded, low loss cables designed for the cable TV industry, and have equivalent performance at the GPS frequency with loss of 10 dB/100 feet. The difference between these two cables is the DC resistance, which becomes important for very long cables. Belden 9104 is constructed with a copper-

plated steel center conductor and an aluminum outer braid. Belden 1505A is constructed of all solid copper conductors and has very low DC resistance. For very long cables, if the DC resistance is too high, not enough voltage will be available at the end farthest from the Sonoma timeserver where the antenna and preamplifiers are installed. For cable lengths less than 700 feet, Belden 9104 is acceptable. Longer runs require Belden 1505A.

If you are responsible for the GPS installation and you are supplying the cable, then you must make sure the cable you install is comparable to these cables, with 10 dB or less of loss per 100 feet at 1.5 GHz. If the cable length is longer than 700 feet, you must make sure that the cable has equivalently low DC resistance to the Belden 1505A type. Choosing an inferior cable type can cause a myriad of GPS reception problems. You will also need preamplifiers if the cable length is greater than 250 feet. See the chart below for details.

Using GPS Preamplifiers

EndRun produces a GPS Preamplifier which is a very high-performance, low-noise, low-power drain, inline amplifier for difficult GPS signal environments and long cable runs (greater than 250 feet of factory-supplied cable). The following table shows the number of preamplifers we recommend for each GPS antenna installation using our factory-supplied cable. Installations using other cable types may have different preamplifer requirements.

Cable Length	Cable Type	Number of Preamplifiers
Up to 250 feet (76 meters)	RG-59 Belden 9104	0
251 to 500 feet (77 to 152 meters)	RG-59 Belden 9104	1
501 to 700 feet (153 to 213 meters)	RG-59 Belden 9104	2
701 to 750 feet (214 to 228 meters)	RG-59 Belden 1505A	2
751 to 1000 feet (229 to 305 meters)	RG-59 Belden 1505A	3

A page of the Installation Guide for installing a rooftop-mounted antenna with GPS preamplifer is shown at the end of this appendix in Figure 2. Complete guide is here:
endruntechnologies.com/pdf/5050-0004-000.pdf

Using Three Preamplifiers

Installation for one or two preamplifiers is simple. But the physical layout of three preamplifiers is critical. Preamplifiers should be in a straight line departing from the bottom of the antenna so that any leakage from the downlead cable is as far from the antenna as possible. A positive feedback path can occur from the output of the last pre-amp, through the cable shield and back up to the antenna. This highlights the importance of properly constructed cable terminations and double shielded cable.

For installations using three preamps, we recommend that the last pre-amp be located as far as is practical from the antenna. This is because the antenna and three preamplifers will have more than 100 dB of gain, increasing the likelihood that enough leakage from the cable can cause “round-the-

world" feedback to the antenna and set up oscillation. Here is the suggested configuration for an antenna installation with three preamplifiers:

GPS antenna
One foot cable
Preamplifier
One foot cable
Preamplifier
Up to 1,000 feet (305 meters) cable
Preamplifier
One foot cable
Sonoma GPS Time Server

Other Accessories

Lightning Arrestor

A lightning arrestor helps protect your GPS installation from damage due to lightning strikes. It is designed to pass the DC voltage that is needed to power the antenna and/or preamps without degrading the GPS signal. It is installed between the antenna and the receiver where the cable enters the building, near an earth-ground. You must bond the lightning arrestor to the earth-ground.

Signal Splitters

Signal splitters are used when two time servers are sharing one antenna installation. The smart GPS Splitter supplied by EndRun is a one-input, two-output device. In the normal configuration, one of the splitter RF outputs (J1) passes DC from the connected GPS Receiver through the splitter to the antenna, allowing the GPS Receiver to power both the antenna and the splitter amplifier. The other RF output (J2) is DC loaded with a 200-ohm resistor to simulate the antenna current draw.

When selecting and installing a signal splitter keep these points in mind:

1. The splitter must be DC-blocked on one leg. The GPS Receivers in both time servers output 5 VDC up the coax to power the GPS antenna's built-in preamp. You must not connect these two power sources together.

2. It is desirable that the DC-blocked leg has a DC load resistor to simulate a GPS antenna load. This way you will not get a false alarm from the GPS Receiver's antenna load sensor. However, the Sonoma time server allows you to mask an antenna fault alarm from causing a system fault by using the `setantfltmask` command. See details in ***Chapter 9 - Console Port Control and Status***.

3. The signal splitter supplied by EndRun has a built-in preamplifier to compensate for signal loss through the splitter. If using a splitter other than the one supplied by EndRun you may need to compensate for splitter signal loss by using a separate GPS preamplifier.

Calibrate Your Receiver

If your Sonoma is operating with the Precision Time Protocol (PTP), then you may wish to calibrate your GPS receiver for maximum timing accuracy. In order for the Sonoma to synchronize with maximum accuracy to UTC, the delay for the cable and all devices between the antenna and the GPS receiver input (i.e. GPS preamplifiers, signal splitters, lightning arrestors, etc.) must be compensated for. You can do this via the keypad/display (see ***Chapter 11 - Front-Panel Keypad/Display, Receiver: Calibrate***) or via the console port `caldelay` and `setcaldelay` commands (see ***Chapter 9 - Console Port Control & Status)***.

Calibration is used to compensate for the propagation delay between the GPS antenna and the Sonoma GPS receiver input connector. Positive values remove delay by advancing Sonoma's 1 PPS on-time reference by the specified number of nanoseconds. Negative values add delay by retarding the 1 PPS and are used in special circumstances. The calibration value is determined by summing all the delays.

The calibration range is ±500,000 nanoseconds. The default value as shipped from the factory is 0.

The table below lists nominal propagation delays for the GPS cable and accessories supplied by EndRun Technologies. For the most demanding timing applications, it is recommended that the delay between the antenna and Sonoma receiver input be precisely measured.

Part Number	Description	Delay	Notes
0502-0013-000	Standard GPS Antenna	0 seconds	None
0502-0030-000	Multi-GNSS Anti-Jam Antenna	0 seconds	None
0610-0009-001	Antenna Kit with 50' (15m) cable	62 ns	Belden 9104, 1.24ns/ foot
0600-0013-050	50' (15 m) cable	62 ns	Belden 9104, 1.24ns/ foot
0600-0013-100	100' (30 m) cable	124 ns	Belden 9104, 1.24 ns/foot
0600-0013-150	150' (46 m) cable	186 ns	Belden 9104, 1.24 ns/foot
0600-0013-200	200' (61 m) cable	248 ns	Belden 9104, 1.24 ns/foot
0600-0013-250	250' (76 m) cable	310 ns	Belden 9104, 1.24 ns/foot
0600-0060-800	800' (244 m) cable	992 ns	Belden 1505A, 1.24 ns/foot
0600-0060-A00	1000' (304 m) cable	1240 ns	Belden 1505A, 1.24 ns/foot
3509-0001-000	G-LNA2 (GPS Low-Noise Amp)	20 ns	Exact # is on device label.
4011-0002-000	G-LNA2 Kit (includes 1' cable)	21 ns	Exact # is on device label. Add 1.24 ns for 1 foot cable
0502-0009-000	Lightning Arrestor	<1 ns	None
0502-0011-000	GPS Signal Splitter	<1 ns	None
3430-0003-000	Fiber Optic Link Receiver	17 ns per Receiver/ Transmitter	Add the delay of single mode fiber optic cable which is typically pair 1.4/1.5 ns/foot. See cable spec.
3430-0004-000	Fiber Optic Link Transmitter		
3430-0005-000	Fiber Optic Link Transmitter		

Mounting On A Rootop

Mounting your GPS antenna with an unobstructed view of the sky (usually on a rooftop) is the recommended installation. Please follow these guidelines to eliminate exposure to electrical service wiring and to minimize the potential for lightning strikes.

Installations subject to lightning strikes should use a lightning arrestor installed at the building entrance. A lightning arrestor suited for this purpose is available through EndRun Technologies. The arrestor must be installed according to the manufacturer's instructions.

Do NOT route the antenna wiring near or with AC wiring (Class 1 circuits per the NEC). Do NOT mount the antenna wiring where it may become energized by nearby AC wiring or components should they fall.

Mounting Inside A Window

For GPS time servers, it is possible to mount the GPS antenna inside a window and have it perform adequately. Avoid windows with metallic film coating that will inhibit GPS signals and ensure that the window has a good view of the sky. If you are in the Northern hemisphere, then a south-facing window is best and in the Southern hemisphere, the opposite is true.

Your Sonoma needs to calculate its position in order to operate properly. It only needs to do this once, but it requires that four satellites are visible at least some of the time. If your Sonoma has a limited view of the sky, it may not be able to see the required four satellites, so you will need to manually enter your position. See ***Obtaining a Reference Position*** below for instructions.

Because of the reduced sky visibility that is characteristic of a window-mount installation, your time server may go through many hours without locking to a GPS signal. This is fine, as long as it locks for 10-15 minutes at least once every 24 hours. If the time server goes longer than 24 hours without locking, then it will stop serving Stratum 1 time. An OCXO upgrade will allow the time server to go for 35 days without receiving a GPS signal and is extra insurance for window-mount installations.

A window-mount antenna kit is available from EndRun. See installation guide here:
endruntechnologies.com/pdf/5050-0023-000.pdf

Note: We do not recommend mounting the optional Anti-Jam Antenna with the window-mount.

Obtaining A Reference Position

Your Sonoma is capable of operation from either an automatically determined GPS reference position or a manually entered GPS reference position. If you need to provide a reference position to your Sonoma because you are using a window-mounted antenna with inadequate satellite visibility, there are two good ways to do it: 1) use a handheld GPS receiver to obtain a position near the location of your Sonoma antenna or 2) reference a geodetic (World Geodetic Survey of 1984 (WGS-84)) database to obtain a position for your street address.

Using a Handheld GPS Receiver

Obtain an inexpensive, handheld GPS receiver. Use it outside of the building to determine a position that is within 100 meters of the installed Sonoma antenna. Make sure that the handheld GPS receiver is configured to report its positions in the WGS-84 datum. Record the position and then make any adjustments to the height that might be necessary if the antenna is installed in a high-rise building. Input it to the Sonoma via the `setgpsrefpos` command.

Using the Internet

Reasonably accurate position information can be obtained from various websites on the Internet. Using your favorite search engine, type in a search term such as: “street gps position”. Many of the websites displayed will give you the ability to type in your location and provide your GPS position coordinates. The position needs to be accurate, to within 100 meters of the actual antenna location. If you are unable to obtain a GPS ellipsoidal height (WGS-84) then you can do that by following the instructions in ***About WGS-84 Height*** below.

Record the position and then make any adjustments to the height that might be necessary if the antenna is installed in a high-rise building. Input it to the Sonoma via the `setgpsrefpos` command. (See ***Chapter 9 - Console Port Control and Status***.)

About WGS-84 Height

Internally, GPS receivers report latitude, longitude and height above the WGS-84 ellipsoid. However, for a lot of reasons, WGS-84 is not the way that mapmakers and surveyers report the height. That means, in order to use the height information as reported by Sonoma, you need to do a conversion. One easy way to do the conversion is by going to this link:

unavco.org/software/geodetic-utilities/geoid-height-calculator/geoid-height-calculator.html

After entering your latitude and longitude, this website will give you a report showing the GPS ellipsoidal height, the Geoid height, and the Orthometric height. The Orthometric height is the one most people are familiar with, which is height above mean sea level. However, GPS receivers use the GPS ellipsoidal height. Below is a sample report:

GPS ellipsoidal height = 0 (meters)
Geoid height = -31.023 (meters)
Orthometric height (height above mean sea level) = 31.023 (meters)

This page left intentionally blank.

Appendix *F*

Leap Seconds

UTC stands for Coordinated Universal Time. UTC is the international time standard most commonly used in the world and is the one used by the Network Time Protocol (NTP). A leap second insertion is scheduled about every 1½ to three years in order to keep UTC in alignment with the earth's rotation. Possible leap second insertions can be scheduled at midnight (after 23:59:59) on June 30 or December 31.

Automatic Leap Second Insertion

Your GPS-synchronized Sonoma precisely adjusts for leap seconds if and when they occur. There is nothing you need to do in order to keep your Sonoma time server accurately synchronized to UTC.

You can see the current GPS-UTC parameters that are downloaded from the satellites by using the `gpsutcinfo` command. See ***Chapter 9 - Console Port Control and Status*** for details on this command or type `help gpsutcinfo` at the console port.

Background Information

Leap seconds are inserted from time-to-time in order to keep UTC, which is derived from atomic time (TAI), in agreement with the Earth's rotation rate. Relative to TAI, the Earth's rotation rate is slowing down. This means that UTC must be retarded periodically in order to maintain agreement between UTC and the apparent daylength. If this were not done, eventually UTC would drift out-of-sync with Earth's day and many astronomical and navigational problems would ensue.

The International Earth Rotation Service (IERS) is the organization responsible for measuring the relationship between UTC and the rotation rate of the Earth. When the difference between UTC and apparent Earth time has exceeded a certain threshold, the IERS coordinates with the Bureau International of the Hour (BIH) to schedule the insertion of a leap second into the UTC time scale. The IERS publishes Bulletin C about 6 months in advance of each possible leap second insertion point. Bulletin C confirms whether a leap second will or will not be inserted at the next possible insertion point. The IERS website is:

iers.org

EndRun summarizes this information at this link:

endruntechnologies.com/support/leap-seconds

This page intentionally left blank.

Appendix *G*

System Faults

The status of the Sonoma is constantly monitored and a fault will occur when any of several parameters is out of spec. When this happens the Alarm LED on the front panel will light. This appendix defines the various faults.

Overview

The Alarm LED will light when a fault has occurred. You can see which fault is the problem by using the `faultstat` command.

Masking Faults

Some faults can be masked. These are the ANT (GPS Antenna) and SIG (GPS Signal) faults. When masked, these faults will not cause an alarm. You may want to mask the ANT fault if you are using a GPS splitter. You may want to mask the SIG fault if you are operating your Sonoma as a Stratum 2 server and are not using a GPS signal. For information on Stratum 2 see ***Chapter 2 - NTP, Configuring the Sonoma as a Stratum 2 Server***.

To mask a fault use the `setantfltmask` and `setsigfltmask` commands. For more information see ***Chapter 9 - Console Port Control and Status*** or type `help setsigfltmask` and `help setantfltmask` on the console.

If your Sonoma has the Dual Power Supply option then you may mask primary and/or secondary power supply faults. See ***Chapter 10 - Options, Masking Dual Power Supply Fault Alarms*** for more information.

System Fault Definitions

System Oscillator DAC (DAC)

This fault indicates that the electronic frequency control DAC for the oscillator has reached either the high or low alarm limit while locked to the GPS signal. Unless the unit is being subjected to out-of-specification environmental conditions, this would indicate that the oscillator frequency has drifted near to the end of life region. This should normally only occur after at least ten years of operation. The unit will continue to function until the oscillator frequency finally reaches one of the actual DAC endpoints. The unit should be returned to the factory for oscillator replacement at your convenience.

GPS Signal (SIG)

This fault indicates that the unit has not been able to acquire a GPS signal for one hour while the Time Figure of Merit has been 9, the unsynchronized condition. This could be due to a variety of reasons. If there are no other faults that could explain the inability to receive a signal, then there could be an antenna failure or blockage. If the condition persists indefinitely, and a problem with the antenna is not evident, then please contact EndRun Customer Support.

GPS Subsystem FPGA Configuration (FPGA)
This fault indicates that the GPS Subsystem is unable to configure the FPGA. This is a fatal fault. Please contact EndRun Customer Support.

GPS Subsystem FLASH Writes (FLSH)
This fault indicates that the GPS Subsystem is unable to verify a write to the FLASH non-volatile parameter storage area. This should not ever occur under normal operation.. Please contact EndRun Customer Support.

GPS Receiver Communication (RCVC)
This fault indicates that the GPS Subsystem is unable to establish communications with the GPS Receiver. Please contact EndRun Customer Support.

GPS Reference Time (REF)
This fault indicates that the GPS Subsystem received an erroneous time input from the GPS Receiver. If the condition persists please contact EndRun Customer Support.

Subsystem Communication (POLL)
This fault indicates that the GPS Subsystem is not receiving polling requests from the Linux Subsystem. This could be due to a hardware or software failure. If the condition persists please contact EndRun Customer Support.

GPS Receiver Fault (RCVF)
This fault indicates that the GPS Receiver has a fault. See the next section, ***Receiver Fault Definitions*** for details.

System Oscillator PLL (PLL)
This fault indicates that there is an unlock condition between the main system oscillator and the other system timebase clocks. This is a fatal fault. Please contact EndRun Customer Support.

GPS Antenna (ANT)
This fault indicates that the GPS antenna or cable has a fault. It indicates either an over or under current condition. Usually it means that the antenna cable is not plugged into the connector on the rear of the Sonoma. This fault may also occur when using an antenna signal splitter. In this case you may want to mask the fault. Use the `setantfltmask` command.

System Power/Configuration (PWR)
This fault indicates misconfiguration of the Sonoma chassis which may have caused a power overload. This is a fatal fault. Please contact EndRun Customer Support.

Primary Power Supply (PRIPS) - Option
Used only when the Dual-Redundant Power Supplies are installed. This fault indicates that the primary power supply is not producing an output. See ***Chapter 10 - Options, Dual-Redundant Power Supplies*** for information on the dual power supplies option.

Secondary Power Supply (SECPS) - Option
Used only when the Dual-Redundant Power Supplies are installed. This fault indicates that the secondary power supply is not producing an output.. See ***Chapter 10 - Options, Dual-Redundant Power Supplies*** for information on the dual power supplies option.

Receiver Fault Definitions

When a fault on the EndRun GPS Receiver occurs, the system fault indicator RCVF will show fault and the Alarm LED will light. You can see which fault is the problem by using the `faultstat` command. Below are details about each fault indicator.

GPS Receiver Oscillator DAC (DAC)
This fault indicates that the DAC for the oscillator has reached either the high or low alarm limit while locked to the GPS signal. Unless the unit is being subjected to out-of-specification environmental conditions, this would indicate that the oscillator frequency has drifted near to the end of life region. This should normally only occur after at least ten years of operation. The unit will continue to function until the oscillator frequency finally reaches the DAC endpoint. The unit should be returned to the factory for oscillator replacement at your convenience.

GPS Signal (SIG)
This fault indicates that the GPS Receiver has not been able to acquire a GPS signal for one hour while the Time Figure of Merit has been 9, the unsynchronized condition. This could be due to a variety of reasons. If there are no other faults that could explain the inability to receive a signal, then there could be an antenna failure or blockage. If the condition persists indefinitely, and a problem with the antenna is not evident, then please contact EndRun Customer Support.

GPS Receiver FPGA Configuration (FPGA)
This fault indicates that the GPS Receiver is unable to configure the FPGA. This is a fatal fault. Please contact EndRun Customer Support.

GPS Receiver FLASH Writes (FLSH)
This fault indicates that the GPS Receiver is unable to verify a write to the FLASH non-volatile parameter storage area. This should not ever occur under normal operation.. Please contact EndRun Customer Support.

Synthesizer Limits (SYN1)
This fault indicates that the local oscillator synthesizer has reached the alarm limit. This condition should not normally occur unless the unit is subjected to out-of-specification environmental conditions. Otherwise, this is a fatal fault. Please contact EndRun Customer Support.

Synthesizer (SYN2)
This fault indicates that the local oscillator synthesizer has failed. This condition should not normally occur unless the unit is subjected to out-of-specification environmental conditions. Otherwise, this is a fatal fault. Please contact EndRun Customer Support.

GPS Reference Time (REF)
This fault indicates that the GPS Receiver received an erroneous time input from the GPS signals. If the condition persists please contact EndRun Customer Support.

GPS Receiver Oscillator (OSC)
This fault indicates that the main oscillator has failed. This is a fatal fault. Please contact EndRun Customer Support.

Antenna Short (SHRT)
This fault indicates that the GPS antenna has an overcurrent condition (short).

Antenna Open (OPEN)
This fault indicates that the GPS antenna has an undercurrent condition (open).

GPS Receiver Oscillator PLL (Phase-Lock-Loop)
This fault indicates that there is an unlock condition between the receiver oscillator and the other system timebase clocks. This is a fatal fault. Please contact EndRun Customer Support.

Appendix *H*

Specifications

GPS Receiver:

EndRun GPS Timing Receiver.
L1 Band – 1575.42 MHz.
12 Channels, C/A Code.
Single-satellite mode and dynamic-platform mode (shipboard only at less than 60 mph).
15 dB minimum gain at receiver input.
Timing Receiver Autonomous Integrity Monitoring (TRAIM).
Proprietary GPS sub-frame error checking and filtering.

GPS Antenna Kit (Option):

Antenna

TNC jack on rear panel, Z_{in} = 50Ω, antenna power = +5V.
Integral +40 dB gain LNA with bandpass filter for out-of-band interference rejection.
Rugged, all-weather housing capable of operation over –40°C to +85°C.
MTBF: 163,441 hours at 70° C.
Size: 3.25”H x 3.0” diameter.

Anti-Jam Antenna

TNC jack on rear panel, Z_{in} = 50Ω, antenna power = +5V.
Integral +38 dB gain LNA with bandpass filter for out-of-band interference rejection.
Rugged, all-weather housing capable of operation over –40°C to +85°C.
Mitigates jamming signals below 15 degrees
Size: 5”H x 4” diameter.

Mounting via 18” long, ¾” Aluminum pipe with stainless steel clamps.
50’ low-loss RG-59 downlead cable is typical cable length.
Other cable lengths and low noise pre-amplifiers are available.

System Oscillator:

TCXO is standard (2.5×10^{-6} over -20° to 70° C).
Option: OCXO (4×10^{-9} over 0 to 70° C).
Rubidium (1×10^{-9} over 0 to 70°C).
Stratum 1 Holdover Performance: 24 Hours - TCXO
35 Days - OCXO
140 Days - Rubidium

Time to Lock:

< 5 minutes, typical (TCXO).
< 10 minutes, typical (OCXO/Rb).

Server Performance and Synchronization Accuracy:

GPS Receiver Accuracy: <25 nanoseconds RMS to UTC(USNO) when locked.*
<10 nsecs with calibration option.
NTP Timestamp Accuracy: <10 microseconds @ 50,000 requests/second.
NTP Client Synchronization Accuracy: Network factors can limit LAN synchronization accuracy to 1/2 to 2 milliseconds, typical.
*See GPS-UTC Timing Specifications for details.

Server Platform:

Operating System Kernel Version: 6.1.55
Slackware Linux Distribution: 15.0
Processor: 1.2 GHz.
RAM: 2GB
FLASH: 4GB

Supported IPv4 Protocols:

SNTP, NTP v4, SHA/MD5 authentication, broadcast/multicast mode and autokey.
SSH client and server with "secure copy" utility, SCP
SNMP v1, v2c, v3 with Enterprise MIB
RADIUS, TACACS+, LDAP
DHCP client
SYSLOG
HTTPS (TLS v1.3)
PTP/IEEE-1588 (Option)

Supported IPv6 Protocols:

SNTP, NTP v4, SHA/MD5 authentication, broadcast/multicast mode and autokey
SSH client and server with "secure copy" utility, SCP
SNMP v1, v2c, v3 with Enterprise MIB
RADIUS, TACACS+, LDAP
HTTPS (TLS v1.3)
Note: See ***Chapter 8 - IPv6 Information*** for more details.

PTP/IEEE-1588 Grandmaster (Option):

IEEE-1588-2008 (v2) with hardware timestamping.
Parameters: Default Profile. Multicast or Hybrid (mixed Unicast/Multicast). Two-Step Clock.
Delay Mechanism: E2E or P2P. Delay Interval: 32 seconds. Transport: UDP/IPv4.
Sync Interval: 1, 2, 4, 8, 16, 32, 64 or 128 packets / 1 second.
Announce Interval: 1 packet per 1, 2, 4, 8 or 16 seconds.
PTP Timestamp Resolution: 8 nanoseconds.
PTP Timestamp Accuracy to Reference Clock: 8 nanoseconds.
Note: See ***Chapter 4 - PTP/IEEE-1588*** for more information.

Network I/O:

Two rear-panel RJ-45 jacks..
100/1000Base-T Ethernet.
LEDs on each port indicate activity.
Green LED indicates activity.

System Status LEDs:

Sync LED: Amber LED pulses to indicate GPS acquisition and lock status.
Alarm LED: Red LED indicates a fault condition.

USB PORT:

Signal: USB 2.0 TYPE-A, local terminal access.
Parameters: 115200 baud, 8 data bits, no parity, 1 stop bit, Flow Control Xon/ Xoff
Connector: Rear-panel USB connector labeled with USB symbol.
To connect to a computer, an USB cable must be used. The USB cable provided with the shipment is a USB cable A male to MICRO B MALE.
Info on USB to serial converter: FTDI Driver: FT234XD

Size:

Chassis:	1.75”H x 17.0”W x 10.75”D, 19” rackmount
Weight:	< 8 lb. (3.6 kg.)
Antenna:	Standard: 3.25 H x 3.0 diameter.
	Anti-Jam: 5”H x 4” diameter.

Environmental:

Operating Temperature:	0° to +50° C	
Storage Temperature:	-40° to +85° C	
Antenna Operating Temperature:	-40° to +85° C	
Operating Humidity:	5% to 90%, RH, non-condensing	
Storage Humidity:	5% to 95%, RH, non-condensing	
Maximum Operating Altitude:	AC:	13,125 ft. / 4000 meters
	12/24 VDC:	13,125 ft. / 4000 meters
	48 VDC (<61 VDC Max.):	13,125 ft. / 4000 meters
	48 VDC (>60 VDC Max):	6,562 ft. / 2000 meters
	125 VDC:	6,562 ft. / 2000 meters

Power:

Basic Sonoma:	22 watts.
Sonoma with OCXO:	27-29 watts, depending on ambient temperature.
Sonoma with Rb:	36-38 watts, depending on ambient temperature.

90-264 VAC, 47-63 Hz, 1.0 A Max. @ 120 VAC, 0.5 A Max. @ 240 VAC
3-Pin IEC 320 on rear panel, 2 meter line cord is included.

Options:

See ***Chapter 10 - Options*** for more information.
Optional PTP/IEEE-1588 specifications are listed above.
Optional GPS Antenna Kit specifications are listed above.

DC Power Input:
12 VDC (10-20 VDC), 6.0A maximum.
24 VDC (19-36 VDC), 3.0A maximum.

48 VDC (37-76 VDC), 2.0A maximum.
125 VDC (70-160 VDC), 1.0A maximum.
3-position terminal block on rear panel: +DC IN, SAFETY GROUND, -DC IN
(Floating power input: Either "+" or "-" can be connected to earth ground.)
See ***Chapter 10 - Options, DC Power Input*** for more information.

Dual-Redundant Power Supplies:
Any combination of Universal AC and/or DC supplies.
See ***Chapter 10 - Options, Dual Redundant Power Supplies*** for more information.

1 PPS Output: Positive TTL pulse into 50Ω or RS-422 levels.
Width: User selectable to 20 us, 1 ms, 100 ms, 500 ms.
Accuracy: < 30 nanoseconds RMS to UTC(USNO) when locked.*
Stability: TDEV < 20 ns, $\tau < 10^5$ seconds.
Connector (TTL): Rear-panel BNC jack labeled "1PPS".
Connector (RS-422): Rear-panel DB-9M connector labeled "1PPS RS-422".
Pinout (RS-422): Pin 3 is +signal. Pin 6 is -signal. Pin 5 is GND.
*See GPS-UTC Timing Specifications for details.
Note: To change the pulse width refer to ***Chapter 10 - Options***.

AM Code Output: 1 V_{RMS} into 50Ω, 1 KHz carrier.
Signal: Amplitude-modulated (AM), 3:1 ratio.
Format: User selectable to IRIG-B (120/IEEE-1344, 122, 123), NASA-36, 2137.
Connector: Rear-panel BNC jack labeled "AMCODE".
Note: To change the time code format refer to ***Chapter 10 - Options***.

DC Code Output: Positive TTL pulse into 50Ω.
Signal: TTL, DC-shift.
Format: User selectable to IRIG-B (000/IEEE-1344, 002, 003), NASA-36, 2137.
Connector: Rear-panel BNC jack labeled "DCCODE".
Note: To change the time code format refer to ***Chapter 10 - Options***.

Programmable Pulse Output (PPO): Positive TTL pulse into 50Ω on BNC jack.
User-Selectable Output Type: On-time pulse rate.
Rate: User selectable to 1, 10, 100, 1K, 10K, 100K, 1M, 5M, 10M PPS, IPPM, 1PP2S.
Duty Cycle: 50% except 1PPS which mimics the 1PPS Output defined above.
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^2$ seconds, $\sigma_y(\tau) < 10^{-7}/\tau$ for $\tau > 10^2$ seconds.
Connector: Rear-panel BNC jack labeled "PPO".
Note: To change the output selection refer to ***Chapter 10 - Options***.

Direct Digital Synthesizer Output (DDS): Positive TTL pulse into 50Ω on BNC jack.
User-Selectable Output Type: Synthesized pulse rate.
Rate: User selectable 1 PPS to 10 MPPS in 1PPS steps..
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^2$ seconds, $\sigma_y(\tau) < 10^{-7}/\tau$ for $\tau > 10^2$ seconds.
Connector: Rear-panel BNC jack labeled "DDS".
Note: To change the output selection refer to ***Chapter 10 - Options***.

Alarm Output: MMBT2222A open collector, grounded emitter. High impedance in alarm state.
Voltage: 40 VDC, maximum.
Saturation Current: 100 mA, maximum.
Connector: Rear-panel BNC jack or terminal block labeled "ALARM".
Pinout (terminal block): Pins 1, 2, 3 are NC (not connected). Pin 4 is OC. Pin 5 is GND.

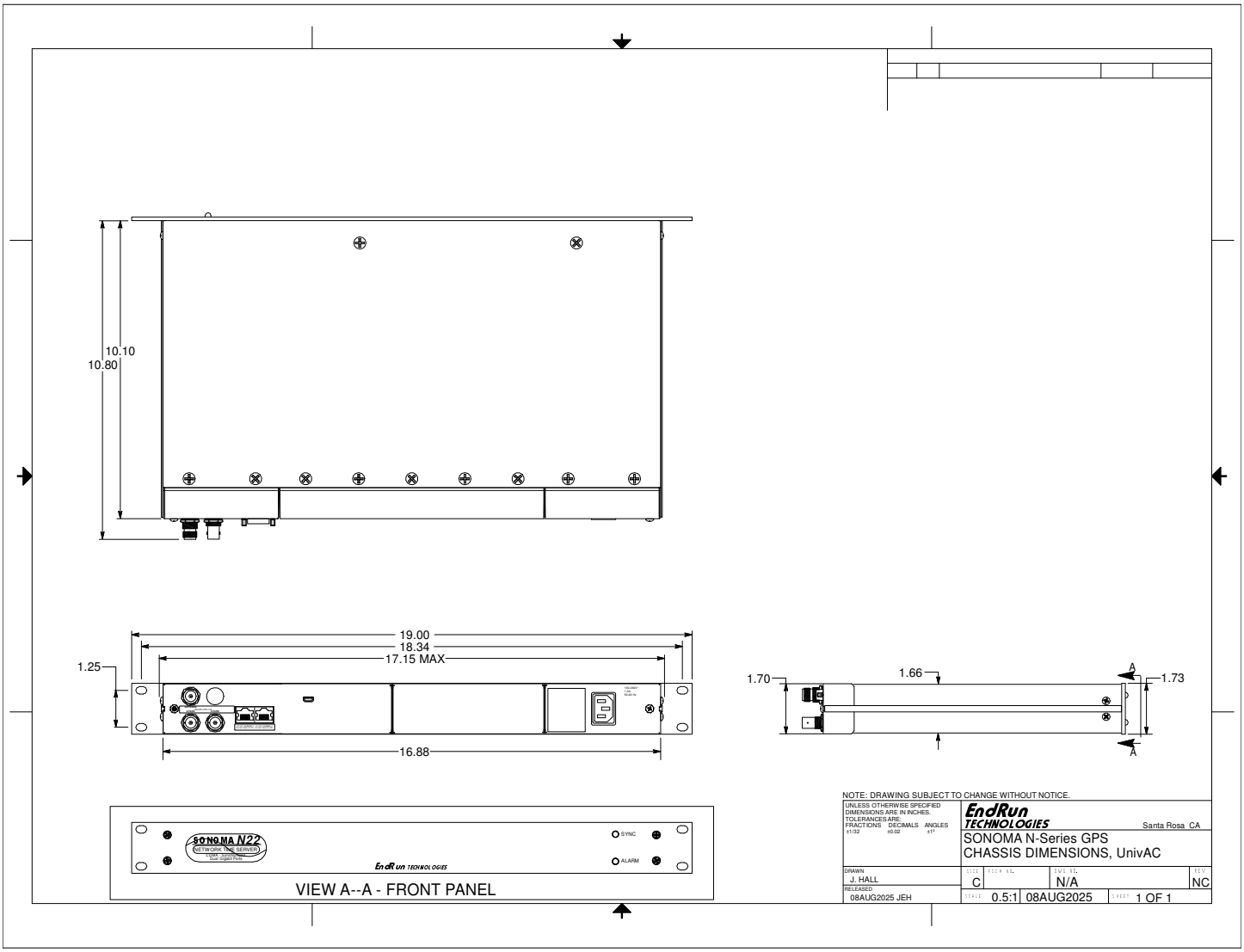
Serial Time Output: Output only port at RS-232 (±5V) or RS-422 levels.
Baud Rate: User Selectable to 4800, 9600, 19200 or 57600.
Parity: User Selectable to Odd, Even or None.
ASCII Formats: User-Selectable to Sysplex, EndRun, EndRunX, Truetime, NENA or NMEA.
Accuracy: The "on-time" characters starts transmitting within the first 20 microsecs of each second.
Connector (RS-232): Rear-panel DB-9M connector labeled "SERIAL TIME".
Pinout (RS-232): Pin 3 is Transmit Data. Pin 5 is GND.
Connector (RS-422): Rear-panel DB-9M connector labeled "SERIAL TIME (RS-422)".
Pinout (RS-422): Pin 3 is +signal. Pin 6 is -signal. Pin 5 is GND.
Note: See ***Chapter 10 - Options, Serial Time Output*** for more information.

Fixed Rate Output: Positive TTL pulse into 50Ω.
Rate: Preset at Factory and cannot be changed.
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^2$ seconds, $\sigma_y(\tau) < 10^{-7}/\tau$ for $\tau > 10^2$ seconds.
Connector: Rear-panel BNC jack labeled with appropriate rate such as "10 MPPS".

Compliance:

CE, FCC, Reach, RoHS 3, WEEE
UL/CSA 62368-1 NRTLC & CB Scheme.
UL for many, but not all, Sonoma configurations.
Contact EndRun for specific UL-approved part numbers.
All UL-approved Sonoma Time Servers have the UL label on the rear-panel.
The Sonoma time server is TAA compliant.

Data subject to change.
EndRun Technologies may make changes
to specifications and product descriptions
at any time, without notice.


10.10
10.80
19.00
18.34
17.15 MAX
1.25
16.88
1.70
1.66
1.73
A
A
SONOMA N22
SYNC
ALARM
EndRun TECHNOLOGIES
VIEW A--A - FRONT PANEL
NOTE: DRAWING SUBJECT TO CHANGE WITHOUT NOTICE.
UNLESS OTHERWISE SPECIFIED DIMENSIONS ARE IN INCHES.
TOLERANCES ARE:
FRACTIONS ±1/32 DECIMALS ±0.02 ANGLES ±1°
EndRun TECHNOLOGIES
Santa Rosa CA
SONOMA N-Series GPS
CHASSIS DIMENSIONS, UnivAC
DRAWN
J. HALL
RELEASED
08AUG2025 JEH
SIZE C
DWG NO. N/A
REV NC
SCALE 0.5:1
08AUG2025
SHEET 1 OF 1

CE

EndRun TECHNOLOGIES

DECLARATION OF CONFORMITY

(According to ISO/IEC 17050-1 and ISO/IEC 17050-2)

Manufacturer's Name: **EndRun Technologies, LLC**

Manufacturer's Address: **2270 Northpoint Parkway**
Santa Rosa, California 95407, U.S.A.
+1-707-573-8633

DECLARES, THAT THE PRODUCT

Product Name: **Network Time Server**

Model Number:
3050-XYYY-ZZZ (Sonoma D22 GPS Network Time Server)
3051-XYYY-ZZZ (Sonoma D24 GPS Network Time Server)
3052-XYYY-ZZZ (Sonoma N22 GPS Network Time Server)
3053-XYYY-ZZZ (Sonoma N24 GPS Network Time Server)
Where: X represents power supply configuration
YYY represents functional-option configuration
ZZZ represents customer-specific variations

CONFORMS TO THE FOLLOWING EUROPEAN DIRECTIVES

Low Voltage Directive: 2014 /35 / EU
Radio Equipment Directive: 2014 /53 / EU
EMC Directive: 2014 /30 / EU
RoHS Directive: 2015 / 863 / EU
WEEE Directive: 2012 / 19 / EU

Supplementary Information:

Safety : ***EN 62368-1/CSA C22.2 No. 62368-1:19***
EMC: ***EN 55032:2015+A11+A1, EN 55035 (2017)+A11***
EN 61000-3-2:2014, EN 61000-3-3-2013
ICES-0003 A, Issue 7
FCC Part 15 Subpart B

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.

Place: Santa Rosa CA USA Signature:

Date: 8/29/2025 Full Name: Bruce M. Penrod

Position: V.P. Product Development

eurofins | E&E

Certification Record

Listing#: E114891
Report #: 131619 c1 137485
Original Certification Date: June 14, 2024
Revised Certification Date: August 23, 2025

This Certification is issued to:
EndRun Technologies
2270 Northpoint Parkway
Santa Rosa, CA 95407
USA

Stating that the product(s):
Network Time Server,
Models Sonoma D12 (3027-XYYY-ZZZ), Sonoma N12 (3029-XYYY-ZZZ), Sonoma D24 (3051-XYYY-ZZZ), Sonoma N24 (3053-XYYY-ZZZ), Sonoma D22 (3050-XYYY-ZZZ),
Sonoma (N22 3052-XYYY-ZZZ), Meridian II 2U GPS TIMEBASE (3045-XYYY-ZZZ)

Product Rating(s):
- 100-240VAC, 1.0A, 50-60Hz
- Rubidium Oscillator and OCXO models: Single or Redundant external AC power feeds
- TCXO model: Single or Redundant AC power feeds

Achieved Certification to the following standard(s):
UL 62368-1/CSA C22.2 No. 62368-1:19, Third Edition: Safety of Audio/Video, Information and Communication Technology Equipment, Rev. October 22, 2021

Hon Keung IP
Certification Reviewer
Eurofins Electrical and Electronic Testing North America, LLC

All changes proposed in the previously identified product that affects the above information must be submitted to Eurofins for evaluation prior to implementation to assure continued NRTL Certification status. The covered product(s) shall be subject to follow-up inspections to ensure that the Certified product(s) are identical to the product sample evaluated by Eurofins E&E NA and that all responsibilities are being fulfilled as specified in the Applicants' Responsibility section of the Certification Report. The Applicant named above has been authorized Eurofins E&E NA to represent the product(s) listed in this record as "MET Certified" and to mark this/these product(s) according to the terms and conditions of the Eurofins E&E NA Applicant Contract, Listing Reports, and the applicable agreements. Only the product(s) bearing the MET Mark and under a follow-up service are considered to be included in this Certification program. This certification has been granted under a System 3 program as defined in ISO/IEC 17067.

SCC Accredited CB-P/6

Eurofins E&E North America, Inc. is accredited by OSHA and the Standards Council of Canada.

NRTL

SAFJ TEMP-130-0, NRTLC Certification Record
7-19-2021 Page 1 of 1

	Ref. Certif. No.
IEC IECEE	US-2614-MET M1A0 r1

IEC SYSTEM FOR MUTUAL RECOGNITION OF TEST CERTIFICATES FOR ELECTRICAL EQUIPMENT (IECEE) CB SCHEME

CB TEST CERTIFICATE

Product	Network Time Server
Name and address of the applicant	EndRun Technologies 2270 Northpoint Parkway, Santa Rosa, CA 95407 United States of America
Name and address of the manufacturer	EndRun Technologies 2270 Northpoint Parkway, Santa Rosa, CA 95407 United States of America
Name and address of the factory *Note: When more than one factory, please report on page 2*	EndRun Technologies 2270 Northpoint Parkway, Santa Rosa, CA 95407 United States of America ☐ Additional information on page 2
Ratings and principal characteristics	100-240VAC, 1.0A, 50-60Hz Rubidium Oscillator and OCXO models: Single or Redundant external AC power feeds TCXO model: Single or Redundant AC power feeds
Trademark / Brand (if any)	EndRun TECHNOLOGIES EndRun Technologies
Customer's Testing Facility (CTF) Stage used	
Model / Type Ref.	Sonoma D12: 3027-XYYY-ZZZ Sonoma N12: 3029-XYYY-ZZZ Sonoma D24: 3051-XYYY-ZZZ Sonoma N24: 3053-XYYY-ZZZ Sonoma D22: 3050-XYYY-ZZZ Sonoma N22: 3052-XYYY-ZZZ Meridian II 2U GPS TIMEBASE: 3045-XYYY-ZZZ Where: • X is 0 or 1 for single or dual AC power supply. • YYY represents functional-option configuration, not affecting safety. • ZZZ represents customer-specific variations, not affecting safety.
Additional information (if necessary may also be reported on page 2)	US-2614-MET EN 131619 M1A0 137485 Addition of models: o Sonoma D24 3051-XYYY-ZZZ GPS Network Time Server, Quad Ethernet Ports, Keypad and Display o Sonoma N24 3053-XYYY-ZZZ GPS Network Time Server, Quad Ethernet Ports o Sonoma D22 3050-XYYY-ZZZ GPS Network Time Server, Dual Ethernet Ports, Keypad and Display o Sonoma N22 3052-XYYY-ZZZ GPS Network Time Server, Dual Ethernet Ports ☐ Additional information on page 2
A sample of the product was tested and found to be in conformity with	IEC 62368-1:2018 National differences: AU, CA, CN, EU Group Differences, JP, NZ, SA, SG, US
As shown in the Test Report Ref. No. which forms part of this Certificate	US-2614-MET EN 131619 M1A0 137485

This CB Test Certificate is issued by the National Certification Body

Eurofins Electrical and Electronic Testing NA, LLC
914 W Patapsco Avenue
Baltimore, , MD 21230
United States of America

eurofins | E&E

This page intentionally left blank.

Special Modifications

Changes for Customer Requirements

From time to time EndRun Technologies will customize the standard Sonoma Time Server for special customer requirements. If your unit has been modified then this section will describe what those changes are.

This section is blank.

This page intentionally left blank.

EndRun TECHNOLOGIES
"Smarter Timing Solutions"
2270 Northpoint Parkway
Santa Rosa, CA 95407
TEL 1-877-749-3878
FAX 707-573-8619
www.endruntechnologies.com