EndRun TECHNOLOGIES
"Smarter Timing Solutions"

Sonoma N12 *Network Time Server*

CDMA-Synchronized

User Manual

USM3028-0000-000 Revision 5
November 2018

Sonoma N12 *CDMA*

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 troublefree 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. USM3028-0000-000 Revision 5
November 2018

About This Manual

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

Introduction – The Sonoma N12, 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, SNMP, HTTP, IPv6 and PTP/IEEE-1588.
Console Port – Description of the console commands for use over the network and serial 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 Technologies will repair or replace, at its option, products which prove to be defective.

For warranty service or repair, this product must be returned to EndRun Technologies. Buyer shall prepay shipping charges to send product to EndRun Technologies and EndRun Technologies 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.

Products not manufactured by EndRun Technologies but included as an integral part of a system (e.g. peripherals, options) are warranted for ninety days, or longer as provided by the original equipment manufacturer, from date of shipment.

Extended Warranty

EndRun products are very reliable and rarely need to be returned to the factory for service. After the initial warranty period it is most cost-effective for the customer to repair the unit on an “as needed basis”, rather than pay for an extended warranty or the annually recurring fees of a service contract..

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, call EndRun Technologies and ask for a customer service agent. It is important to contact us first as many problems may be resolved with a phone call. Please have the serial number of the unit and the nature of the problem available before you call. If it is determined that your equipment will require service, we will issue an RMA number. You will be asked for contact information, including your name, address, phone number and e-mail address.

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. Be sure the RMA number is clearly identified on 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. Call and ask for a customer service agent. It is important to contact us first as many problems may be resolved with a phone call. Please have the serial number of the unit and the nature of the problem available before you call. If it is determined that the equipment has failed and you want EndRun to perform the repairs, we will issue you an RMA number.

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 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 CDMA-Synchronized Sonoma Network Time Server and gives a brief overview of what it is and how it works.

What It Is

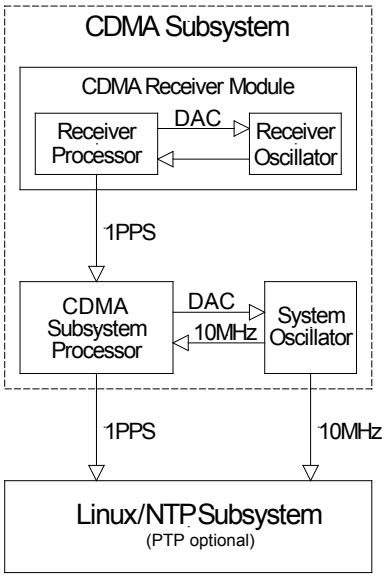
The Sonoma is a precision server of Coordinated Universal Time (UTC) that can be connected via an Ethernet port to any TCP/IP network. Available timing protocols include: Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), Time, Daytime, and the optional Precision Time Protocol (PTP/IEEE-1588).

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:

http://www.endruntechnologies.com/pdf/NTP-Intro.pdf

Time Synchronization Components

The Sonoma is composed of a Code Division Multiple Access (CDMA) Subsystem containing a CDMA Receiver and system oscillator. The CDMA Subsystem is integrated with a fanless, 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.



CDMA Timing - How It Works

The CDMA Subsystem in the Sonoma receives transmissions from base stations, also known as cell sites, that are operating in compliance with the TIA/EIA IS-95 standard for Code Division Multiple Access (CDMA) mobile telecommunications. This system requires a means of synchronizing the base stations throughout the network so that neighboring cells do not interfere with each other and so that calls can be efficiently transferred between the base stations, without interruption, as the mobile user traverses the cell coverage areas. This 'soft hand-off' feature means that the mobile telephone must be able to 'hitlessly' drop one base station and pick up the next one. To do this, the telephone must be able to calculate the relative difference in time between the codes that modulate the signals from each of the base stations, which again, requires that the base stations be synchronized.

The system designers chose the Global Positioning System (GPS), which is itself a CDMA-based system, as the means of maintaining synchronization, and they defined *system time* to be *GPS time*. Each base station throughout the system contains one or more high-performance GPS timing receivers with sophisticated algorithms that control either an extremely stable ovenized quartz crystal oscillator or a Rubidium vapor atomic frequency standard. Such elaborate means are needed to meet the very difficult operating specifications required by the TIA/EIA IS-95 standard. The base station time synchronization must remain within 10 microseconds of GPS time over periods as long as twenty-four hours during which GPS satellite signals might not be available (typically due to antenna/cable failure, damage or vandalism) and in an environment where large ambient temperature swings may occur. Equipment capable of meeting these requirements is at the current state-of-the-art.

The CDMA Subsystem in the Sonoma receives the same initialization signals transmitted by the base stations that are used by the mobile telephones to establish their synchronization to system time. The mobile telephones cannot communicate in the system until they have established synchronization with the received spread spectrum encoded waveform. Unlike the mobile telephones, once this synchronization has occurred, the CDMA Subsystem has all of the information that it needs to perform its function of delivering accurate UTC time to a network of computers. The mobile telephone must decode much more information, establish two-way communications with the base station, and be a paid subscriber to performs its function of placing and receiving calls.

All of this means that during normal operation, the quality of the timing information being transmitted from each of the base stations is virtually a repeat of that directly obtainable from the GPS. The big difference is that the received signal strengths from the base stations are a minimum of 30 dB larger than those from the GPS satellites, which is why you can usually talk on your cell phone indoors. Due to the nature of the IS-95 spread spectrum CDMA modulation scheme, this timing information may be extracted by a well-designed receiver with a precision of a few nanoseconds. The CDMA Subsystem in the Sonoma does just that, and for this reason, we call our technology 'indirect GPS'.

Where to Use It

First, the Sonoma must be deployed in a *cellular* or *PCS* IS-95 CDMA coverage area. *Cellular* is a commonly used term implying that the frequency band for the base station carrier transmissions is 824-895 MHz. This is in contrast to *PCS*, which implies operation in the 1850-1990 MHz frequency band. If available, the Sonoma uses the cellular frequency band because it provides much better propagation characteristics in regards to building penetration and maximum receivable range from the transmitter. In regions lacking cellular coverage, the unit can be set to receive the PCS signals. In general, if your CDMA telephone works where you plan to install the Sonoma, then your Sonoma will work properly there.

Because the Sonoma has been designed to operate in conjunction with existing public domain NTP/SNTP client software that has been created for use with similar time servers, it may be used in any computer 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.

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:

http://www.endruntechnologies.com/ntp-client.htm

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

http://www.endruntechnologies.com/ptp-slave.htm

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 like **`ping`**, **`telnet`** *and* **`ftp`** *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 N12 Time Server (CDMA) shipment typically contains:

- Sonoma N12 (part # 3028-0001-000 or #3028- variant)
- Sonoma N12 User Manual (part #USM3028-0000-000) on CD (part #5102-0001-000)
- IEC 320 AC Power Cord (part #0501-0003-000)
  (This part will not be present if using the DC power option.)
- DB9F-to-DB9F Null-Modem Serial I/O Cable (part #0501-0002-000)
- RJ-45 to RJ-45 CAT-5 patch cable, 2 meters (part #0501-0000-000)
- Magnetic-mount CDMA antenna/cable assembly (part #0502-0007-001)

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 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 downlead cable from the external antenna.
RS-232 Connector	This DB9M connector provides the RS-232 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*** for more information including the RS-232 pin assignments.
10/100/1000Base-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 speed (green) and activity (amber). The green LED will pulse once for a speed of 10M, twice for 100M, and three times for 1G. 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 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. Plug one end of the supplied AC power cord into an 85-270 VAC outlet.

3. Plug the other end into the AC input connector on the chassis rear panel of the Sonoma.

Place the antenna on a flat, preferably metallic surface while the unit is searching for the signal. Make sure that it is not blocked by large metallic objects closer than one meter.

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 has detected a CDMA signal, the Sync LED will begin to flash very slowly (about a .4 Hz rate).

4. As the unit locks onto the CDMA signal and begins to decode the timing data, the Sync LED will flash very rapidly (about a 6 Hz rate) until the data is fully decoded.

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

At this point, the CDMA Subsystem has fully synchronized, and you may proceed to permanently mounting the chassis and antenna in the desired location.

If this sequence has not occurred within twenty minutes, please read ***Appendix E - Installing the CDMA Antenna*** for details on antenna placement and on switching your Sonoma to search *PCS*, rather than *cellular*, frequencies.

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 locks on to a CDMA 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.

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 10/100/1000Base-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 RS-232 serial I/O 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 the RS-232 serial I/O port. The following section contains a brief description on how to do that.

Configuring Ethernet with the Serial Port

To configure your Ethernet interfaces with the serial 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 RS-232 serial I/O port.

Connect the RS-232 Serial I/O Port

To test serial communications with the Sonoma you will need either a VT100 compatible terminal or 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 DB9F-to-DB9F null modem adapter cable to the serial I/O jack on the Sonoma.

3. Connect the other end of the DB9F-to-DB9F null modem adapter cable to the terminal. If the serial I/O port on your terminal does not have a DB9M connector, you may need to use an adapter. Refer to ***Appendix H - Specifications*** for details on the signal wiring. *If you are using a computer for your terminal, remember which port you are using because you will need to know that in order to set up your terminal software.*

NOTE

You must use an RS-232 null-modem cable or adapter if you are connecting the Sonoma N12 to another computer. The cable included in the shipping kit is a null-modem cable.

If your computer does not have a serial port, you can use a USB port with a USB-RS232 converter similar to Gearmo GM-FTDI-8. First, connect the USB converter to your computer, then connect the converter to the null-modem cable. Finally, connect the null-modem cable to the Sonoma.

Test the Serial Port

You must configure your terminal to use the serial I/O port you used in ***Connect the RS-232 Serial I/O Port*** above. You must also configure your terminal as shown below:

- Baud Rate: 19200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Handshaking / Flow Control: OFF (both hardware and software)
- Terminal Emulation (if any): VT100 (or similar) or Linux

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

```
************************************************************
* 6010-0066-000 Linux Bootloader v1.00 Jan  1 2013 21:24:16 *
************************************************************


Default kernel: FACTORY
To override and boot the UPGRADE version of the kernel, type UPGRADE within 5 seconds
.....
 Booting with FACTORY Kernel


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

These lines are the Linux bootloader boot prompts. These prompts will timeout 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:

```
*******************************************************************************
*           Welcome to Sonoma_N12 CDMA console on:  Sonoma_N12.your.domain
*           Tue Feb 20  2013 21:47:03 UTC
*******************************************************************************

Sonoma_N12 login:
```

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 N12 CDMA and shows the software part number, version and build date. The out-of-the-box hostname is set to “Sonoma_N12”, and the domainname is set to “your.domain”.

```
Sonoma_N12 CDMA 6010-0065-000 v 1.00 Sat Jan 19 14:17:44 UTC 2013
Sonoma_N12 CDMA (root@Sonoma_N12:~)->
```

This last line is the standard Sonoma N12 CDMA 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 the Sonoma over the network using **`telnet`** or **`ssh`** and synchronize your network computers to UTC using NTP.

Using netconfig to Set Up Your IP

The script file **`netconfig`** will configure the TCP/IP network parameters for your Sonoma.

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

NOTE

If you want to use the HTTPS Interface, then be sure to configure the name server IP address during the **`netconfig`** process. The HTTPS Interface will not operate properly if this is configured incorrectly. Only one name server is required, but two gives some redundancy.

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

```
*******************************************************************************
************** Sonoma_N12 CDMA IPV4/IPV6 Network Configuration ***************
*******************************************************************************
*                                                                             *
*   This script will configure the TCP/IPV4/IPV6 network parameters for your  *
*   Sonoma_N12 CDMA.  We will first configure IPV4 and then IPV6.  Your       *
*   Sonoma_N12 CDMA has two ethernet interfaces, called eth0 and eth1.  For   *
*   each of IPV4 and IPV6, we will first configure eth0 and then eth1.        *
*                                                                             *
*   You can choose to keep the existing configuration of either interface and *
*   reconfigure the other.  You can also choose to "unconfigure" either of    *
*   the two interfaces if both are not needed in your application.            *
*                                                                             *
*   You will be able to reconfigure your system at any time by typing:        *
*                                                                             *
*   netconfig                                                                 *
*                                                                             *
*   The settings you make now will not take effect until you reboot your      *
*   Sonoma_N12 CDMA, so if you make a mistake, just re-run this script before *
*   rebooting.                                                                *
*                                                                             *
*   You will be prompted to enter your IPV4/IPV6 network parameters now.      *
*                                                                             *
*******************************************************************************
*******************************************************************************

Configure IPV4 for either eth0 or eth1?
  (Answer yes to continue on and reconfigure either eth0 or eth1 for IPV4.)
  (Answer no to "unconfigure" both eth0 and eth1 for IPV4.  Only the
   IPV4 loopback interface will be setup.) ([y]es, [n]o):
```

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

```
Sonoma N12 CDMA(root@Sonoma_N12:~)-> reboot
```

Verify Network Configuration

If you are using the RS-232 serial I/O 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 RS-232 serial I/O 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 **`telnet`** or **`ssh`** to verify successful DHCP configuration. Refer to the subsequent topics in this section ***Using Telnet*** and ***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**:

```
Sonoma N12 CDMA(root@host:~)-> ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0e:fe:01:00:1c
          inet addr:192.168.1.120  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9694 errors:0 dropped:970 overruns:0 frame:0
          TX packets:459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:829805 (810.3 KiB)  TX bytes:50242 (49.0 KiB)
          Interrupt:11

eth1      Link encap:Ethernet  HWaddr 00:0e:fe:01:00:1d
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10143 errors:0 dropped:970 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:881081 (860.4 KiB)  TX bytes:0 (0.0 B)
          Interrupt:15

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5808 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5808 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:728178 (711.1 KiB)  TX bytes:728178 (711.1 KiB)
```

Pay particular attention to the settings shown for **eth0** and **eth1**, in particular the **Mask**: setting, which should match that which is appropriate for your network. Now check the remaining configuration parameters using **route**:

```
Sonoma N12 CDMA(root@host:~)-> route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    1      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
localnet        *               255.255.255.0   U     0      0        0 eth0
192.168.5.0     *               255.255.255.0   U     0      0        0 eth1
```

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:

```
Sonoma N12 CDMA(root@host:~)-> 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 via **telnet** and **ftp**. The Sonoma provides both client and server operation using **telnet**. For security reasons, only client operation is supported using **ftp**. You may also monitor the Sonoma via the HTTPS interface (see ***Chapter 7 - HTTPS***).

Security conscious users will want to use **ssh**, the secure shell replacement for **telnet**, 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, OpenSSH*** for more information about the secure shell protocol.

Using Telnet

When establishing a **telnet** connection with your Sonoma, logging in directly as *root* is not permitted. This is a security measure that makes it slightly more difficult to gain access by simply trying passwords, since it is also necessary to know the name of a user. When you initiate a **telnet** session with the Sonoma, this banner will be displayed:

```
*******************************************************************************
*        Welcome to Sonoma_N12 CDMA telnet console on:  host.your.domain
*******************************************************************************

host login:
```

Here you may log in as “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. After correctly entering the password at this prompt,

```
Password:
```

the sign on message is shown. It identifies the host system as Sonoma CDMA and shows the software part number, version and build date:

```
Sonoma_N12 CDMA 6010-0065-000 v 1.00 Sat Jan 19 14:17:44 UTC 2013
Sonoma_N12 CDMA (root@host:~)->
```

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

To gain *root* access, you must now issue the “super user” command at the prompt:

```
Sonoma_N12 CDMA(root@host:~)-> su root
```

You will then be prompted for the password, which is "endrun_1", and be granted *root* access to the system. To leave "super user" mode, issue the command **`exit`**. Issuing **`exit`** again will close the **`telnet`** session.

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_N12 CDMA SSH console on:  host.your.domain
******************************************************************************

root@192.168.1.120's 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_N12 CDMA 6010-0065-000 v 1.00 Sat Jan 19 14:17:44 UTC 2013
Sonoma_N12 CDMA (root@host:~)->
```

This last line is the standard Sonoma N12 CDMA 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.

Using HTTPS

You may monitor the status of the Sonoma via the HTTPS interface. For security reasons, you may not change any settings via the HTTPS interface. See ***Chapter 7 - HTTPS*** for more information.

IMPORTANT

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

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

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

This page intentionally left blank.

Chapter *Three*

Network Time Protocol (NTP)

This chapter describes how to configure the Sonoma as an 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 the 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:

http://www.ntp.org

A simple introduction to NTP is here:

http://www.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, the Sonoma is configured to respond to NTP requests from clients that may or may not be using MD5 authentication. If the clients are using MD5 authentication, they must be configured properly with the same MD5 authentication keys as the Sonoma. If you need to modify the factory default Sonoma MD5 keys (recommended) or set up broadcast/multicast operation, then you will need to reconfigure the NTP subsystem. You may perform the configuration from either a **`telnet`** or **`ssh`** session or the local RS-232 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.

Sonoma_N12 CDMA(root@Sonoma_N12:~)-> ntpconfig

```
*******************************************************************************
**********************Network Time Protocol Configuration**********************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure the ntp.conf and ntp.keys files   *
*   that control Sonoma_N12 CDMA NTP daemon operation.                        *
*                                                                             *
*   You will be able to create new MD5 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_N12 CDMA.  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 "untrusted".

Clients that use any of the "trusted" keys in their NTP polling packets will
receive authenticated replies from the Sonoma_N12 CDMA.  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_N12 CDMA
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_N12 CDMA
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_N12 CDMA 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 the 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 CDMA 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 CDMA 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 insructions 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. For Stratum 2 operation you may not want to see this alarm. You can mask it (prevent it from showing) by using the console port (serial/network) command **`setsigfltmask`**.

Setting Up NTP Clients on Unix-like Platforms

To configure your Unix-like computer to use your Sonoma Time Server, 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 priviledges 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 the 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. The Sonoma is factory configured to authenticate its replies to NTP MD5 clients using its default set of keys.

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 the 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 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 the Sonoma server. Use the NTP utility **`ntpq`** to check that **`ntpd`** is able to communicate with the 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 the 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 Serial 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. You can **`telnet`** into your Sonoma and start an **`ftp`** session with your client computer to send the Sonoma's */etc/ntp.keys* file to your client computer, use the secure copy utility **`scp`**, or 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 by **`ftp`**, 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 Serial 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 the 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 **ftp** or **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 the 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 authentication, your Sonoma must have been configured to operate with authenti-

cation 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 Authenticated NTP Client Setup*** on your client computer, if you plan to use MD5 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 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 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 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 Authenticated NTP Client Setup***:

```
server 192.168.1.120 key 1
```

Test Broadcast/Multicast

Restart **`ntpd`** to have it begin using the Sonoma as a broadcast or multicast server. Use the NTP utility **`ntpq`** to check that **`ntpd`** is able to communicate with the 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 **`ftp`** or **`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 Time Server, you must have successfully completed the procedures in ***Configuring the NTP Server*** above. Client installation must be performed by a user with administrative priviledges.

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 the Sonoma with NTP clients on Windows 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. The Sonoma is factory configured to authenticate its replies to NTP MD5 clients using its default set of keys.

Broadcast/Multicast: This method simplifies configuration of the clients on large networks since specific server addresses need not be configured in each client's *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.

Windows: Basic NTP Client Setup

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

http://www.endruntechnologies.com/ntp-client.htm

Windows: w32time

Windows uses a time service called **`w32time`** which is automatically enabled by default during Windows installation. **`w32time.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.

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.

Windows: ntpd

For more precise timekeeping you should use **`ntpd`**. An easy way to install **`ntpd`** is by using a third-party NTP compilation. A list for Windows is at this link:

http://support.ntp.org/bin/view/Main/ExternalTimeRelatedLinks

Configure NTP

Directory path names are not given in the instructions below because there are multiple ways to install **ntpd** and multiple versions of Windows.

After installing **ntpd**, you must edit the *ntp.conf* file by adding a line similar to this:

```
server 192.168.1.120
```

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

Restart **ntpd.exe** to have it begin using the Sonoma server. By default, the NTP installation program installs **ntpd.exe** as a service called Network Time Protocol, and starts it. You must use the Services utility in Control Panel to stop the Network Time Protocol service and then restart it.

Use the NTP utility **ntpq.exe** to check that **ntpd.exe** is able to communicate with the Sonoma. From a console window, after issuing the command

```
ntpq
```

you will see the **ntpq.exe** 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.

Windows: MD5 Authenticated NTP Client Setup

MD5 authenticated setup is relatively simple, if:

- You have been able to successfully communicate with the 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 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 ***Windows: Basic NTP Client Setup*** on your client computer.

Create the ntp.keys File

You must create a file named *ntp.keys* in the */program files/ntp/etc* directory (for example). It must be a copy of the one residing in the */etc* directory of your Sonoma. You can **`telnet`** into your Sonoma and start an **`ftp`** session with your client computer to send the Sonoma */etc/ntp.keys* file to your client computer, or use the secure copy utility **`scp`**, or use a text editor to create the equivalent file. Although you should first test your setup using the factory default */etc/ntp.keys* file in your Sonoma server, you should create your own keys after you understand the process and have your clients operating correctly with the default file.

IMPORTANT

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

After transferring the file, make sure that its security properties are set such that it is readable only by the "administrator".

Configure NTP

Add these lines to the end of the *ntp.conf* file, but substitute your particular directory path for the one shown (*program files\ntp\etc*):

```
keys \program files\ntp\etc\ntp.keys
trustedkey 1 2
```

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

```
server 192.168.1.120 key 1
```

Restart **`ntpd.exe`** to have it begin using the Sonoma server with MD5 authentication. By default, the NTP installation program installs **`ntpd.exe`** as a service called Network Time Protocol, and starts it. You must use the Services utility in Control Panel to stop the Network Time Protocol service and then restart it.

Use the NTP utility **`ntpq.exe`** to check that **`ntpd.exe`** is able to communicate with the Sonoma. From a console window, after issuing the command

```
ntpq
```

you will see the **ntpq.exe** 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 *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 **ftp** or **scp**, this shouldn't be a problem.) It is also possible to have a typing error in the *ntp.conf* file that causes the needed key to not be included in the "trustedkey" list.

Windows: Broadcast/Multicast NTP Client Setup

Broadcast/multicast client setup is relatively simple, if:

- You have been able to successfully communicate with the 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 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 ***Windows: MD5 Authenticated NTP Client Setup*** on your client computer, if you plan to use MD5 authentication.

Configure NTP Client for Broadcast

You must edit the *ntp.conf* file. 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 authentication, you would add these lines:

```
disable auth
broadcastclient
```

You may remove the line added previously in ***Windows: Basic NTP Client Setup***:

```
server 192.168.1.120
```

or the authenticated version added in ***Windows: MD5 Authenticated NTP Client Setup***:

```
server 192.168.1.120 key 1
```

Configure NTP Client for Multicast

You must edit the *ntp.conf* file. 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:

```
multicastclient 224.0.1.1
```

or for IPv6:

```
multicastclient ff05::101
```

If you are not using MD5 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 ***Windows: Basic NTP Client Setup***:

```
server 192.168.1.120
```

or the authenticated version added in ***Windows: MD5 Authenticated NTP Client Setup***:

```
server 192.168.1.120 key 1
```

Test Broadcast/Multicast

Restart **`ntpd.exe`** to have it begin using the Sonoma as a broadcast or multicast server. By default, the NTP installation program installs **`ntpd.exe`** as a service called Network Time Protocol, and starts it. You must use the Services utility in Control Panel to stop the Network Time Protocol service and then restart it.

Use the NTP utility **`ntpq.exe`** to check that **`ntpd.exe`** is able to communicate with the Sonoma. After issuing the command

```
ntpq
```

you will see the **ntpq.exe** 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 *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 **ftp** or **scp**, this shouldn't be a problem.) It is also possible to have a typing error in the *ntp.conf* file that causes the needed key to not be included in the "trustedkey" list.

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 **`get_sw_opts`** command:

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

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 cases below, PTP is installed.

Command: **`get_sw_opts`**
Sonoma reply: **`00000000000000000000000000000001`** (PTP installed on port 0 only.)
or
Sonoma reply: **`00000000000000000000000000000011`** (PTP installed on ports 0 and 1.)

About PTP

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

http://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:

http://www.nist.gov/el/isd/ieee/ieee1588.cfm

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 either a **telnet** or **ssh** session, or the local RS-232 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 Serial 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) 16

---PTP Priority1 Configuration

Set the PTP Priority1 value (0-255) 127

---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) P2P

---PTP Domain Configuration

Set the PTP Domain value (0-255) 0

---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 Serial 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.

FT is 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.

NOTE

If using a single Grandmaster, keep the default setting of 128 for Priority 1 and Priority 2. If using two redundant Grandmasters, then you can configure the preferred clock by setting Priority 1 to 127 and Priority 2 to 128.

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 CDMA Subsystem TFOM level is at 6 (see ***Appendix A - TFOM***). The Clock Class is HOLDOVER when the CDMA Subsystem TFOM level is greater than 6 and less than 9. The Clock Class is UNLOCKED when the CDMA 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 GPS designator is used in this CDMA-synchronized time server because CDMA is sometimes called “indirect GPS”. For an explanation of “indirect GPS” see ***Chapter 1 - Introduction, CDMA Timing - How It Works***.

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 the following:

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.

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 Secure Sockets Layer (SSL) 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.

IMPORTANT

SSH, Telnet, SNMP and HTTP are all enabled with default passwords. To ensure security, change the passwords or disable the protocols. To change the passwords for SSH, Telnet 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, Telnet and SNMP. To restrict access via these protocols to specific hosts, see ***Restrict Access - Telnet, 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 RS-232 console or via SSH.

- The secure copy utility, **scp**, eliminates the need to use the insecure FTP protocol for transferring program updates to the Sonoma.

- HTTP access for system monitoring only, is allowed only via SSL, so passwords and session data are encrypted on the wire. Access via HTTPS may be restricted or completely disabled. See ***Restrict Access - HTTPS*** and ***Disable SNMP, SSH and 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 - Telnet, 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 **in.telnetd, 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 - Telnet, SSH and SNMP*** below.

- Insecure protocols like Time, Daytime and Telnet may be completely disabled by configuration of the **inetd** super-server daemon using the interactive script **inetdconfig**. See ***Disable Telnet, Time and Daytime*** below.

Restrict Access

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

Restrict Access - Telnet, SSH and SNMP

By default, the Sonoma is configured to allow access by all users via Telnet, 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 **in.telnetd, 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:

```
in.telnetd:  ALL
sshd:  ALL
snmpd:  ALL
```

This tells **tcpd** to deny access to **in.telnetd, 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 **in.telnetd, sshd** and **snmpd**. These appear in the */etc/hosts.allow* as lines like this:

```
in.telnetd:  192.168.1.2, 192.168.1.3
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 />
  AllowOverride none
  Require all denied
</Directory>
```

To restrict access to a specific host, you would begin by modifying this directive as follows:

```
<Directory />
  AllowOverride none
  Require all granted
</Directory>
```

Next, the default file contains these lines that must be edited:

```
# Controls who can get stuff from this server.
#
Require all granted
```

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:

```
# Controls who can get stuff from this server.
#
   Order Deny,Allow
   Deny from all
   Allow from xxx.xxx.xxx.xxx
```

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:

http://www.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
```

Disable Protocols

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

Disable Telnet, Time and Daytime

To disable Telnet, Time and Daytime use the **`inetdconfig`** command to start an interactive script that will ask you which protocols to disable. Then it will modify the */etc/inetd.conf* file, which is read by the super-server daemon, **`inetd`**. Requests from remote hosts for protocols not configured in */etc/inetd.conf* will be refused. Currently, three servers are configurable via **`inetdconfig`**: Time and Daytime (whose protocol servers are contained within the **`inetd`** daemon itself), and **`in.telnetd`**. Any one or all of these may be enabled or disabled for start-up.

Disable SNMP, SSH and HTTPS

To disable SNMP, SSH or HTTPS, 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
chmod -x /etc/rc.d/rc.httpd
```

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
```

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 and HTTPS

If you have disabled SNMP, SSH or HTTPS, 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
rm /boot/etc/rc.d/rc.httpd
```

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

Is the Protocol Disabled?

Telnet, TIME and DAYTIME: To determine if one of these protocols is disabled, use the **`inetdconfig`** command.

SNMP, SSH and HTTPS: To determine if one of these protocols is disabled, 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:

http://www.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 - Telnet, 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_keys2* 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 unfamilar 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 2.4.10 distribution from:

http://httpd.apache.org

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

http://www.modssl.org

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

HTTP and SSL 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*** above.)

Configure Certificate and Key

For SSL 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 SSL 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 Authenticated NTP Client Setup*** or ***Chapter 3 - NTP, Windows: MD5 Authenticated NTP Client Setup***. You can also restrict NTP query access. See ***Restrict Query Access - NTP*** in this chapter.

Network Security Vulnerabilities

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

http://www.endruntechnologies.com/fsb.htm

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

http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

Chapter *Six*

Simple Network Management Protocol (SNMP)

Your Sonoma includes the NET-SNMP version 5.5.1 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:

http://www.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:

SONOMA-MIB

Which is located on your Sonoma in this ASCII file:

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

In addition to a complete set of NTP and CDMA 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 destination 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 configure 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 *nt-*

puser 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.

Disable or Restrict Access

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

This page intentionally left blank.

Chapter *Seven*

Hyper Text Transport Protocol Secure (HTTPS)

This chapter briefly describes the HTTPS interface that resides on the Sonoma CDMA 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 Secure Socket Layer (SSL). Security-conscious customers may disable the HTTPS interface (see the end of this chapter for instructions).

The HTTPS implementation in the Sonoma uses HTTP over SSL. SSL 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/2.4.10 distribution from:

http://httpd.apache.org

See ***Chapter 5 - Security, HTTPS*** for information on changing the default HTTPS configuration and SSL 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 serial port.

NOTE

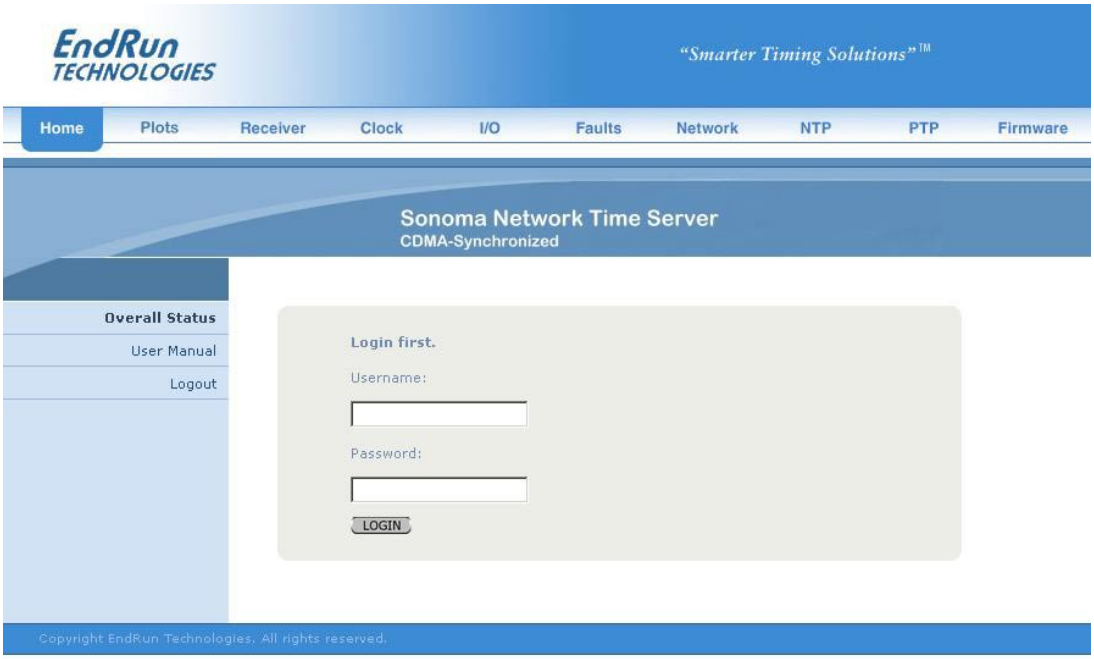
For proper operation, your web browser must be configured to allow pop-up windows.

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: http://192.168.1.1
IPv6: http://[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 SSL. The browser should change from http: to https:, indicating that the page is protected by SSL. To maximize security you should replace the SSL Certificate. See ***Chapter 5 - Security, HTTPS*** for details.

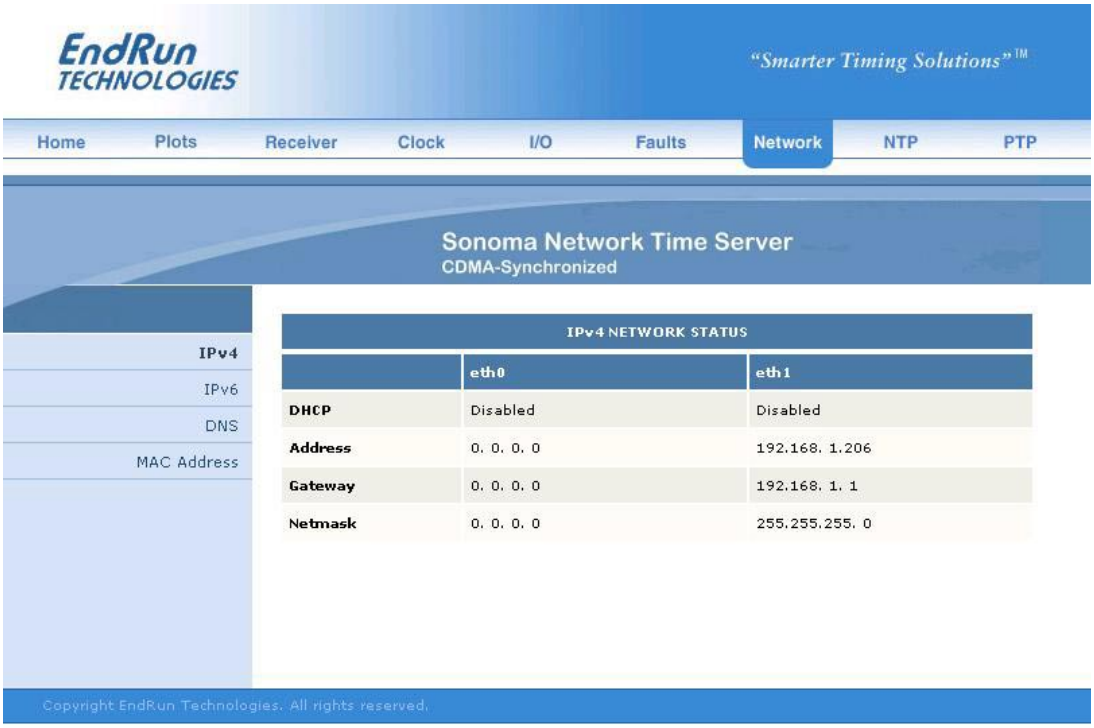
Below is a picture of the login page:



Navigation

The main menu tabs across the top of each webpage allow you to navigate through the status information 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, Plots, Receiver, 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 N12
Serial Number	Serial number of the Sonoma N12. This field will not be shown for units shipped before August 2015.
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 CDMA Subsystem/Receiver as follows: WRM: Warmup period for units with oscillator upgrades. ACQ: Acquiring. Searching for a signal. LKG: Locking to the CDMA 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

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

Home: User Manual

This link provides access to the Sonoma User Manual that is resident in the FLASH memory. The most recent version of the User Manual is on the EndRun website at:

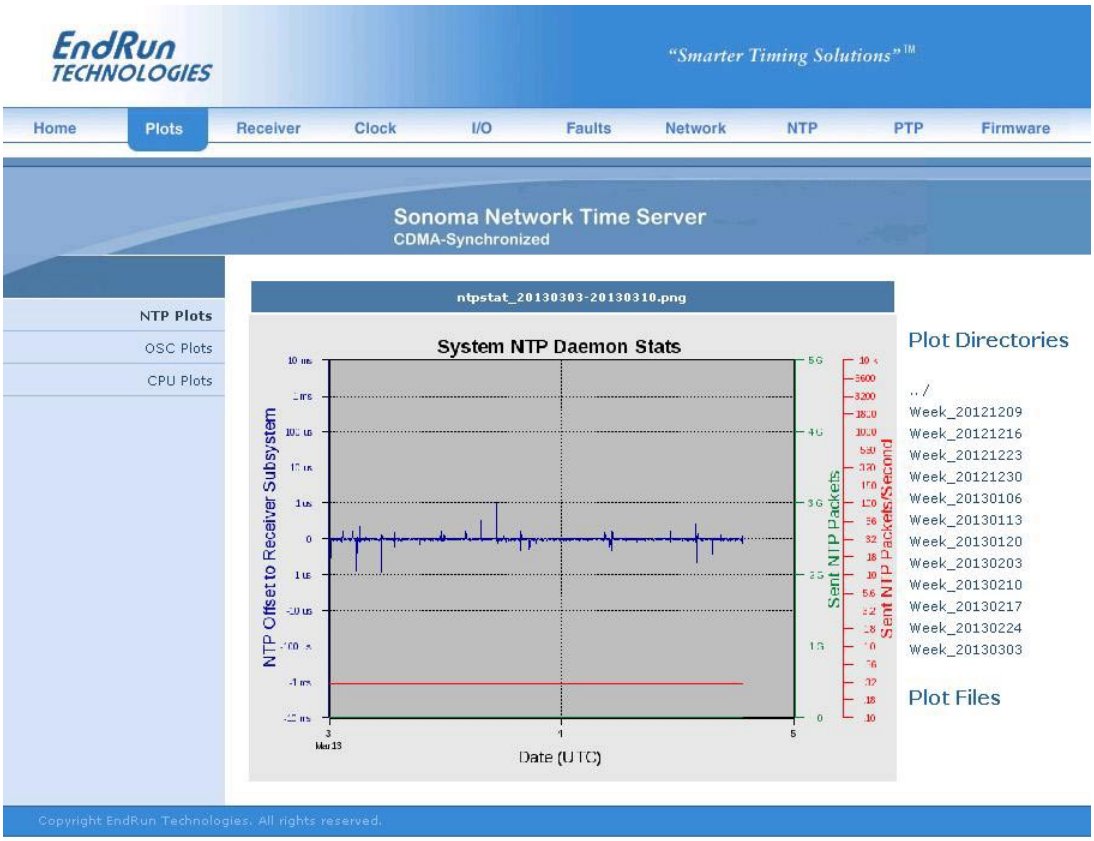
http://www.endruntechnologies.com/pdf/USM3028-0000-000.pdf

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 three types of data plots available for viewing: CPU, NTP and Oscillator. 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 three data types (CPU, NTP, Oscillator).

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 CDMA Subsystem/Receiver. Data fields are:

CDMA Receiver Status

Subsystem State — This shows whether the current state of the CDMA Subsystem:

WRM:	Warmup period for units with oscillator upgrades.
ACQ:	Searching for a signal.
LKG:	Locking to the CDMA Signal.
LKD:	Locked. Fully synchronized to signal.

TFOM — The current TFOM value (see ***Appendix A - TFOM***).

AGC — Automatic Gain Control DAC. Typical value is 150 to 220 in good signal conditions.

SNR — Signal-to-Noise Ratio. Typical value is > 2.5.

FER — Frame Error Rate when decoding CDMA sync channel frames.

PNO — Pseudo-Noise Offset of the basestation.

Channel — This is the CDMA frequency channel being used.

Receiver DAC — This is the CDMA Receiver 16-bit DAC value.

Receiver State — This shows the current state of the CDMA Receiver:

WRM:	Warmup period for units with oscillator upgrades.
ACQ:	Searching for a signal.
DET:	A signal is detected.
LKG:	Locking to the Pseudonoise (PN) Code.
TRK:	Locking to the carrier.
LKD:	Locked. Fully synchronized to signal.

Configuration

Clock Calibration — Clock Calibration is used to advance or retard the clock in order to correct for propagation delay due to distance from the basestation. Calibration range is ±500,000 nanoseconds.

Channel Set — This shows the current channelset being used by the CDMA Receiver. It could be North America Cellular, Korea Cellular, North American PCS, India Cellular and Japan Cellular.

Receiver: Oscillator Page

This page shows CDMA Subsystem 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 the last measured time offset of the CDMA Subsystem to CDMA while locked, in seconds.
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 CDMA Receiver.
Oscillator Ageing Rate	This field shows the regression-computed system oscillator ageing rate per day (several-hour delay before the first measurements are displayed).
Control Loop TAU	This field shows the oscillator control loop averaging time constant, in seconds. It's value is automatically adjusted to maintain optimum system clock offset and stability.
Coast Duration	This shows the number of seconds the CDMA Subsystem has been in coast mode, while the Sonoma is unlocked to CDMA. Coast mode is another term for holdover mode.
Estimated Time Error	This is the estimated time error of the CDMA Subsystem when in coast mode, in seconds.
Internal Chassis Temperature	Internal chassis temperature in °C. Available with OCXO or Rubidium oscillators.

Clock Page

This page shows the configuration of the clock or timekeeping parameters. Fields are:

Clock Configuration

Time Mode	This field shows the current time mode setting. Possible settings are UTC, GPS Local-Manual and Local-Auto. 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. Local-Manual means the user enters the time zone offset and the DST. Local-Auto means that the time zone offset is decoded from the CDMA signal.

Time Zone Offset — This field shows the offset from UTC and is only valid when the Time Mode is Local-Manual. A positive time zone offset implies a longitude east of the Greenwich meridian. To change the time zone use the **`systimemodeconfig`** command. In Local-Auto mode the time zone is decoded from the CDMA signal.

Daylight Saving Time — This field will show whether DST control is enabled or not.
DST fields are only used when the Time Mode is Local-Manual.
If the Time Mode is Local-Auto then this field will show "automatic".

DST Start, DST End — These fields will only display if the Daylight Saving Time field above shows enabled. If DST is 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. To change the DST settings use the **`systimemodeconfig`** command.

Current & Future Leap Seconds — These fields show the leap second settings, which are user-entered. Use the **`cdmaleapmodeconfig`** command to change the settings.
See ***Appendix F - Leap Seconds*** for more information.

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 system fault conditions of the Sonoma - the Linux Subsystem and the CDMA Subsystem. For details on each fault see ***Appendix G - System Faults***.

Faults: Receiver Faults Page

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

Faults: Fault Mask Page

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 CDMA 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.

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. Fields are:

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. Thie field will show whether DHCP is enabled or disabled.
Address, Gateway, Netmask	These fields show the settings for the IP address, gateway and netmaks. To change these esttings use the **`netconfig`** command via the console port.

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. Fields are:

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 CDMA. 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 CDMA Subsystem clock. Positive implies that the NTP system clock is ahead of the CDMA Subsystem clock.	

Leap Indicator — This field shows whether a leap second is pending.
Leap seconds about every 1½ to 2 years. Possible indicator values are:

00:	Normal, locked operation.
01:	Leap second insertion will occur after 23:59:59 UTC.
10:	Leap second deletion will occur after 23:59:58 UTC.
11:	Fault. Unsynchronized state.

I/O Statistics

Time Since Reset, Packets Sent/Received, 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

Linux RFS PN, Linux RFS Version — These fields show the Linux root file system part number, version & date.

Linux Kernel PN, Linux Kernel Version — These fields show the Linux kernel part number, version & date.

CDMA Subsystem Firmware — This field shows the CDMA Subsystem firmware version.

CDMA Subsystem FPGA — This field shows the CDMA Subsystem Field Programmable Gate Array (FPGA) version.

CDMA Receiver Firmware — This field shows the CDMA Receiver firmware version.

CDMA Receiver FPGA — This field shows the CDMA Receiver FPGA version.

Firmware: Linux RFS Upgrade

This page is used for upgrading the Linux RFS firmware. You must be logged in as "root" in order to have access to this page. 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: Linux Kernel Upgrade

This page is used for upgrading the Linux kernel firmware. You must be logged in as "root" in order to have access to this page. 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: CDMA Subsystem Upgrade Page

This page is used for upgrading the firmware for the CDMA Subsystem. 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: CDMA Receiver Upgrade Page

This page is used for upgrading the firmware for the CDMA Receiver. 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 CDMA 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, Disable SNMP, SSH and HTTPS***. To restrict access to specific hosts see ***Chapter 5 - Security, Restrict Access - HTTPS***.

This page intentionally left blank.

Chapter *Eight*

IPv6

The Sonoma Time Servers support IPv6 out-of-the-box with a modern version 3.2.2 Linux kernel. 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 domain-name 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: **telnet** (client and server), **ftp** and **dhcpcd**. Due to their intrinsic insecurity, **telnet** and **ftp** are rapidly being deprecated, and probably have little business running over an IPv6 network. The address autoconfiguration capabilities of IPv6 along with the Neighbor Discovery Protocol (NDP) make the DHCP protocol less important in IPv6 networks. The optional PTP/IEEE-1588 protocol is also not available on IPv6.

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 RS-232 serial port. The Sonoma supports several application-specific commands for configuration and for monitoring the performance and status of the Linux and CDMA 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 N12. Two are 10/100/1000Base-T Ethernet ports and one is an RS-232 serial port. Network cables and a serial cable are provided with each Sonoma shipment. The serial cable is wired as a null-modem adapter and can be used to connect the Sonoma to the serial port on your computer. Detailed specifications on the ports, including the RS-232 pinout, 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::

http://www.tldp.org

Available User Commands

COMMAND	FUNCTION
accessconfig	Interactive script that guides you in configuring **`telnet, 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.
caldelay	Prints the calibration delay. See the **`setcaldelay`** command.
cdmachannelset	Prints the current CDMA channelset being used. It can be one of North American Cellular, South Korean Cellular, North American PCS, Indian Cellular or Japanese Cellular. See the **`setcdmachannelset`** command.
cdmaleapconfig	Guides the user in configuring the way in which UTC leap seconds are handled: either automatically via CDMA basestation transmissions or by user-entered current and future leap second parameters. See the **`cdmaleapmode`** command.
cdmaleapmode	Prints the current CDMA leap second mode of operation, either automatic or user-entered. If user-entered, prints the current and future leap second values. See the **`cdmaleapconfig`** command.
cdmastat	Prints the CDMA Subsystem status information to the console.
cdmaversion	Prints the CDMA Subsystem firmware and FPGA version information.
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.
get_sw_opts	Returns the current software options enabled in your Sonoma. See ***Chapter 10 - Options, Software Options*** for more information.
help help command	Prints help list for all Sonoma-specific (not Linux) commands. Prints command-specific help. For example: **`help cdmastat`**.
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.
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 CDMA 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.
rcvrversion	Prints the CDMA Receiver firmware and FPGA version information.
serialnumber	Prints the serial number of the Sonoma. The serial number is not available using this command for units shipped before August 2015.
setcaldelay	An interactive utility that allows you to change the clock calibration delay. See the **`caldelay`** command.
setcdmachannelset	Command that allows the user to select the channelset for the CDMA Subsystem to receive. This command is not functional in units comfigured for Japanese Cellular operation. See the **`cdmachannelset`** 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 CDMA Subsystem reset.
syskernel	Prints the currently booted Linux kernel, either 0 or 1, where 0 is the factory-installed kernel and 1 is the upgraded kernel.
sysosctype	Prints the installed system oscillator type, which is one of TCXO, OCXO or Rubidium.

sysrootfs	Prints the currently loaded Linux root file system image, either 0 or 1, where 0 is the factory installed root file system, and 1 is the upgraded root file system.
sysstat	Prints detailed NTP status information. Included is the offset of the NTP-steered system clock to the CDMA 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 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.
updatekernelflag	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 kernel.
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.
upgradekernel	Command that performs the Linux kernel upgrade process.
upgradercvr	Command that performs the CDMA Receiver upgrade process.
upgraderootfs	Command that performs the Linux root file system upgrade process.
upgradesubsys	Command that performs the CDMA Subsystem firmware update 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 **telnet**, **ssh** and **snmp** to the Sonoma. By default, the unit is configured to allow access by all users. If you need to limit **telnet**, **ssh** or **snmp** access, e.g. for security reasons, you must run this script as root from either the RS-232 serial I/O port or from a **telnet** or **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.

caldelay

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

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

cdmachannelset

This command displays the CDMA channelset currently being used by the CDMA Subsystem. It can be one of: North American Cellular, South Korean Cellular, North American PCS, Indian Cellular or for certain units, Japanese Cellular.

Command: **cdmachannelset**
Sonoma reply: **Channelset is North American PCS**

cdmaleapconfig

Leap seconds affect NTP, UTC and Local Time (not GPS Time). Leap second insertions occur about every 1½ to 3 years. This command starts an interactive shell script that will guide you (as root user) in configuring the leap seconds.

You will need to execute this command when a leap second is pending. The interactive script is very detailed in explaining how these values are obtained and used. There is also more information in ***Appendix F - Leap Seconds***.

Command: **cdmaleapconfig**
Sonoma reply: Interactive shell script is started.

cdmaleapmode

This command displays the current and future leap second settings. The leap second mode is always

USER, meaning that the leap second information is user-entered. For more information on leap seconds see ***Appendix F - Leap Seconds***.

Command: **cdmaleapmode**
Sonoma reply: **CDMA Leap Second Mode is USER: Current LS = 18, Future LS = 18**

cdmastat

This command allows the user to query the status of the CDMA Subsystem. During normal operation, the NTP daemon polls the CDMA 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 CHANNEL PNO AGC VCDAC OSCDAC
SN.R F.ERR FLTR FLTS
```

Where:

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

TFOM = ? A value between 6 and 9 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 NTP polling request received by the CDMA Subsystem from the NTP reference clock driver.

DOY is the day-of-year of the UTC timestamp of most recent NTP polling request received by the CDMA subsytem from the NTP reference clock driver.

HH:MM:SS is the hour, minute, second UTC timestamp of the most recent NTP polling request received by the CDMA Subsystem from the NTP daemon reference clock driver.

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 (Code Locking), 2 (Locked), 9 (Warming Up).

C is the CDMA frequency channel being used, for example NAP_01_A which is North American PCS, Provider A, Channel 1.

PNO is the base station pseudonoise offset, 0 to 511 in units of 64 pseudonoise code chips.

AGC is the automatic gain control DAC byte, 0 to 255 with larger numbers implying higher RF gain. Typical range is 150 to 220.

VCDAC is the upper 16 bits of the TCXO voltage control DAC word, 0 to 65535 with larger numbers implying higher TCXO frequency. Typical range is 20000 to 38000. This is the oscillator on the CDMA Receiver.

OSCDAC 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. This is the system oscillator on the CDMA Subsystem.

SN.R is the carrier signal-to-noise ratio, 0.00 to 99.9, measured in the CDMA sync channel symbol rate bandwidth. Typical range is 2.5 to 11.0.

F.ERR is the CDMA sync channel frame error rate, 0.000 to 1.000, with a higher number implying more Cyclical Redundancy Check (CRC) failures when processing the sync channel message frames. Higher numbers will correlate with lower signal-to-noise ratios.

FLTR is the fault status for the CDMA Receiver. This is a numeric value consisting of four hexadecimal characters where each bit indicates a particular receiver 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	CDMA Rcvr FLASH Writes	CDMA Rcvr FPGA Config	CDMA Signal	CDMA Rcvr Oscillator DAC
Char 1	CDMA Rcvr Oscillator	CDMA Reference Time	Synthesizer	Synthesizer Limits
Char 2	N/A	N/A	N/A	N/A
Char 3	N/A	N/A	N/A	N/A

FLTS is the fault status for the CDMA 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	CDMA Signal	System Oscillator DAC
Char 1	CDMA Receiver	Subsystem Communication	CDMA Reference Time	CDMA Receiver Communication
Char 2	N/A	System Oscillator PLL	Secondary Power Supply	Primary Power Supply
Char 3	System Power / Configuration	N/A	N/A	N/A

The Sonoma response shown below is an example that shows TFOM=6, the time and date, the current and future leap seconds are 18, the signal processor is locked, the CDMA channel is NAP_01_A, the PNO is 369, the AGC is 197, the VCDAC is 28233, the EFCDAC is 346593, the signal-to-noise ratio is 3.2 and the frame error rate is 0.049.

Command: **cdmastat**
Sonoma reply:

```
LOCKED TFOM = 6 2017  40 20:47:50 18 18 2 NAP_01_A 369 197 28233 346593  3.2 0.049
0000 0000
```

cdmaversion

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

Command: **cdmaversion**
Sonoma reply:

```
F/W 6010-0071-000 Ver 0.50 - FPGA 6020-0012-000 Ver 01 - FEB 01 16:56:37 2013
```

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: **20130116.22:24:00 23% 320056kB +67.9C**

faultstat

This command returns the summary of all system fault states in a user-friendly format. It decodes the two fault status words (FLTR and FLTS) returned in the **cdmastat** command and displays the result in a tabular form with verbose descriptions. See ***Appendix G - System Faults*** for details.

Command: **faultstat**

Sonoma reply:

```
System Fault Status:
System Oscillator DAC -------------------------> OK
CDMA Signal -----------------------------------> OK
FPGA Configuration ----------------------------> OK
FLASH Writes ----------------------------------> OK
CDMA Receiver Communication -------------------> OK
CDMA Reference Time ---------------------------> OK
Subsystem Communication -----------------------> OK
CDMA Receiver ---------------------------------> *FAULT*
System Oscillator PLL -------------------------> OK
System Power/Configuration --------------------> OK
```

If the CDMA Receiver shows a FAULT, then the list will also display receiver faults. For example:

```
CDMA Receiver Fault Status:
CDMA Receiver Oscillator DAC-------------------> OK
CDMA Signal------------------------------------> *FAULT*
CDMA Receiver FPGA Configuration---------------> OK
CDMA Receiver FLASH Writes---------------------> OK
Local Oscillator Synthesizer Tuning------------> OK
Local Oscillator Synthesizer-------------------> OK
CDMA Reference Time----------------------------> OK
CDMA Receiver Oscillator-----------------------> OK
```

get_sw_opts

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

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 cdmastat**

Sonoma reply: Information specific to the **cdmastat** command is displayed.

inetdconfig

This command starts an interactive script that allows you to configure the list of protocol servers which are started by the **inetd** super-server daemon running in the Sonoma. Three protocol servers may be configured: Time, Daytime, and Telnet. By default, the unit is configured to start all of these protocol servers. If you need to disable start-up of some or all of these, e.g. for security reasons, you must run this script as *root* from either the RS-232 serial I/O port or from a **telnet** or **ssh** session.

This script modifies the */etc/inetd.conf* file, which is 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: **inetdconfig**
Sonoma reply: Interactive script is started.

kernelversion

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

Command: **kernelversion**
Sonoma reply:
6010-0064-000_v1.00 Linux Kernel 3.2.2-Sonoma #2 Dec 19 01:08:43 2012

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 RS-232 serial I/O 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 CDMA 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 CDMA Subsystem.

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

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

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

```
20130117.00:02:40 -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 CDMA Subsystem.

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

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

LKSTAT	is the CDMA Subsystem control status, either WRM (warming up), ACQ (acquiring), LKG (locking) or LKD (locked).
COAST	is the number of seconds the CDMA Subsystem has been in coast mode (unlocked to CDMA).
ESTERR	is the estimated time error of the CDMA Subsystem when in coast mode, in seconds.
MEASERR	is the last measured time offset of the CDMA Subsystem to CDMA 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 CDMA 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 system clock 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 dis play 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:

```
20130117.00:23:10 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, Telnet and HTTPS. **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.

rcvrversion

This command displays the firmware and hardware versions of the CDMA Receiver.

Command: **`rcvrversion`**
Sonoma reply:

```
F/W 6010-0063-000 Ver 1.04 - FPGA 6020-0008-000 Ver 01 - JAN 28 13:08:52 2013
```

serialnumber

This command shows the serial number of the Sonoma. The serial number is not available using this command for units shipped before August 2015.

Command: **`serialnumber`**
Sonoma reply: **`15080056`**

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.

setcdmachannelset

This command sets the CDMA channelset to be used by the CDMA Subsystem. By factory default, the channelset is North American Cellular, unless the unit is configured for Japanese Cellular operation. In that case the hardware configuration limits operation to only the Japanese Cellular band, and this command will have no affect. The command requires one argument, which may be one of these four strings: NAC (North American Cellular), SKC (South Korean Cellular), NAP (North American PCS) or IND (India Cellular).

Command: **setcdmachannelset NAP**
Sonoma reply: **Channelset is North American PCS**

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 CDMA Subsystem reset which is similar to cycling the power on the CDMA Subsystem. It also resets the CDMA Receiver. After about 10 seconds, the boot messages from the CDMA 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 02 2013 17:48:28
FPGA 6020-0012-000 v 01
Wait 20 seconds while resetting CDMA Receiver...
Done.
```

syskernel

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: **syskernel**
Sonoma reply: **BOOTED KERNEL IMAGE = 1 (Upgrade)**

sysosctype

This command displays the 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.**

sysrootfs

This command returns the currently loaded Linux root file system, either 0 or 1, where 0 is the factory-installed root file system and 1 is the upgraded root file system.

Command: **sysrootfs**
Sonoma reply: **BOOTED ROOT FILE SYSTEM IMAGE = 1 (Upgrade)**

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 CDMA 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 CDMA, 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 CDMA Subsystem, either LOCKED or NOTLKD. NOTLKD can imply several things: the system has just started, there is a fault in the CDMA Subsystem which has caused NTP to either be unable to obtain timing information from the CDMA 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 CDMA Subsystem clock. Positive implies that the system clock is ahead of the CDMA 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.
10:	Leap second deletion will occur after 23:59:58 UTC.
11:	Fault. Unsynchronized state.

TFOM = ? A value between 6 and 9 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 CDMA Subsystem.

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

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

LS is 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 CDMA, Offset = +0.000000171, LI = 00, TFOM = 6 @ 2017  35 21:39:20 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, LOCAL-MANUAL and LOCAL-AUTO. If the time mode is Local, then you will also see the Local Time Offset (includes time zone and DST). A positive Local Time Offset implies a longitude east of the Greenwich meridian and that local time is ahead of UTC. LOCAL-MANUAL means you enter the time zone and DST information. LOCAL-AUTO means this information is decoded from the CDMA signal.

Command: **systimemode**
Sonoma reply: **Time Mode = GPS**

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_N12 CDMA 6010-0065-000 v 0.91 - Jan 25 20:50:17 2013**

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 root file system partition of the Sonoma FLASH disk. You may also use it to reset the default back to the FACTORY root 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 root 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: **updaterootflag 1**
Sonoma reply: **Default Root File System now set to: UPGRADE**

Command: **updaterootflag 2**
Sonoma reply: **Default Root File System = UPGRADE**

updatekernelflag

This command allows you to update the configuration of the Linux bootloader after a new kernel image has been written to the UPGRADE kernel partition of the Sonoma FLASH disk. You may also use it to reset the default back to the FACTORY kernel 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 kernel image should be loaded by default. If an argument value of 2 is given, then the currently configured default kernel is shown.

Command: **updatekernelflag 1**
Sonoma reply: **Default Kernel now set to: UPGRADE**

Command: **updatekernelflag 2**
Sonoma reply: **Default Kernel = UPGRADE**

upgradekernel

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: **upgradekernel**
Sonoma reply: Shows progress indicator.

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.

upgradercvr

This utility allows you to upgrade the CDMA Receiver firmware. (Prior to executing this command, you must copy the new binary firmware file to */tmp/rcvr.bin*.)

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

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

upgradesubsys

This utility allows you to upgrade the CDMA 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 CDMA Subsystem that are needed to start the X-modem file transfer, and then displays progress to the console. See ***Performing the CDMA 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.

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

An example of a software option is the Precision Time Protocol which is described in detail in ***Chapter 4 - PTP/IEEE-1588***. This section is about enabling software options in general, using the PTP Option in the examples below.

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`**

get_sw_opts

This command shows which software options are enabled in your Sonoma. The 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

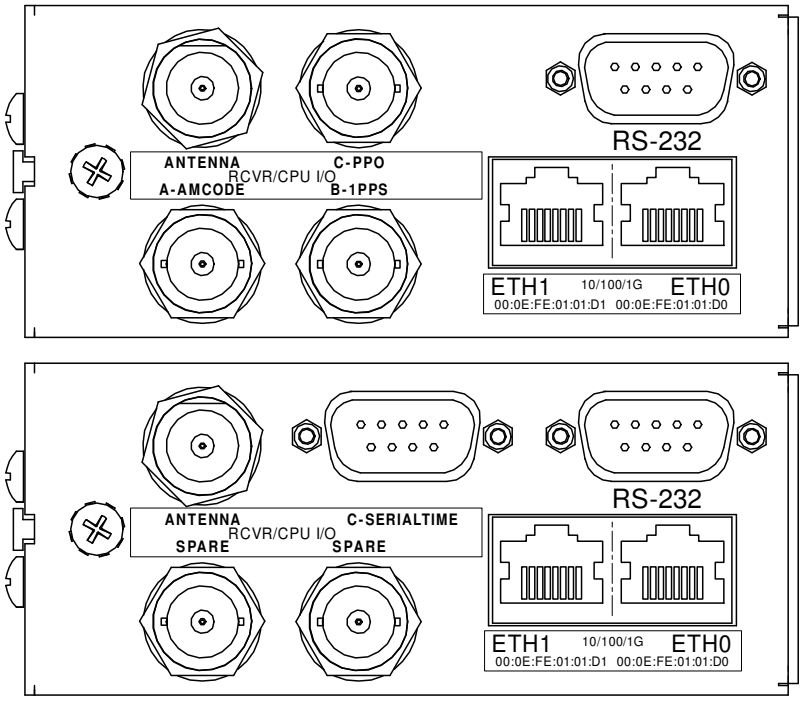
Bits are numbered from 0 to 31, from right to left. Currently, there are only two software options defined in the Sonoma. These are for PTP/IEEE-1588 enabled on port 0 (eth0) or port 1 (eth1). The table below shows the currently defined bits.

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 RS-232 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 a second 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 CDMA 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 and are GGA, GLL, GSA, RMC, VTG and ZDA. However, position and navigation are not available in a CDMA-synchronized product, so the only sentence that has been fully implemented is ZDA (time and date information).

NOTE: Up to 3 sentences may be transmitted 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..

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>

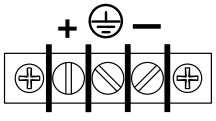
Msg ID	$GPZDA	
Field 1	175658.00	UTC time at 1PPS (hhmmss.ss)
Field 2	20	Day (01 to 31)
Field 3	05	Month (01 to 12)
Field 4	2008	Year (1980 to 2079)
Field 5	07	Local time zone hour, offset from UTC (- for east longitude)
Field 6	00	Local time zone minutes, offset from UTC
Checksum	*69	
Msg End	<CR><LF>	

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 **`cdmastat`** 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 6 to 9:

6	time error is < 100 us
7	time error is < 1 ms
8	time error is < 10 ms
9	time error is > 10 ms, unsynchronized state if never locked to CDMA

In all cases, the Sonoma reports this value as accurately as possible, even during periods of CDMA signal outage where the Sonoma is unable to directly measure the relationship of its timing outputs to UTC. During these CDMA 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 CDMA signal reception will not induce an immediate alarm condition. 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 CDMA Subsystem reaches the unsynchronized TFOM state, the NTP daemon will cease to use the timing information returned by the CDMA Subsystem in its polling event timestamps. At this point, the NTP daemon will report in its replies to network NTP clients that it is running at stratum 16 and the leap indicator bits will be set to the fault state. NTP clients will recognize that 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).

http://www.endruntechnologies.com/upgradesonomaC.htm

IMPORTANT

The Sonoma firmware consists of four 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 four firmware image files are for the Linux root file system (RFS), the Linux kernel, the CDMA Subsystem and the CDMA Receiver.

Upgrade via the HTTPS Interface

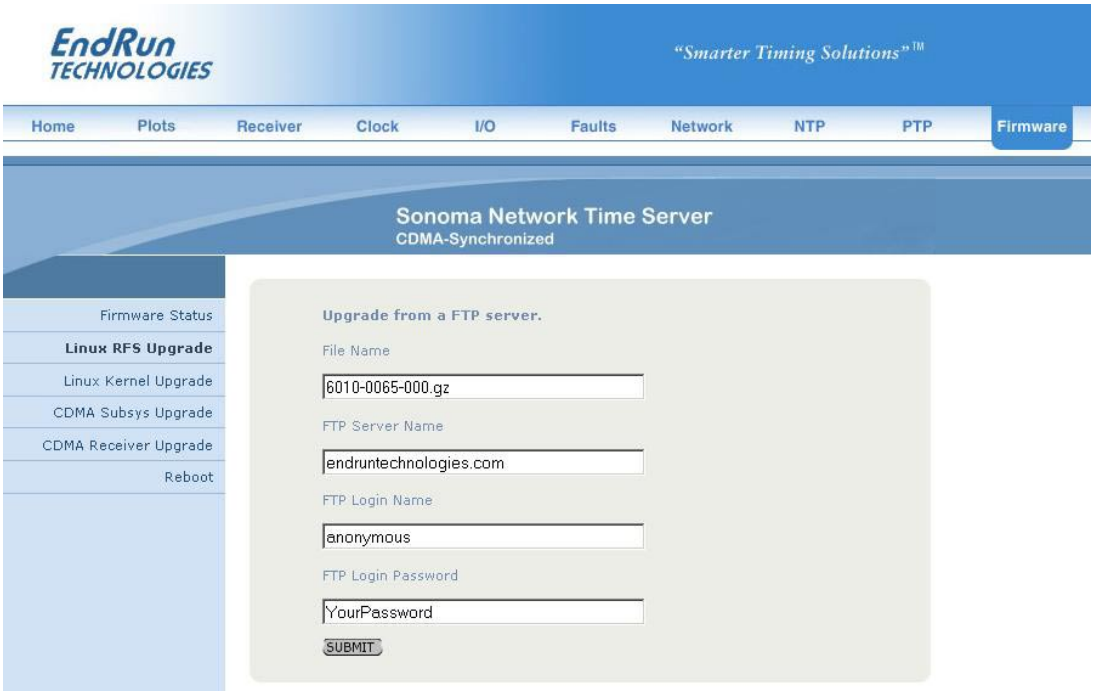
Software upgrades via the HTTPS interface are simple, with your choice of two methods:

1. If your Sonoma has access to the Internet, the HTTPS interface can automatically retrieve the appropriate files from the FTP server at **endruntechnologies.com** to temporary locations on the Sonoma. You will need to enter "root" as the user name and enter root's password. Then follow the prompts from the HTTPS interface to complete each upgrade as needed.

IMPORTANT

The 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.

The following picture shows the Linux root file system (RFS) Upgrade page. All fields are filled in with the default values needed to download the appropriate firmware image from the EndRun Technologies website. You can use these default values unless you want to point to a different FTP server.



2. If your Sonoma does not have access to the Internet, 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:

http://www.endruntechnologies.com/upgradesonomaC.htm

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 four 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 four firmware image files are for the Linux root file system (RFS), the Linux kernel, the CDMA Subsystem, and the CDMA Receiver. Here is the website link:

http://www.endruntechnologies.com/upgradesonomaC.htm

Performing the Linux RFS Upgrade

NOTE TO LINUX GEEKS

There are two FLASH disk partitions which hold the compressed Linux root file system images. 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 Linux RFS 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.

CAUTION

Some browsers will automatically unzip the file when downloading from the website. Please make sure that the downloaded file size matches what the website says it should be. Upgrading the partition with a too-large file size will cause problems.

Transfer File to Sonoma

You may transfer the file to your Sonoma using either **`ftp`** or **`scp`**. If you are using **`ftp`**, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your Sonoma: */tmp/rootfs.gz*. The root file system image will be named with the software part number and version like: *6010-0065-000_3.00.gz*. When following the instructions below, substitute the name of the actual root file system image that you are installing for *6010-0065-000_3.00.gz*. Issue these commands from the console of your Sonoma:

```
ftp remote_host                          {perform ftp login on remote host}
bin                                      {set transfer mode to binary}
get 6010-0065-000_3.00.gz /tmp/rootfs.gz  {transfer the file}
quit                                     {close the ftp session after transfer }
```

If you are 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 6010-0065-000_3.00.gz root@host.your.domain:/tmp/rootfs.gz
```

Now issue the following command to the Sonoma console to initiate the upload:

```
upgraderootfs
```

Next, update the default file system partition by issuing this command to your Sonoma console:

```
updaterootflag 1
```

You should see this line displayed:

```
Default Root File System 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 **telnet** or **ssh**. If all has gone well, you should be able to log in the usual way. After you have entered your password, the system 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

```
sysversion
```

which will cause the system version message to be re-displayed.

You can also check to see which root file system image the system is currently booted under by issuing this command at the shell prompt:

```
sysrootfs
```

Which should cause this to be printed to the console:

```
BOOTED ROOT FILE SYSTEM IMAGE = 1 (Upgrade)
```

If so, and your unit seems to be operating normally, you have successfully completed the root file system upgrade. If your unit does not boot up successfully, and you are not able to **telnet** or **ssh** into the system after 90 seconds, then there has been some kind of problem with the root file system upgrade. It is possible that the file downloaded was corrupt or that you forgot to set your **ftp** download file mode to binary when downloading the file--either from the EndRun Technologies website or when transferring it to the Sonoma.

Recovering from a Failed RFS Upgrade

To restore your Sonoma to a bootable state using the factory root file system, you must use the serial I/O port and reboot the Sonoma by cycling the power. Refer to ***Chapter 2 – Basic Installation, Con-***

nect the Serial I/O Port and Test the Serial I/O Port for setup details. When you have connected your terminal to the serial I/O 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 kernel: FACTORY
To override and boot the UPGRADE version of the kernel,
type UPGRADE within 5 seconds
.....
Booting with FACTORY Kernel


Default Root File System: UPGRADE
To override and boot the FACTORY version of the Root File System,
type FACTORY within 5 seconds
```

you must begin typing “factory” within five seconds to let the bootloader know that you are going to override the default root file system. After you hit <enter> the bootloader will boot the factory root 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 root file system upgrade and re-perform it.

Performing the Linux Kernel Upgrade

First you need to download the Linux kernel 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 either **`ftp`** or **`scp`**. If you are using **`ftp`**, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your Sonoma: */tmp/kernel.gz*. The kernel image will be named with a software part number like: *6010-0064-000_2.00.uImage*. When following the instructions below, substitute the name of the actual kernel image that you are installing for *6010-0064-000_2.00.uImage.* Issue these commands from the console of your Sonoma:

```
ftp remote_host                      {perform ftp login on remote host}
bin                                  {set transfer mode to binary}
get 6010-0064-000_2.00.uImage /tmp/kernel.gz     {transfer the file}
quit                                 {close the ftp session after transfer }
```

If you are using **`scp`**, you may open a command window on the remote computer and securely transfer the kernel image from the remote computer to your Sonoma. A command like this should be used:

```
scp -p 6010-0064-000_2.00.uImage root@host.your.domain:/tmp/kernel.gz
```

Now issue the following command to the Sonoma console to initiate the upload:

```
upgradekernel
```

Next, update the default file system partition by issuing this command to your Sonoma console:

```
updatekernelflag 1
```

You should see this line displayed:

```
Default Kernel 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 **telnet** or **ssh**. If all has gone well, you should be able to log in the usual way. You can check the running kernel version at any time by issuing

```
kernelversion
```

which will cause the kernel version message to be displayed.

You can also check to see which kernel image the system is currently booted under by issuing this command at the shell prompt:

```
syskernel
```

Which should cause this to be printed to the console:

```
BOOTED KERNEL IMAGE = 1 (Upgrade)
```

If so, and your unit seems to be operating normally, you have successfully completed the kernel upgrade. If your unit does not boot up successfully, and you are not able to **telnet** or **ssh** into the system after 90 seconds, then there has been some kind of problem with the kernel upgrade. It is possible that the file downloaded was corrupt or that you forgot to set your **ftp** download file mode to binary when downloading the file--either from the EndRun Technologies website or when transferring it to the Sonoma.

Recovering from a Failed Kernel Upgrade

To restore your Sonoma to a bootable state using the factory kernel, you must use the serial I/O port and reboot the Sonoma by cycling the power. Refer to ***Chapter 2 – Basic Installation, Connect the Serial I/O Port and Test the Serial I/O Port*** for setup details. When you have connected your terminal to the serial I/O 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 kernel: UPGRADE
To override and boot the FACTORY version of the kernel,
type FACTORY within 5 seconds
```

you must begin typing “factory” within five seconds to let the bootloader know that you are going to override the default kernel. After you hit <enter> the bootloader will boot the factory kernel. 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 kernel upgrade and re-perform it.

Performing the CDMA Subsystem Upgrade

This section has instructions for upgrading the CDMA Subsystem. If you want to upgrade the CDMA Receiver see the section below called ***Performing the CDMA Receiver Upgrade***.

First you need to download the CDMA Subsystem 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 either **`ftp`** or **`scp`**. If you are using **`ftp`** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your Sonoma: */tmp/subsys.bin*. The CDMA Subsystem image will be named with the software part number and version like: *6010-0071-000_3.01.bin*. When following the instructions below, substitute the name of the actual CDMA Subsystem image that you are installing for *6010-0071-000_3.01.bin*. You will be transferring the file to a temporary file, */tmp/subsys.bin* on your Sonoma.

```
ftp remote_host                {perform ftp login on remote host}
bin                            {set transfer mode to binary}
get 6010-0071-000_3.01.bin /tmp/subsys.bin       {transfer the file}
quit                           {close the ftp session after the transfer }
```

If you are using SSH to perform the CDMA Subsystem upgrade, you may open another command window on the remote computer and securely transfer the CDMA Subsystem image to */tmp/subsys.bin* using **`scp`** from the remote computer. A command like this could be used:

```
scp -p 6010-0071-000_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 CDMA Subsystem. You will see a file transfer progress message while it is performing the transfer. After it completes, wait about 60 seconds and issue this command to check the CDMA Subsystem version:

```
cdmaversion
```

You should see a message like this:

```
F/W 6010-0071-000 Ver 3.01 - FPGA 6020-0012-000 Ver 01 - JAN 12 15:30:58 2013
```

The firmware version should match that of the binary file that you uploaded.

Problems with the CDMA 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 CDMA 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 CDMA Subsystem upgrade, you should contact Customer Support at EndRun Technologies.

Performing the CDMA Receiver Upgrade

This section has instructions for upgrading the CDMA Receiver. If you want to upgrade the CDMA Subsystem see the section above called ***Performing the CDMA Subsystem Upgrade***.

First you need to download the CDMA 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 either **`ftp`** or **`scp`**. If you are using **`ftp`** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your Sonoma: */tmp/rcvr.bin*. The CDMA Receiver image will be named with the software part number and version like: *6010-0063-000_1.04.bin*. When following the instructions below, substitute the name of the actual CDMA Receiver image that you are installing for *6010-0063-000_1.04.bin*. You will be transferring the file to a temporary file, */tmp/rcvr.bin* on your Sonoma.

```
ftp remote_host              {perform ftp login on remote host}
bin                          {set transfer mode to binary}
get 6010-0063-000_1.04.bin /tmp/rcvr.bin  {transfer the file}
quit                         {close the ftp session after the transfer }
```

If you are using SSH to perform the CDMA Receiver upgrade, you may open another command window on the remote computer and securely transfer the CDMA Receiver image to */tmp/rcvr.bin* using **`scp`** from the remote computer. A command like this could be used:

```
scp -p 6010-0063-000_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 CDMA 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 CDMA Subsystem (and Receiver):

```
subsysreset
```

After it completes, wait about 60 seconds and issue this command to check the CDMA Receiver version:

```
rcvrversion
```

You should see a message like this:

```
F/W 6010-0063-000 Ver 1.04 - FPGA 6020-0008-000 Ver 01 - JAN 28 13:08:52 2013
```

The firmware version should match that of the binary file that you uploaded.

Problems with the CDMA 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 CDMA 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 CDMA Receiver upgrade, you should contact Customer Support at EndRun Technologies.

This page intentionally left blank.

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).

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.

Change Password

This command is used to change the password for the user that you are logged in as. It affects the serial port, SSH, Telnet 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 serial port banner, the Telnet 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 (10/100/1000Base-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.

GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) 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 this service 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 make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. 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.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in

reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NTP Software License

Information about the NTP Project, led by Dr. David Mills, 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:

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
***********************************************************
*                                                         *
* Copyright (c) David L. Mills 1992-2006                  *
*                                                         *
* 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

The Apache server as implemented in the Sonoma is cover by copyrights.

See the license at http://www.apache.org/licenses/LICENSE-1.1

Information about Apache can be found at http://httpd.apache.org. The distribution and usage of Apache is allowed, as long as the following copyright notice is included in our documentation. This notice applies as if the text was explicitly included each file.

```
/*  ====================================================
 * The Apache Software License, Version 1.1
 *
 * Copyright (c) 2000 The Apache Software Foundation.  All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
```

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 at
http://standards.ieee.org/db/patents/pat1390.html

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 following 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 CDMA Antenna

Installing the CDMA Antenna is usually very easy, simply mount on top of your equipment rack inside your building. This appendix contains antenna mounting guidelines in case you encounter problems receiving a signal.

Antenna Location

Place the antenna on a flat, preferably metallic surface while the unit is searching for the signal. Make sure that it is not blocked by large metallic objects closer than one meter. The Sonoma Sync LED should follow the sequence below within 20 minutes.

Acquire and Lock Status Sequence

The Lock LED on the front-panel shows the status of the CDMA Subsystem/Receiver as it acquires and locks on to a signal:

1. The Sync LED is solid amber while not detecting a signal.

2. When the unit has detected a CDMA signal, the Sync LED will flash very slowly (about a .4 Hz rate).

3. As the unit locks onto the CDMA signal and begins to decode the timing data, the Sync LED will flash very rapidly (about a 6 Hz rate) until the data is fully decoded.

4. Once the Sonoma is fully locked to a signal, then the Sync LED will pulse at precisely a one second rate, synchronized to UTC seconds.

If your Sonoma does not lock within 20 minutes, then you should move the antenna or change its orientation as described below.

Moving the Antenna

Although the antenna should normally be installed in a vertical orientation, usually multipath conditions due to signal reflections indoors cause at least some of the signal to be horizontally polarized, so do not be surprised if you find that the unit will work with the antenna oriented either way.

Multipath conditions can also cause another effect: signal cancellation. Since the wavelength of the signal is only about 12 to 30 centimeters, movement of the antenna just a few centimeters can sometimes cause significant signal strength changes.

Changing the Channelset

If you are still unable to find an antenna location where the unit will acquire the CDMA signals, you may not have *cellular* coverage in your area or the *cellular* signals might be too weak in your facility.

Use the **`setcdmachannelset`** command to change your Sonoma to search *PCS*, rather than *cellular* frequencies. (If you are in Japan, India, or Korea you will not be able to do this.) Use the **`cdmachannelset`** command to view the current setting. For more details on these commands see ***Chapter 9 - Console Port Control and Status***. Type this at the console:

```
setcdmachannelset NAP
```

NAP means North American PCS. It takes longer for the Sonoma to search all the PCS signals so do not be surprised if you need to wait a few hours. If your Sonoma is still unable to lock to a signal, then continue to try for at least a day, since base stations are taken down for service from time to time.

If you have a CDMA phone, see if it will work in *digital* mode. If it will, then your Sonoma should be able to lock. Please contact EndRun Customer Support for assistance.

Using a CDMA Preamplifier

EndRun produces a CDMA Preamplifier which is a very high-performance, low-noise, low-power drain, inline amplifier for difficult signal environments. Using the preamplifer you can use a longer cable and locate your antenna up to 100 feet (30 meters) away from the Sonoma. This may be useful at some facilities where the CDMA signal is poor.

There is a different preamplifier for *PCS*, *cellular,* and *Japanese* frequencies. So you will need to know which type you want before ordering. An Installation Guide for installing a CDMA antenna with preamplifer is shown in Figure 1A and 1B.

CDMA Antenna Mounting Guidelines
(with in-line amplifier)

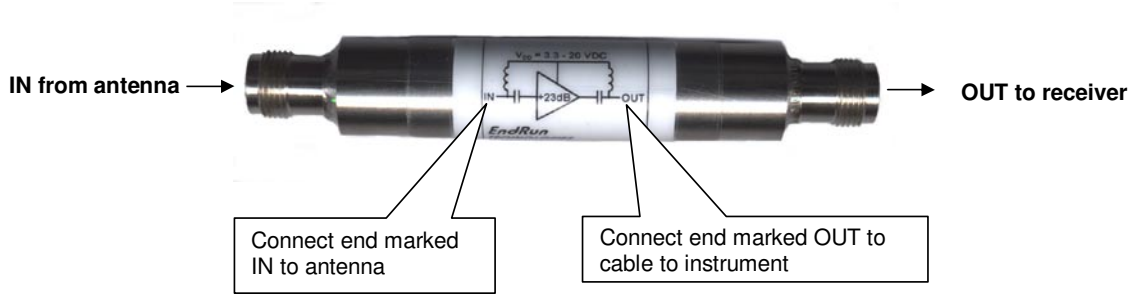
Locating Mounting Site

The ideal mounting would be to locate the antenna on a flat, preferably metallic surface such as the top of the equipment rack. The antenna base is magnetic and will hold in place on steel surfaces. Make sure that the antenna is not blocked by large metallic objects closer than one meter. Although the antenna should normally be installed in a vertical orientation, usually multipath conditions due to signal reflections indoors cause at least some of the signal to be horizontally polarized, so do not be surprised if you find that the unit will work with the antenna oriented either way. Multipath conditions can also cause another effect: signal cancellation. Since the wavelength of the signal is only about thirty centimeters, movement of the antenna just a few centimeters can sometimes cause significant signal strength changes.

Antenna Cable Connection

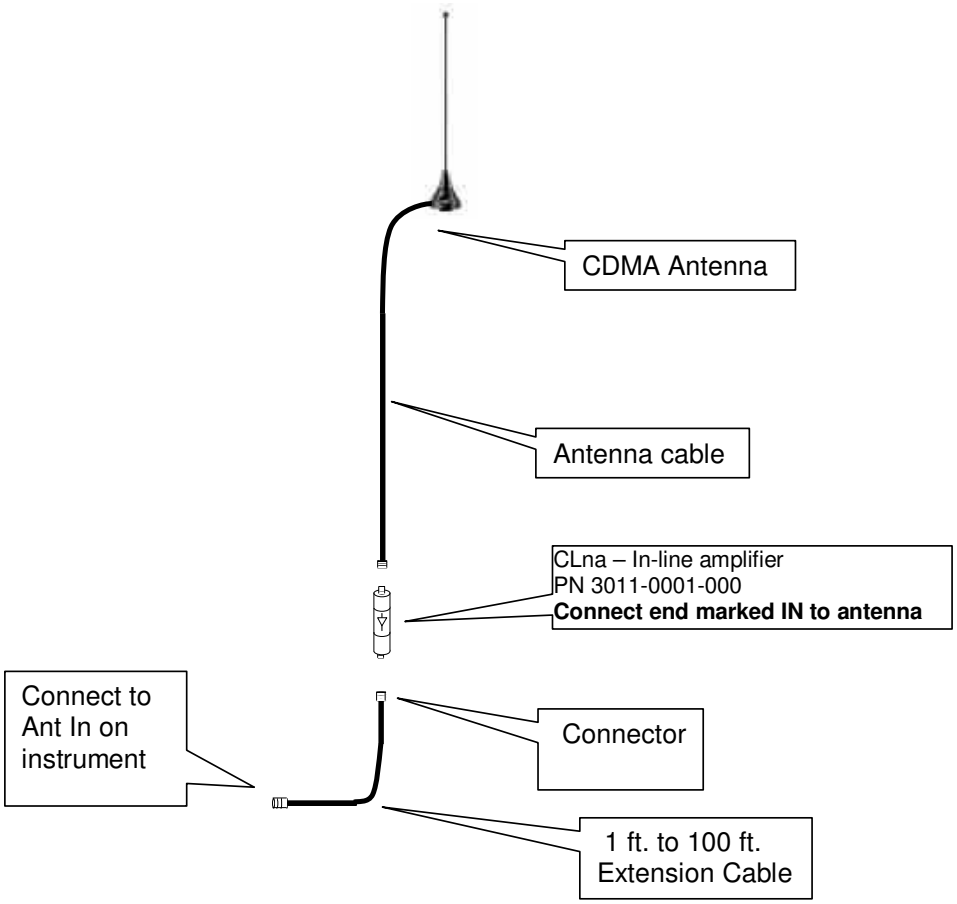
Locate end of antenna cable with connector. Connect this end to the in-line amplifier (end marked input). Connect extension cable (1 foot to 100 feet long) between in-line amplifier (end marked output) to the CDMA receiver unit.

IMPORTANT! Observe in-line amplifier connection orientation as illustrated below:



5050-0005-000 1 of 2 27Apr2007

FIGURE 1A - CDMA ANTENNA MOUNTING GUIDELINES WITH PREAMPLIFIER



5050-0005-000 2 of 2 27Apr2007

FIGURE 1B - CDMA ANTENNA MOUNTING GUIDELINES WITH PREAMPLIFIER

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 3 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.

Notification of Leap Second Insertion

Your CDMA-synchronized Sonoma delivers very precise time and is generally troublefree. However, when a leap second insertion is scheduled (about every three years), then you must manually program the new leap seconds into your unit. You will have many months notice in which to do this. It is a very simple procedure. See ***Configure for Leap Second Event*** below.

The International Earth Rotation Service (IERS) notifies the world of a pending leap second event almost six months ahead of time. The EndRun Technologies' website has a page devoted to notifying users of the next leap second occurrence. This page will also tell you exactly what you need to do to program the new leap seconds in your Sonoma. The appropriate link is:

http://www.endruntechnologies.com/leap.htm

If you wish to be notified by EndRun Customer Support when a leap second is pending, then send an email request to support@endruntechnologies.com. Ask to be put on the leap second notification list.

Configure for Leap Second Event

About once every three years you will need to program your Sonoma with new leap second information. To view and change the leap second settings use commands **`cdmaleapmode`** and **`cdmaleapconfig`**. (See ***Chapter 9 - Console Port Control & Status***.) Once you have programmed the unit for the next leap second insertion you can forget about it. Since the values you set are stored in FLASH memory, you can cycle power on your Sonoma with no problem.

The information at the website link shown above gives you details on programming the new leap second information.

When the unit is configured at the factory prior to shipping, the current and future leap second values are set appropriately for the next possible leap second insertion date (June 30th or December 31st).

Background Information

Another way to get the leap second information is to go to the International Earth Rotation Service (IERS) website. If a leap second is pending it will be posted by the IERS approximately six months in advance of insertion. This information is available in the latest Bulletin C at the (IERS) website:

http://www.iers.org

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. Leap seconds may only be inserted at UTC midnight (after 23:59:59) on June 30 or December 31. Bulletin C confirms either that a leap second will or will not be inserted at the next possible insertion point. Since the introduction of leap seconds in 1961, they have been added approximately once every 18 months.

The leap seconds which are needed for your Sonoma are actually the difference between GPS and UTC. The GPS time scale began on January 6, 1980. At that time, the UTC timescale had already undergone 19 leapsecond insertion events. If you are obtaining your leap second information from the IERS website, you will need to subtract 19 from the TAI-UTC leap second values published there to obtain GPS-UTC, the number needed to set the current and future leap seconds for the Sonoma. At the time of this writing in April 2017, TAI-UTC was 37 seconds and GPS-UTC was 18 seconds.

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

One fault can be masked. This is the SIG (CDMA Signal) fault. When masked, this fault will not cause an alarm. You may want to mask the SIG fault if you are operating your Sonoma as a Stratum 2 server and are not using a CDMA signal. For information on Stratum 2 see ***Chapter 2 - NTP, Configuring the Sonoma as a Stratum 2 Server***.

To mask the fault use the **`setsigfltmask`** command. For more information see ***Chapter 9 - Console Port Control and Status*** or type **`help setsigfltmask`** at the console port.

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 DAC for the oscillator has reached either the high or low alarm limit while locked to the CDMA 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.

CDMA Signal (SIG)

This fault indicates that the CDMA Subsystem has not been able to acquire a CDMA 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.

CDMA Subsystem FPGA Configuration (FPGA)
This fault indicates that the CDMA Subsystem is unable to configure the FPGA. This is a fatal fault. Please contact EndRun Customer Support.

CDMA Subsystem FLASH Writes (FLSH)
This fault indicates that the CDMA 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.

CDMA Receiver Communication (RCVC)
This fault indicates that the CDMA Subsystem is unable to establish communications with the CDMA Receiver. Please contact EndRun Customer Support.

CDMA Reference Time (REF)
This fault indicates that the CDMA Subsystem received an erroneous time input from the CDMA Receiver. If the condition persists please contact EndRun Customer Support.

Subsystem Communication (POLL)
This fault indicates that the CDMA 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.

CDMA Receiver (RCVF)
This fault indicates a problem with the CDMA Receiver. See the section below (***Receiver Faults***) for more information.

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.

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 CDMA 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.

CDMA 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 CDMA 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.

CDMA Signal (SIG)
This fault indicates that the CDMA Receiver has not been able to acquire a CDMA 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.

CDMA Receiver FPGA Configuration (FPGA)
This fault indicates that the CDMA Receiver is unable to configure the FPGA. This is a fatal fault. Please contact EndRun Customer Support.

CDMA Receiver FLASH Writes (FLSH)
This fault indicates that the CDMA 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.

Local Oscillator Synthesizer Tuning (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.

Local Oscillator 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.

CDMA Reference Time (REF)
This fault indicates that the CDMA Receiver received an erroneous time input from the CDMA signals. If the condition persists please contact EndRun Customer Support.

CDMA Receiver Oscillator (OSC)
This fault indicates that the main oscillator has failed. Please contact EndRun Customer Support.

This page intentionally left blank.

Appendix *H*

Specifications

CDMA Receiver:

Cellular Mobile Receive Band - 869-894 MHz (Standard)
North American PCS Mobile Receive Band – 1930-1990 MHz (Standard)
Japanese Cellular Mobile Receive Band – 860-875 MHz (Optional Configuration)
TIA/EIA IS-95 CDMA Pilot and Sync channels.

Antenna:

TNC jack on rear panel, Z_{in} = 50Ω.
Dual Band, 824-896 MHz/1850-1990 MHz,
magnetic-base monopole with integral 12 ft. RG-58/U cable and TNC plug.
Extension cables and low noise pre-amplifiers are available as options.

System Oscillator:

TCXO is standard (2.5 x 10^{-6} over -20° to 70° C).
Options: OCXO (4x10^{-9} over 0 to 70° C).
Rubidium (1x10-9 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).

Server Performance and Synchronization Accuracy:

CDMA Receiver Accuracy: <10 microseconds to UTC when locked, typical.
NTP Timestamp Accuracy: <10 microseconds @ 7500 requests/second.
NTP Client Synchronization Accuracy: Network factors can limit LAN synchronization accuracy to 1/2 to 2 milliseconds, typical.

Server Platform:

Operating System Kernel Version: 3.2.2
Slackware Linux Distribution: 13.1
Processor: 1.2 GHz.
RAM: 512M
FLASH: 512M

Supported IPv4 Protocols:

SNTP, NTP v2, v3, 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
TIME and DAYTIME server
TELNET client/server
FTP client
DHCP client
SYSLOG
HTTPS
PTP/IEEE-1588 (Option)

Supported IPv6 Protocols:

SNTP, NTP v2, v3, 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
TIME and DAYTIME server
HTTPS
Note: See ***Chapter 8 - IPv6 Information*** for more details.

PTP/IEEE-1588 Grandmaster (Option):

IEEE-1588-2008 (V2).
Parameters: Default Profile. Multicast or Hybrid (mixed Unicast/Multicast). Two-Step Clock.
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..
10/100/1000Base-T Ethernet.
Two LEDs on each port indicate speed and activity:
Amber LED indicates activity.
Green LED indicates speed (1 pulse = 10M, 2 pulses = 100M, 3 pulses = 1G).

System Status LEDs:

Sync LED: Amber LED pulses to indicate CDMA acquisition and lock status.
Alarm LED: Red LED indicates a fault condition.

Serial Port I/O:

Signal: I/O port at RS-232 levels for secure, local terminal access.
Parameters: 19200 baud, 8 data bits, no parity, 1 stop bit.
Connector: Rear-panel DB-9M connector labeled “RS-232”.
To connect to a computer, a null-modem adapter must be used. The serial cable provided with the shipment is wired as a null-modem. Pinout for the RS-232 console port is shown below.
Note: For operational details see ***Chapter 9 - Console Port Control and Status***.

Sonoma DB9M Pin	Signal Name
1	Not Connected
2	Receive Data (RX)
3	Transmit Data (TX)
4	Not Connected
5	Ground
6	Not Connected
7	Not Connected
8	Not Connected
9	Not Connected

Size:

Chassis:	1.75”H x 17.0”W x 10.75”D, 19” rackmount
Weight:	< 8 lb. (3.6 kg.)
Antenna:	14”H x 2” diameter at base.

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:	10 watts.
Sonoma with OCXO:	11-13 watts, depending on ambient temperature.
Sonoma with Rb:	16-23 watts, depending on ambient temperature.

90-264 VAC, 47-63 Hz, 1.0A Max. @ 120 VAC, 0.5A 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.

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: < 10 microseconds to UTC when locked, typical.
Stability: TDEV < 50 ns, $\tau < 10^4$ 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.
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: $< 10^{-11}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^3$ seconds, $\sigma_y(\tau) < 10^{-6}/\tau$ for $\tau > 10^3$ 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: $< 10^{-11}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^3$ seconds, $\sigma_y(\tau) < 10^{-6}/\tau$ for $\tau > 10^3$ 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".

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: $< 10^{-11}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^3$ seconds, $\sigma_y(\tau) < 10^{-6}/\tau$ for $\tau > 10^3$ seconds.
Connector: Rear-panel BNC jack labeled with appropriate rate such as "10 MPPS".

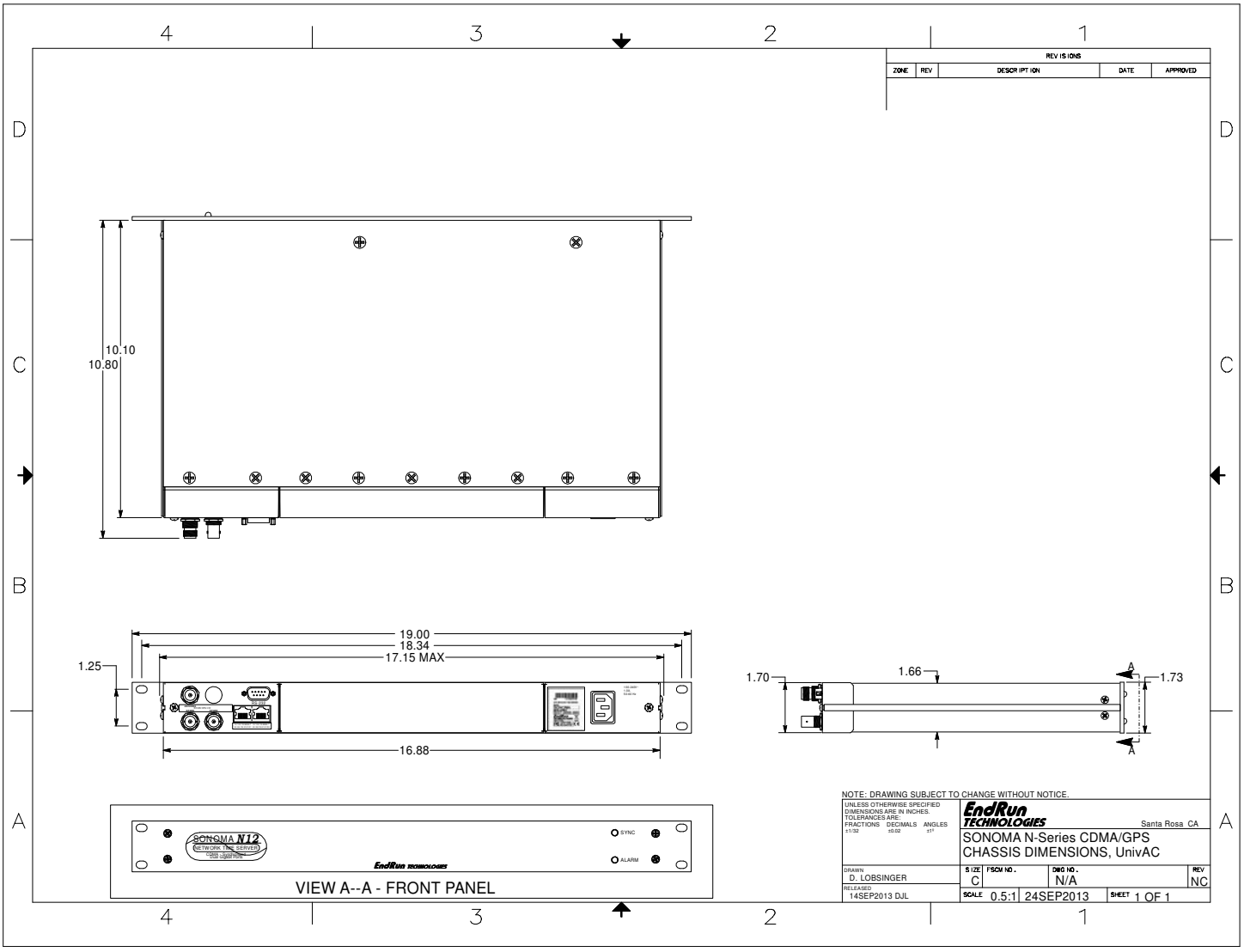
Compliance:

CE/FCC:	RTTE Directive 1999/5/EC
	Low Voltage Directive 2006/95/EC
	EMC Directive 2004/108/EC
RoHS:	RoHS Directive 2011/65/EC
WEEE:	WEEE Directive 2012/19/EC

Supplementary Compliance Data:

Safety:	EN60950-1:2006/A11:2009/A1:2010/A12:2011
EMC:	EN55022:2010, EN55024:2010
	EN61000-3-2:2006 +A1 +A2, EN61000-3-3:2008
	VCCI (V3/2012.04)
	AS/NZS CISPR 22 (2009) +A1
	FCC Part 15 Subpart B Sections 15.107 and 15.109

Data subject to change.
EndRun Technologies may make changes
to specifications and product descriptions
at any time, without notice.


REVISIONS
ZONE
REV
DESCRIPTION
DATE
APPROVED
10.10
10.80
19.00
18.34
17.15 MAX
1.25
16.88
1.70
1.66
1.73
SONOMA N12
NETWORK TIME SERVER
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 CDMA/GPS
CHASSIS DIMENSIONS, UnivAC
DRAWN
D. LOBSINGER
RELEASED
14SEP2013 DJL
SIZE
C
FSCM NO.
DWG NO.
N/A
REV
NC
SCALE
0.5:1
24SEP2013
SHEET
1 OF 1

CE

EndRun TECHNOLOGIES

DECLARATION OF CONFORMITY

(According to ISO/IEC GUIDE 22 and EN 45014)

Manufacturer's Name: EndRun Technologies, LLC

Manufacturer's Address: 2270 Northpoint Parkway, Santa Rosa, California 95407, U.S.A.

DECLARES, THAT THE PRODUCT

Product Name: Network Time Server

Model Number:
3026-XYYY-ZZZ (Sonoma D Series CDMA Network Time Server)
3027-XYYY-ZZZ (Sonoma D Series GPS Network Time Server)
3028-XYYY-ZZZ (Sonoma N Series CDMA Network Time Server)
3029-XYYY-ZZZ (Sonoma N Series GPS Network Time Server)
3030-XYYY-ZZZ (Tycho CDMA Frequency Reference)
3031-XYYY-ZZZ (Tycho GPS Frequency Reference)
3032-XYYY-ZZZ (Meridian CDMA Frequency Reference)
3033-XYYY-ZZZ (Meridian GPS Precision TimeBase)
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: 2006 / 95 / EC
R&TTE Directive: 1999 / 5 / EC
EMC Directive: 2004 / 108 / EC
RoHS Directive: 2011 / 65 / EC
WEEE: 2012 / 19 / EC

Supplementary Information:

Safety: EN60950-1:2006/A11:2009/A1:2010/A12:2011

EMC: EN55022:2010, EN55024:2010
EN61000-3-2:2006 +A1 +A2, EN61000-3-3:2008
VCCI (V3/2012.04)
AS/NZS CISPR 22 (2009) +A1
FCC Part 15 Subpart B Sections 15.107 and 15.109

Year Mark First Applied: 2013

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.

Place: Santa Rosa, CA, USA
Date: 4/2/2013

Signature: _____
Full Name: David J. Lobsinger
Position: V. P. Hardware Engineering

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