EndRun TECHNOLOGIES
"Smarter Timing Solutions"

Unison *GPS*

Network Time Server

User Manual

Unison *GPS*

Network Time Server User Manual

Preface

Thank you for purchasing the Unison Network Time Server. Our goal in developing this product is to bring precise, Universal Coordinated Time (UTC) into your network quickly, easily and reliably. Your new Unison 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 is dedicated to the development and refinement of the technologies required to fulfill the demanding needs of the time and frequency community.

Our innovative engineering staff, with decades of experience in the research and development of receiver technology for the Global Positioning System (GPS), has created our window-mount GPS antenna and extended hold-over oscillator-control algorithms.

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 earth stations, and calibration laboratories.

EndRun Technologies is committed to fulfilling your precision timing needs by providing the most advanced, reliable and cost-effective time and frequency equipment available in the market today.

Trademark Acknowledgements

IBM-PC, Linux, NotePad, Timeserv, UNIX, Windows NT, WordStar are registered trademarks of the respective holders.

Part No. USM3017-0000-000 Revision 15
February 2012

Copyright © EndRun Technologies 2005-2012

About This Manual

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

Introduction – The Unison, how it works, where to use it, its main features.
Basic Installation – How to connect, configure and test your Unison with your network.
Client Set-Up – Two sections; one for Unix-like platforms and one for Windows NT/2000/XP.
Console Port – Description of the Linux console commands for use over the network and serial ports.

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 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

The MTBF (Mean Time Between Failures) for this product is 225,000 hours (25 years). 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 REMEMDIES 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 shipping 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 shipping 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.

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

Table of Contents

Chapter*One*

Introduction

The Unison is a precision server of Universal Coordinated Time (UTC) that can be connected via a 10/100Base-T ethernet port to any TCP/IP network. In its most basic operation, it sends Network Time Protocol (NTP)/Simple Network Time Protocol (SNTP) reply packets in response to NTP/SNTP request packets which it has received from clients. The timestamps it sends in its NTP/SNTP reply packets are accurate to less than one-hundred microseconds. NTP/SNTP client software is available for virtually all operating systems.

The Unison is composed of a Global Positioning System (GPS) time and frequency engine integrated with an IBM-PC compatible fanless, convection-cooled 133 MHz CPU with integral ethernet interface, RS-232 serial port and a power supply. Non-volatile storage of the embedded Linux operating system and the Unison application software is via FLASH memory.

For more detailed information that is not included in this manual, and links to other sites, please visit our website: http://www.endruntechnologies.com*. There you can also download firmware upgrades, the latest manuals and other documentation.*

GPS Timing-How It Works

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

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

Each satellite in the constellation contains redundant cesium beam or rubidium vapor atomic frequency standards. These provide the timebase for all transmissions from each satellite. These transmissions are monitored from ground stations located around the world and carefully measured relative to

GPS time. The results of these measurements for each satellite are then uploaded to that satellite so that they may be incorporated into the data contained in its transmissions. The receiver can use this data to relate the time-of-arrival of the received transmissions from that satellite to GPS time.

All of this means that during normal operation, the source of the timing information being transmitted from each of the satellites is directly traceable to UTC. Due to the nature of the GPS spread spectrum Code Division Multiple Access (CDMA) modulation scheme, this timing information may be extracted by a well-designed receiver with a precision of a few nanoseconds. The GPS time and frequency engine in the Unison does just that.

Where to Use It

Since signals from the GPS satellites are available at all locations on the globe, you may deploy the Unison virtually anywhere. However, you must be able to install an antenna either on the rooftop or in a window so that satellite transmissions may be received at least several times during the day. Once synchronized, the Unison can maintain acceptable network synchronization accuracy for about a day without GPS reception, by flywheeling on its standard temperature compensated crystal oscillator.

Because the Unison 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.

Main Features

Performance, Reliability and Economy

The Unison provides high performance and reliability combined with low power consumption and cost. Its internal sub-assemblies are fabricated using state-of-the-art components and processes and are integrated in a solid, high-quality chassis.

Flexibility

It supports a variety of TCP/IP network protocols compatible with a variety of platforms and operating systems.

Easy Installation

Its standard 1U high, 19” rack-mountable chassis and rooftop or window-mounted antenna make installation simpler compared to competing products that require rooftop installation of the antenna. The rack-mount chassis may be mounted in any convenient location. Connect it to your network via the rear panel mounted, 10/100Base-T RJ-45 connector and plug in the AC power cord. Initial network configuration is automatic on networks using the Dynamic Host Configuration Protocol (DHCP). Manual network configuration is via the RS-232 serial I/O port and a simple Linux shell script.

Free FLASH Upgrades

Firmware and configurable hardware parameters are stored in non-volatile FLASH memory, so the Unison can be easily upgraded in the field using FTP and TELNET or the local RS-232 serial I/O port. Secure upgrades are possible via SSH and SCP. We make all firmware upgrades to our products available to our customers free of charge.

Chapter *Two*

Basic Installation

This chapter will guide you through the most basic checkout and physical installation of your Unison. Subsequent chapters and appendices will give you the information needed to configure your installation for the maximum performance in your operating environment. General NTP client setup instructions will also be supplied to get you started using your Unison quickly.

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.*

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 Unison shipment typically contains:

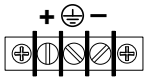
- Unison (part # 3017-0001-000 or #3017- variant)
- Unison User Manual (part #USM3017-0000-000) on CD (part# 5102-0001-000)
- IEC 320 AC Power Cord (part #0501-0003-000)
  (This part will not be present if using the DC power option.)
- DB9F-to-DB9F Null-Modem Serial I/O Cable (part #0501-0002-000)
- RJ-45 to RJ-45 CAT-5 patch cable, 2 meters (part #0501-0000-000)
- Antenna/cable assembly (part #0610-0007-001 or #0610- variant)

Unison Physical Description

Sync LED	This green LED flashes to indicate synchronization status.
Network LED	This amber LED illuminates when the Unison is connected to the network and flashes when receiving or transmitting packets..
Alarm LED	This red LED illuminates briefly at power-up, and thereafter whenever a serious fault condition exists.

Antenna Jack	This TNC connector mates with the downlead cable from the external antenna.
RS-232 Connector	This DB-9M connector provides the RS-232 serial I/O console interface to the Unison. This console allows the user to initialize and maintain the Unison. See ***Chapter 5 - RS-232 Serial I/O Port Signal Definitions*** for detailed information.
10/100Base-T Jack	This RJ-45 connector mates with the ethernet twisted pair cable from the network.
1PPS Jack *(Option)*	This optional BNC connector provides the 1PPS Output (TTL). The pulse width is normally 1 millisecond wide when shipped from the factory but can be changed via console command **`cpuoptsconfig`**. See signal definition in ***Appendix J - Specifications*** for the 1PPS Output.
1PPS (RS-422) *(Option)*	This optional DB-9M connector provides the 1PPS output at RS-422 levels and is usually not installed.. The pulse width is normally 1 millisecond wide when shipped from the factory but can be changed via console command **`cpuoptsconfig`**. See pinout details in ***Appendix J - Specifications*** for the 1PPS RS-422 Output.
AM Code Jack *(Option)*	This BNC connector provides the optional amplitude-modulated time code output, and is usually labeled “SPARE”. The time code output is normally IRIG-B122 when shipped from the factory, but can be changed via command **`cpuoptsconfig`**. See details in ***Appendix J - Specifications*** for the AM Code Output.

Alarm Jack *(Option)*	This BNC connector (or terminal strip) provides the optional alarm output, and is usually not installed. If installed, see details in ***Appendix I - Specifications*** for the Alarm Output.
Prog TTL Jack *(Option)*	This BNC connector provides the optional Programmable TTL pulse rate output and is usually not installed. If installed, see signal definition in ***Appendix J - Specifications***. This pulse rate is normally shipped from the factory as 10MPPS but can be changed via command **`cpuoptsconfig`**.
10 MPPS or 100 PPS, etc. *(Option)*	This BNC connector provides an optional customer-specified rate output and is usually not installed. If installed, it will be labeled for the appropriate rate such as "10 MPPS" or "100 PPS", etc. This output is set at the factory and cannot be changed. See signal definition in ***Appendix J - Specifications*** for the Fixed Rate Output.
Serial Time *(Option)*	This optional DB-9M connector provides the serial I/O interface with a once-per-second ASCII time string output and is usually not installed. For further information refer see description in ***Appendix G - Serial Time Output.***
AC Power Input Jack	This IEC 320 standard three-prong connector provides AC power.
DC Power Input Block	This optional 3-position terminal block provides connection to the DC power source, and replaces the AC power input jack.



Performing an Initial Site Survey

Using the status LED indicators, it's easy to find out if your Unison 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 Unison.

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 Unison.

Place the antenna in a window, or for best performance, mount it on the roof using the supplied mounting hardware. Make sure that it is not blocked by large metallic objects closer than one meter. Although the antenna should normally be installed in a vertical orientation for rooftop installations, when window mounting it should be pointed out the window, in the direction that gives the best clear view to the sky. This will improve its ability to receive signals from satellites near the horizon. For more information see ***Appendix I - Installing the GPS Antenna***.

Initially upon power up:

1. The unit will light the red Alarm Status LED for about ten seconds.

2. Then it will continuously light the green Sync Status LED.

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

4. Then the green Sync Status LED will pulse at precisely a 1 Hz rate, synchronized to UTC seconds, with a short on duration relative to the off duration.

At this point, the GPS time and frequency engine has fully synchronized, and you may proceed to permanently mounting the chassis and antenna in their desired locations.

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

If you are unable to achieve GPS lock after trying all of these suggestions, then your Unison may be damaged and should be returned to the factory for repair or exchange.

Installing the Unison

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 harmful interference in which case the user will be required to correct the interference at his own expense.

Mount the Unison

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

CAUTION

Ground the unit properly with the supplied power cord.

Position the power cord so that you can easily disconnect it from the Unison.

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

Connecting the DC Power Option

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 Unison 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 in-lbs (1 nM).

Branch circuit must have circuit breaker, 15A or less.

Install terminal block cover after wiring.

Connecting and Configuring Ethernet

Connect one end of the CAT-5 patch cable supplied with your Unison to the rear panel mounted RJ-45 connector labeled 10/100BASE-T. Connect the other end of the patch cable to your network through a 'straight' port on your hub. Do not connect it to a 'crossover' port on your hub.

By factory default, the Unison will attempt to configure the ethernet interface automatically via the Dynamic Host Configuration Protocol (DHCP). The Unison 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 Unison to also set its hostname via DHCP, if your DHCP server is configured to provide it. You can do this by running a simple shell 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 Unison up and running, you may procede 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 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 interface using the RS-232 serial I/O port. The following sections contain brief descriptions on how to do that.

Configuring Ethernet with the Serial Port

To configure your ethernet interface with the serial port, after logging in as the *root* user, you must run a simple shell script called **`netconfig`** from the **`bash`** shell prompt. This shell 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 Unison using its RS-232 serial I/O port.

Connect the RS-232 Serial I/O Port

You will need to use the RS-232 serial I/O port if your network does not support the Dynamic Host Configuration Protocol (DHCP). In that case, you must be able to configure the Unison network

parameters manually using the Linux console shell interface which is provided by this serial I/O port. Under certain conditions, you may also need to use the RS-232 serial I/O port if you encounter a problem while upgrading the firmware in your Unison.

To test serial communications with the Unison 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 Unison.

2. Connect one end of the DB9F-to-DB9F null modem adapter cable to the serial I/O jack on the Unison.

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 ***Chapter 5 - RS-232 Serial I/O Port Signal Definitions*** 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.*

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***. You must also configure your terminal to use the correct baud rate, number of data bits, parity type and number of stop bits. *Be sure to turn off any hardware or software handshaking.* The settings for the Unison are:

- 19200 is the Baud Rate
- 8 is the number of Data Bits
- None is the Parity
- 1 is the number of Stop Bits

After configuring these parameters in your terminal, apply power to the Unison. After about 20 seconds, your terminal should display a sequence of boot messages similar to these:

```
************************************************
* 6010-0040-000 Linux Bootloader v1.00 08/17/2004 *
************************************************
Default root file system: FACTORY
To override and boot the UPGRADE partition type 'UPGRADE' within 5 seconds...
.....
```

These lines are the Linux bootloader boot prompt. This prompt will timeout after 5 seconds and the Linux kernel and the factory default Unison 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:

```
Booting Linux with FACTORY root file system...

6010-0041-000 Linux Kernel v2.4.26-1 #0 Wed Aug 18 17:28:45 UTC 2004
BIOS-provided physical RAM map:
BIOS-88: 0000000000000000 - 000000000009f000 (usable)
BIOS-88: 0000000000100000 - 0000000002000000 (usable)
32MB LOWMEM available.
On node 0 totalpages: 8192
```

```
zone(0): 4096 pages.
zone(1): 4096 pages.
zone(2): 0 pages.
DMI not present.
Kernel command line: config=11000001 initjffs=0 console=ttyS0,19200 root=/dev/
mtdblock4 load_ramdisk=1 rw
Initializing CPU#0
Calibrating delay loop... 66.96 BogoMIPS
Memory: 30784k/32768k available (812k kernel code, 1596k reserved, 162k data, 68k
init, 0k highmem)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
Dentry cache hash table entries: 4096 (order: 3, 32768 bytes)
Inode cache hash table entries: 2048 (order: 2, 16384 bytes)
Mount cache hash table entries: 512 (order: 0, 4096 bytes)
Buffer cache hash table entries: 1024 (order: 0, 4096 bytes)
Page-cache hash table entries: 8192 (order: 3, 32768 bytes)
CPU: AMD 486 DX/4-WB stepping 04
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
PCI: Using configuration type 1
PCI: Probing PCI hardware
PCI: Probing PCI hardware (bus 00)
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
Starting kswapd
JFFS2 version 2.1. (C) 2001 Red Hat, Inc., designed by Axis Communications AB.
Serial driver version 5.05c (2001-07-08) with MANY_PORTS SHARE_IRQ SERIAL_PCI enabled
ttyS00 at 0x03f8 (irq = 4) is a 16550A
ttyS01 at 0x02f8 (irq = 3) is a 16550A
ttyS02 at 0x03e8 (irq = 0) is a ST16654
ttyS03 at 0x02e8 (irq = 3) is a ST16654
sc520_wdt: CBAR: 0x800df000
sc520_wdt: MMCR Aliasing enabled.
sc520_wdt: WDT driver for SC520 initialised.
RAMDISK driver initialized: 16 RAM disks of 16384K size 1024 blocksize
pcnet32.c:v1.28 02.20.2004 tsbogend@alpha.franken.de
PCI: Enabling device 00:0d.0 (0000 -> 0003)
pcnet32: PCnet/FAST III 79C973 at 0x1000, 00 0e fe 00 00 33
    tx_start_pt(0x0c00):~220 bytes, BCR18(9a61):BurstWrEn BurstRdEn NoUFlow
    SRAMSIZE=0x1700, SRAM_BND=0x0800, assigned IRQ 12.
eth0: registered as PCnet/FAST III 79C973
pcnet32: 1 cards_found.
Tempus SC520 flash device: 1000000 at 2000000
 Amd/Fujitsu Extended Query Table v1.3 at 0x0040
number of CFI chips: 1
Creating 7 MTD partitions on "Tempus SC520 Flash Bank":
0x00000000-0x000e0000 : "Tempus kernel"
mtd: Giving out device 0 to Tempus kernel
0x000e0000-0x00100000 : "Tempus Lo BootLdr"
mtd: Giving out device 1 to Tempus Lo BootLdr
0x00100000-0x00200000 : "Tempus /boot"
mtd: Giving out device 2 to Tempus /boot
0x00200000-0x00300000 : "Tempus /logs"
mtd: Giving out device 3 to Tempus /logs
0x00300000-0x00900000 : "Tempus FACTORY rootfs"
mtd: Giving out device 4 to Tempus FACTORY rootfs
0x00900000-0x00fe0000 : "Tempus UPGRADE rootfs"
mtd: Giving out device 5 to Tempus UPGRADE rootfs
0x00fe0000-0x01000000 : "Tempus Hi BootLdr"
mtd: Giving out device 6 to Tempus Hi BootLdr
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP, IGMP
```

```
IP: routing cache hash table of 512 buckets, 4Kbytes
TCP: Hash tables configured (established 2048 bind 2048)
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
mtdblock_open
ok
RAMDISK: Compressed image found at block 0
mtdblock_release
ok
VFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 68k freed
INIT: version 2.76 booting
/etc/rc.d/rc.S: /bin: is a directory
mtdblock_open
ok
mtdblock_open
ok
Loading GPS
Fri Aug 20 00:53:54 2004 -0.707128 seconds
2004
Setting system time using hwclock
INIT: Entering runlevel: 3
Entering multiuser...
Attempting to configure eth0 by contacting a DHCP server...
```

At this point, if you do not have a DHCP server configured on your network the unit will time-out and print these messages:

```
Unison GPS DHCP Client was unable to find the DHCP Server!
Fix the problem and reboot or set up static IP address
by running netconfig.
dnsdomainname: Host name lookup failure
(none)
```

Then these messages are printed, in either case:

```
Disabling IPv4 packet forwarding...
Starting daemons:  syslogd klogd inetd
Starting the Network Time Protocol daemon...
Starting the SNMP daemon...
Starting the system logfile manager...
Starting the system watchdog...woof!
```

During this process, the factory default UnisonGPS_0 root file system is loaded from FLASH disk to an 16MB ramdisk and the remainder of the boot process completes. At this point, the Unison login prompt is displayed:

```
*******************************************************************************
*           Welcome to Unison GPS console on:  gntp.your.domain
*           Tue Feb 20  2001 21:47:03 UTC
*******************************************************************************

gntp login:
```

Here you may log in as “gntpuser” with password “Praecis” or you may log in as the “root” user with password “endrun_1”. When logged in as “gntpuser”, 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 Unison GPS and shows the software part number, version and build date:

```
Unison GPS 6010-0042-000 v 1.00 Wed May  9 14:17:44 UTC 2002
Unison GPS (root@gntp:~)->
```

This last line is the standard Unison GPS shell prompt. The Unison uses the **bash** shell, which is the Linux standard, full-featured shell. After configuring the unit, you should change the passwords using the **gntppasswd** command issued from the shell 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 ***Chapter 5 - RS-232 Serial I/O Port Signal Definitions*** for the signal connections for the Unison.

NOTE

You must use a null-modem cable or adapter if you are connecting the Unison to another computer or other equipment configured as Data Terminal Equipment (DTE). The supplied cable is a null-modem cable.

Once you have successfully established communications with the Unison, you may procede to configuring the network parameters. Then you can communicate with the Unison 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 Unison. If you want to have the HTTP Interface enabled in your Unison then be sure to configure the name server IP address during the **netconfig** process. The HTTP Interface will not start if this is configured incorrectly. Only one name server is required, two gives some redundancy.

The following is a sample transcript which illustrates the use of **netconfig**. The entries made by the user are underlined and are provided purely for illustrative purposes. You must provide equivalent entries that are specific to your network. Those shown here are appropriate for a typical network that does not use DHCP. Start the configuration process by typing **netconfig** at the shell prompt:

```
Unison GPS(root@gntp)-> netconfig
*******************************************************************************
****************** Unison GPS Network Configuration  ***********************
*******************************************************************************
*                                                                             *
*   This script will configure the TCP/IP network parameters for your         *
*   Unison GPS. 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 restart your     *
*   Unison GPS, so if you make a mistake, just re-run this script before      *
*   rebooting.                                                               *
*                                                                             *
*   You will be prompted to enter your network parameters now.                *
*                                                                             *
*******************************************************************************
*******************************************************************************

---DHCP Settings
Use a DHCP server to configure the ethernet interface? ([y]es, [n]o) n

---HOST name setting

Set the hostname of your Unison GPS. Only the base
hostname is needed, not the domain.
Enter hostname: gntp

---DOMAIN name setting

Set the domain name. Do not supply a leading '.'
Enter domain name for gntp: your.domain

---STATIC IP ADDRESS setting

Set the IP address for the Unison GPS. Example: 111.112.113.114
Enter IP address for gntp (aaa.bbb.ccc.ddd): 192.168.1.245

---DEFAULT GATEWAY ADDRESS setting

Set the default gateway address, such as 111.112.113.1
If you don't have a gateway, just hit ENTER to continue.
Enter default gateway address (aaa.bbb.ccc.ddd): 192.168.1.241

---NETMASK setting

Set the netmask. This will look something like this: 255.255.255.0
Enter netmask (aaa.bbb.ccc.ddd): 255.255.255.248

Calculating the BROADCAST and NETWORK addresses...
Broadcast = 192.168.1.247     Network = 192.168.1.240

Your Unison GPS's current IP address, full hostname, and base hostname:
192.168.1.245       gntp.your.domain    gntp

---DOMAIN NAMESERVER(S) address setting

Will your Unison GPS be accessing a nameserver ([y]es, [n]o)? y

Set the IP address of the primary name server to use for domain your.domain.
Enter primary name server IP address (aaa.bbb.ccc.ddd): 192.168.1.1

Will your Unison GPS be accessing a secondary nameserver ([y]es, [n]o)? y

Set the IP address of the secondary name server to use for domain your.domain.
Enter secondary name server IP address (aaa.bbb.ccc.ddd): 192.168.1.2

Setting up TCP/IP...
Creating /etc/HOSTNAME...
Creating /etc/rc.d/rc.inet1...
Creating /etc/networks...
Creating /etc/hosts...
Creating /etc/resolv.conf...
```

```
*******************************************************************************
*******************************************************************************
*                                                                             *
*          The Unison GPS network configuration has been updated.             *
*                                                                             *
*             Please reboot now for the changes to take effect.              *
*                                                                             *
*******************************************************************************
*******************************************************************************
```

Verify Network Configuration

If you have made changes to your network configuration using **`netconfig`**, you should shutdown the Unison and reboot it. There are two ways to do this:

1. Cycle power to the Unison.

2. Issue the shutdown with reboot command at the shell prompt:

```
Unison GPS(root@gntp:~)-> shutdown -r now
```

If you are using the RS-232 serial I/O port to communicate with the Unison, you will be able to see the kernel generated boot messages when the unit reboots. You should note the line

```
Configuring eth0 as 192.168.1.245...
```

if you have set up a static IP address, or this line

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

if you are using DHCP. It appears 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 Unison 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 Unison 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`**:

```
Unison GPS(root@gntp:~)-> ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0E:FE:00:00:34
          inet addr: 192.168.1.245 Bcast:192.168.1.247 Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3779 errors:0 dropped:0 overruns:0 frame:0
          TX packets:727 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0x300

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:170 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

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

```
Unison GPS(root@gntp:~)-> route

Kernel IP routing table
Destination     Gateway         Genmask           Flags Metric Ref Use Iface
localnet        *               255.255.255.248   U     0      0   0   eth0
loopback        *               255.0.0.0         U     0      0   0   lo
default         192.168.1.241   0.0.0.0           UG    1      0   0   eth0
```

Here you are interested in the default gateway address. It should match the appropriate one for your network. If so, then the ethernet interface of your Unison has been successfully configured to operate on your network and you are ready to check operation of the Unison 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 shell command:

```
Unison GPS(root@gntp:~)-> 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 your domain name and the nameserver IP address(es) to use for that domain.

Check Network Operation

With your Unison 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 Unison. Alternatively, you could **ping** one of your servers or workstations from the Unison shell prompt to test the setup.

Once you have successfully established network communications with the Unison, you may perform all maintenance and monitoring activities via **telnet** and **ftp**. The Unison provides both client and server operation using **telnet**. For security reasons as well as to reduce the memory footprint in the Unison, only client operation is supported using **ftp**. You may also monitor the Unison via the HTTP interface (see ***Chapter 7 - HTTP Interface***).

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 Unison. Both of these protocols are supported in the Unison via the OpenSSH implementations for Linux. Refer to ***Appendix A - Security*** for more information about the secure shell protocol.

Using Telnet

When establishing a **telnet** connection with your Unison, 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 Unison, this banner will be displayed:

```
*******************************************************************************
*           Welcome to Unison GPS telnet console on:  gntp.your.domain
*******************************************************************************

gntp login:
```

Here you may log in as “gntpuser” with password “Praecis”. When logged in as “gntpuser”, 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 Unison GPS and shows the software part number, version and build date:

```
Unison GPS 6010-0004-000 v 1.00 Wed May 16 14:17:44 UTC 2002
Unison GPS(root@gntp:~)->
```

This last line is the standard Unison GPS shell prompt. The Unison uses the **bash** shell, which is the Linux standard, full-featured shell. After configuring the unit, you should change the passwords using the **gntppasswd** command issued from the shell prompt.

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

```
Unison GPS(root@gntp:~)-> 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 shell command **exit**. Issuing **exit** again will close the **telnet** session.

Using SSH

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

```
*******************************************************************************
*             Welcome to Unison GPS SSH console on:  gntp.your.domain
*******************************************************************************

root@gntp.your.domain'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 Unison and shows the software part number, version and build date:

```
Unison GPS 6010-0042-000 v 1.00 Fri Aug 20 14:17:44 UTC 2004
Unison GPS(root@gntp:~)->
```

This last line is the standard Unison GPS shell prompt. The Unison uses the **bash** shell, which is the Linux standard, full-featured shell. After configuring the unit, you should change the passwords using the **gntppasswd** command issued from the shell prompt.

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

Using HTTP

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

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 `gntppasswd` command. To change the passwords/community strings for SNMP see ***Appendix C - SNMP***.

To disable Telnet use the `inetdconfig` command. To disable SSH, SNMP and HTTP see ***Appendix A - Security***, ***Disabling Protocols***.

Configuring the Network Time Protocol

Now that the network has been configured and tested, you may configure the operation of the NTP server. By default, the Unison 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 Unison. If you need to modify the factory default Unison 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 multicast address: 224.0.1.1, when you are prompted to enter the broadcast address.

Configuring NTP Using the Network Interface or Serial Port

The following is a transcript of the question and answer configuration utility provided by **`ntpconfig`**. The user entered parameters are underlined:

```
Unison GPS(root@gntp:~)-> ntpconfig

*******************************************************************************
*********************Network Time Protocol Configuration***********************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure the ntp.conf and ntp.keys files   *
*   that control Unison 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 reboot the       *
*   Unison GPS.  If you make a mistake, just re-run ntpconfig prior to        *
*   rebooting.                                                               *
*                                                                             *
*   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
SPACE, TAB, LF, NULL, or # characters!

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

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

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

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

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

Writing key number: 2 and Key: Tempus_GPS 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 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 Unison GPS.  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 Unison GPS to use.  For
broadcast mode, this address is the all 1's address on the sub-net.
Example: 111.112.113.255
For multicast operation, it is this specific address:  224.0.1.1

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

You have selected multicast operation.  Enter the number of hops that
are needed for the multicast packets on your network (positive integer): 1

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 Unison GPS 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 mode? ([y]es, [n]o) y

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

*******************************************************************************
*******************************************************************************
*                                                                             *
*    The Unison GPS Network Time Protocol configuration has been updated.     *
*                                                                             *
*              Please reboot now for the changes to take effect.             *
*                                                                             *
*******************************************************************************
*******************************************************************************
```

Configuring the Unison as a Stratum 2 Server

Operating the Unison as a Stratum 1 Server is the recommended mode. You may operate the unit as a Stratum 2 server but 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 are:

Edit NTP.CONF

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 ***Using Edit*** below.) Here is an example:

```
server 192.168.1.1
```

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

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

IMPORTANT

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

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

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

Mask Alarm

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

Using Edit

A very compact editor is available on the system for editing files: **`edit`**. If you start **`edit`** without giving it a file name to open, it will display its help screen, showing all supported keystrokes.

Chapter *Three*

Setting Up NTP Clients on Unix-like Platforms

To configure your Unix-like computer to use your Unison, you must have successfully completed the Basic Installation procedures in Chapter 2. This manual is not a 'How-To' on installing and using NTP; basic approaches to NTP client configuration for operation with the Unison will be described. 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 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

If you have a 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 Unison 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 Unison 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.

Basic NTP Client Setup

Basic setup is relatively simple, if:

- You have been able to successfully communicate with the Unison 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 192.168.1.245
```

This line tells **ntpd** to use the NTP server at address 192.168.1.245 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 Unison server. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Unison. 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 Unison 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 Unison 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.

MD5 Authenticated NTP Client Setup

MD5 authenticated setup is relatively simple, if:

- You have been able to successfully communicate with the Unison on your network.
- Your Unison has been configured to perform authentication either by factory default, or by running the **ntpconfig** shell script. The example Unison authentication configuration shown in ***Chapter 2 - Configuring the Network Time Protocol*** will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.
- You have successfully performed the ***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 Unison. You can **telnet** into your Unison and start an **ftp** session with your client computer to send the Unison'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 the example in the previous chapter, add these lines to the end of the *ntp.conf* file:

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

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

```
server 192.168.1.245 key 1
```

Restart **ntpd** to have it begin using the Unison server with MD5 authentication. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Unison. 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 Unison 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 Unison 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.

Broadcast/Multicast NTP Client Setup

Broadcast/multicast client setup is relatively simple, if:

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

- Your Unison 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 Unison 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 Unison configuration shown in ***Chapter 2 - Configuring the Network Time Protocol*** will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.

- You have successfully performed the ***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 Unison server has been configured to use key 2 for broadcast authentication as shown in the example in chapter 2, 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 ***Basic NTP Client Setup***:

```
server 192.168.1.245
```

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

```
server 192.168.1.245 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 ***Basic NTP Client Setup***:

```
server 192.168.1.245
```

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

```
server 192.168.1.245 key 1
```

Test Broadcast/Multicast

Restart **ntpd** to have it begin using the Unison as a broadcast or multicast server. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Unison. 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 Unison 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 Unison 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.

Chapter *Four*

Setting Up NTP Clients on Windows NT 4.0/2000/XP

To configure your Windows NT 4.0/2000/XP computer to use your Unison, you must have successfully completed the Basic Installation procedures in Chapter 2. This manual is not a 'How-To' on installing and using NTP; basic approaches to NTP configuration for operation with the Unison will be described here. Installation must be performed by a user with administrative priviledges on the system. If you have never used NTP, then you should spend some time reading the on-line documents at: http://www.ntp.org.

If you have a 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 Unison with NTP clients on Window NT 4.0 platforms will be described:

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

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 Unison 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 *\winnt\system32\drivers\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.

Basic NTP Client Setup

Basic setup is relatively simple, if:

- You have been able to successfully communicate with the Unison on your network.
- You have installed NTP on your client computer.

Configure NTP

You must edit the *ntp.conf* file which **ntpd.exe**, the NTP daemon, looks for by default in the the *\winnt\system32\drivers\etc* directory of the boot partition. If your NTP installation placed this file in a different place, you must find it and edit it. For example, XP uses *\windows\system32\drivers\etc*. Add this line to the *ntp.conf* file:

```
server 192.168.1.245
```

This line tells **ntpd.exe** to use the NTP server at address 192.168.1.245 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 Unison 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 Unison. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT/2000/XP partition. 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 Unison 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 Unison 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. The debug version of the NTP daemon is located in the *debug* sub-directory of your NTP directory. Refer to the NTP documentation for detailed usage of these debug utilities.

MD5 Authenticated NTP Client Setup

MD5 authenticated setup is relatively simple, if:

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

- Your Unison has been configured to perform authentication either by factory default, or by running the **ntpconfig** shell script. The example Unison authentication configuration shown in ***Chapter 2 - Configuring the Network Time Protocol*** will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.

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

Create the ntp.keys File

You must create a file named *ntp.keys* in the *\winnt\system32\drivers\etc* directory or, for XP, the *\windows\system32\drivers\etc* directory. It must be a copy of the one residing in the */etc* directory of your Unison. You can **telnet** into your Unison and start an **ftp** session with your client computer to send the Unison */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 Unison 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 ***\windows\system32\drivers\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

You must edit the *ntp.conf* file which **ntpd.exe**, the NTP daemon, looks for by default in the the *\winnt\system32\drivers\etc* directory. If your NTP installation placed this file in a different place, you must find it and edit it. For example, XP uses *\windows\system32\drivers\etc*. Add these lines to the end of the *ntp.conf* file:

```
keys \winnt\system32\drivers\etc\ntp.keys
trustedkey 1 2
```

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

```
server 192.168.1.245 key 1
```

Restart **ntpd.exe** to have it begin using the Unison 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 Unison. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT/2000/XP partition. 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 Unison 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 Unison 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 *\winnt\system32\drivers\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 *\winnt\system32\drivers\etc\ntp.conf* file that causes the needed key to not be included in the "trustedkey" list.

Broadcast/Multicast NTP Client Setup

Broadcast/multicast client setup is relatively simple, if:

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

- Your Unison 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 Unison 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 Unison configuration shown in ***Chapter 2 - Configuring the Network Time Protocol*** will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.

- You have successfully performed the ***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.exe**, the NTP daemon, looks for by default in the the \ *winnt\system32\drivers\etc* directory or, for XP, the *windows\system32\drivers\etc* directory. Assuming that your Unison server has been configured to use key 2 for broadcast authentication as shown in the example in chapter 2, 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 ***Basic NTP Client Setup***:

```
server 192.168.1.245
```

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

```
server 192.168.1.245 key 1
```

Configure NTP Client for Multicast

You must edit the *ntp.conf* file which **ntpd.exe**, the NTP daemon, looks for by default in the the \ *winnt\system32\drivers\etc* directory or, for XP, the *windows\system32\drivers\etc* directory. Assuming that your Unison server has been configured to use key 2 for broadcast authentication as shown in the example in chapter 2, 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 ***Basic NTP Client Setup***:

```
server 192.168.1.245
```

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

```
server 192.168.1.245 key 1
```

Test Broadcast/Multicast

Restart **ntpd.exe** to have it begin using the Unison 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 Unison. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT/2000/XP partition. 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 Unison 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 Unison 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 *\windows\system32\drivers\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 *\windows\system32\drivers\etc\ntp.conf* file that causes the needed key to not be included in the "trustedkey" list.

Chapter*Five*

Control and Status Commands

This chapter describes the Unison control and status commands. The Unison supports several application-specific commands for performing initialization/setup and for monitoring the performance and status of the Linux/NTP and GPS Subsystems. You do not need knowledge of Linux commands in order to operate the Unison. However, the Unison does support a subset of the standard Linux shell commands and utilities. A wealth of information is available from a variety of sources on Linux. Only the Unison-specific commands will be described in this chapter. The serial I/O port physical and electrical characteristics are defined as well.

General Linux Shell Operation

You do not need to know Linux in order to operate the Unison. However, for those interested, the command shell used by the Unison is the Linux standard: **`bash`**. All commands and file names are case sensitive, which is standard for Unix-like operating systems. 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 Unison you should consult good Linux reference books like:

Linux in a Nutshell, Seiver, O'Reilly & Associates, 1999.

Running Linux, Welsh, Dalheimer & Kaufman, O'Reilly & Associates, 1999

Or the web at:

http://www.tldp.org

Available User Commands

COMMAND	FUNCTION
accessconfig	Interactive shell script that guides the user in configuring **`telnet, ssh`** and **`snmpd`** access to the Unison that is limited to specific hosts. The resulting */etc/hosts.allow* and */etc/hosts.deny* files are saved to the non-volatile FLASH disk. Factory default configuration allows access by all hosts.
antfltmask	Prints the current settings for the Antenna Fault Mask.
cpuopts	Returns the current settings for any installed, user-selectable, CPU Options. These are: 1PPS, AM Code or Prog TTL.
cpuoptsconfig	An interactive script that allows the user to modify the settings for the CPU Options listed above.
cpusertime	Prints the current settings for the optional Serial Time output.
cpusertimeconfig	An interactive script that allows the user to modify the settings for the optional Serial Time output.
eraserootfs_1	Command to erase the UPGRADE root file system FLASH partition. This must be executed prior to loading the new file system image during the Linux/NTP upgrade process.
gpsdynmode	Prints the GPS dynamic mode currently in effect to the console.
gpsrefpos	Prints the GPS reference position to the console.
gpsstat	Prints the GPS Subsystem status information to the console.
gpstrkstat	Prints the GPS satellite tracking status to the console.
gpsversion	Prints the GPS firmware and FPGA version information to the console.
gntphwaddr	Prints the ethernet hardware address, if the ethernet has been configured.
gntposctype	Prints the installed oscillator type, which is TCXO or MS-OCXO.
gntppasswd	Allows the *root* user to change the password for the two configured users on the Unison: *gntpuser* and *root*. This script calls the standard Linux **`passwd`** binary and then saves the resulting */etc/shadow* file to the non-volatile FLASH disk.
gntprootfs	Prints the current root file system image, either UnisonGPS_0 (factory default) or UnisonGPS_1 (field upgrade) which is running in the Unison to the console.
gntpstat	Parses the output of **`ntpq -c peers`** to obtain the system peer status of the NTP GPS reference clock. It also retrieves the current reference clock polling status data and prints it to the console.
gntptimemode	Prints the time mode settings in effect for any optional AM Code Output (time code) or optional Serial Time Output.

gntptimemodeconfig	Interactive shell script that guides the user in configuring the time mode settings for any optional AM Code Output (time code) or Serial Time Output. Allows setting to the LOCAL, GPS or UTC timescale and if LOCAL, the setting of the offset to UTC and the Daylight Savings Time (DST) start and stop date/time parameters.
gntpversion	Prints the Linux/NTP Subsystem software version information to the console.
gptpstat *(optional)*	Prints the status of the optional PTP/IEEE-1588 subsystem.
help	Prints help for Unison commands (not Linux).
inetdconfig	Interactive shell script that allows the user to configure the list of protocol servers which are started by the **`inetd`** server daemon running in the Unison.
netconfig	Interactive shell script that allows the user to configure the IP network subsystem of the Unison.
ntpconfig	Interactive shell script that guides the user in configuring the Unison NTP subsystem. Allows configuration of MD5 authentication and broadcast/multicast mode. All parameters are retained in non-volatile FLASH disk storage.
ptpconfig ptp2config *(optional)*	Interactive shell script that guides the user in configuring parameters for the optional PTP/IEEE-1588 protocol.
ptpversionconfig *(optional)*	Interactive shell script that guides the user in selecting either PTP/IEEE-1588 version 1 or version 2.
setantfltmask	Command to enable or mask the Antenna Fault.
setgpsdynmode	Allows the user to set the dynamic mode of operation of the GPS Subsystem. It may be ON or OFF.
setgpsrefpos	Interactive shell script that prompts the user for an accurate reference position, performs syntax and argument validity checking then passes the position to the GPS Subsystem.
setsigfltmask	Command to mask or enable the Signal Loss Fault.
sigfltmask	Prints the current setting for the Signal Loss Fault mask.
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 or UPGRADE root file system.
upgradegps	Shell script that facilitates the GPS Subsystem firmware upgrade process.
upgradekernel	Shell script that facilitates the Linux kernel firmware upgrade process. Limited applicability. Use with caution.

Detailed Command Descriptions

accessconfig

This command starts an interactive shell script that will allow the root user to configure limitation of **telnet**, **ssh** and **snmp** access to the Unison. 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 Unison after running this script for the changes to take effect.

Set:	**accessconfig**
Unison response:	Interactive shell script is started.

antfltmask

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

Query:	**antfltmask**
Unison response:	**Antenna Fault is ENABLED**

cpuopts

This command displays the current settings for the installed CPU Options.

Query:	**cpuopts**
Unison response:	**CPU Option TIME CODE is installed.** **Current Setting = IRIG-B122.**

cpuoptsconfig

This command starts an interactive shell script that will allow the root user to change the settings of any installed CPU Options. The user-selectable options are: 1PPS, AM Code, and Prog TTL.

Set:	**cpuoptsconfig**
Unison response:	Interactive shell script is started.

cpusertime

This command displays the current settings for the optional Serial Time Output. Settings for the three NMEA Sentences are always shown but are only applicable if you have selected NMEA as the Output Format Setting. More information about the various formats is in ***Appendix G - Serial Time Output***.

Query:	**cpusertime**
Unison response:	**Current Serial Time Output Baud Rate Setting = 9600** **Current Serial Time Output Format Setting = Sysplex** **Current Serial Time Output Parity Setting = Odd** **Current NMEA Sentence 1 Setting - ZDA** **Current NMEA Sentence 2 Setting - NONE** **Current NMEA Sentence 3 Setting - NONE**

cpusertimeconfig

This command starts an interactive shell script that will allow the root user to change the settings of the optional Serial Time Output. The user-selectable outputs are the format (Sysplex, Truetime, EndRun, EndRunX, NENA0, NENA1, NENA8 and NMEA), the baud rate (4800, 9600, 19200, 57600) and the parity (ODD, EVEN, or NONE). The three NMEA sentences can also be changed but are applicable only if the Output Format is NMEA. More information about the various formats is in ***Appendix G - Serial Time Output***.

Set:	**cpusertimeconfig**
Unison response:	Interactive shell script is started.

eraserootfs_1

This command erases the UPGRADE root file system FLASH partition in preparation for performing a Linux/NTP Subsystem firmware upgrade. See ***Appendix B - Upgrading the Firmware*** for more information.

Set:	**eraserootfs_1**
Unison response:	Erase progress as percent is shown.

gpsdynmode

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

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

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

Query:	**gpsdynmode**
Unison response:	**OFF**

gpsrefpos

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

Query:	**gpsrefpos**
Unison response:	

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

gpsstat

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

```
LKSTAT TFOM = ? YEAR DOY HH:MM:SS.sssssssss LS LF S N VCDAC C/No FLTS
```

Where:

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

TFOM = ? A detailed explanation of TFOM is in ***Appendix E - Time Figure-of-Merit***.
Briefly, TFOM indicates clock accuracy where:

3	time error is < 100 ns
4	time error is < 1 us
5	time error is < 10 us
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 GPS.

YEAR is the year of the UTC timestamp of the most recent NTP polling request received by the GPS 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 GPS Subsystem from the NTP reference clock driver.

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

LS is the current number of leap seconds difference between the UTC and GPS timescales (13 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 (13 at the time of this writing).

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

N is the number of GPS satellites being tracked, 0 to 8.

VCDAC is the upper 16 bits of the oscillator Voltage Control DAC word, 0 to 65535 with larger numbers implying higher oscillator frequency. Typical range is 20000 to 38000.

C/No is the Carrier Signal-To-Noise Ratio, 0.00 to 99.9, measured in dB in the GPS data rate bandwidth. Typical range is 30 to 45.

FLTS is the fault status, which displays the current summary status of the GPS Subsystem. The summary status is contained in sixteen bits which are displayed in four

hexadecimal characters. Assertion of any of these bits will also be indicated by illumination of the red LED. Each bit of each character indicates the status of a subsystem component:

	Bit 3	Bit 2	Bit 1	Bit 0
Char 0	FLASH Write Fault	FPGA Config Fault	No Signal Time-Out	DAC Control Over-Range
Char 1	Antenna Fault	No Polling Events	Time Input Fault	GPS Comm Fault
Char 2	Not Used	Not Used	Not Used	Not Used
Char 3	Not Used	Not Used	Not Used	Not Used

DAC Control Over-Range: This bit indicates that the electronic frequency control DAC for the oscillator has reached either the high (55000) or low (10000) limit while locked to the GPS signal. Unless the unit is being subjected to out-of-specification environmental conditions, this would indicate that the oscillator frequency has drifted near to the end of life region. This should normally only occur after about ten years of operation. The unit will continue to function until the oscillator frequency finally reaches one of the actual DAC endpoints. The unit should be returned to the factory for oscillator replacement at the customer's convenience.

No Signal Time-Out: This bit indicates that the unit has not been able to acquire a GPS signal for one hour while the Time Figure of Merit has been 9, the unsynchronized condition. This could be due to a variety of reasons. If there are no other faults that could explain the inability to receive a signal, then there could be an or antenna failure or blockage. If the condition persists indefinitely, and a problem with the antenna is not evident, the unit may need to be returned to the factory for repair.

FPGA Config Fault: This bit indicates that the microprocessor was unable to configure the FPGA. This would be a fatal fault and the unit should be returned to the factory for repair .

FLASH Write Fault: This bit indicates that the microprocessor was unable to verify a write to the FLASH non-volatile parameter storage area. This should not ever occur under normal operation. The unit should be returned to the factory for repair.

GPS Comm Fault: This bit indicates that the microprocessor is unable to establish communications with the GPS Subsystem. Please report this fault condition to the factory (1-877-749-3878).

Time Input Fault: This bit indicates that the microprocessor received an erroneous time input from the GPS Subsystem. If the condition persists please report it to the factory (1-877-749-3878).

No Polling Events: This bit indicates that the GPS Subsystem is not receiving polling request from the Linux Subsystem. This could be due to a hardware or software failure. If the condition persists after cycling the power to the unit, this is a fatal fault and the unit should be returned to the factory for repair.

Antenna Fault: This bit indicates that the GPS antenna or downlead cable has a fault. It indicates either an over or under current condition. Usually it means that the antenna downlead cable is not plugged into the connector on the rear of the Unison. If the condition persists after checking the antenna/downlead for obvious faults, this is a fatal fault and the unit should be returned to the

factory for repair.

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

Query: **gpsstat**
Unison response:
LOCKED TFOM = 4 2001 092 04:48:56.347916732 13 13 2 7 28605 41.6 008A

gpstrkstat

This command displays the current GPS Subsystem satellite tracking status. A list of eight satellite numbers is displayed, one for each receiver channel. Satellite number 0 is an invalid number and indicates that no satellite is being tracked on that channel. Valid satellite numbers range from 1 to 32.

Query: **gpstrkstat**
Unison response: **CURRENT SVs TRKD = 08 11 13 22 31 00 00 00**

gpsversion

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

Query: **gpsversion**
Unison response: **F/W 1.00 FPGA 0202**

gntphwaddr

This command displays the ethernet hardware address, if the IP network is properly configured. Otherwise it returns nothing.

Query: **gntphwaddr**
Unison response: **00:D0:C9:25:78:59**

gntposctype

This command displays the installed oscillator type. It is TCXO or MS-OCXO. The standard oscillator is the TCXO.

Query: **gntposctype**
Unison response: **Installed Oscillator is TCXO.**

gntppasswd

This command allows the root user to change the passwords of the two configured users on the system: *root* and *gntpuser*. Arguments passed to **gntppasswd** on the command line are passed verbatim to the real **passwd** binary program. When **passwd** returns, the resulting modified */etc/shadow* file is copied to the non-volatile */boot/etc* directory.

To change root password:
Set: **cntppasswd**
Unison response: The passwd interactive utility starts.

To change cntpuser password:
Set: **cntppasswd cntpuser**
Unison response: The passwd interactive utility starts.

gntprootfs

This command displays the currently booted root file system image. It can be either UnisonGPS_0 (factory image) or UnisonGPS_1 (field upgrade image). Refer to ***Appendix B - Upgrading the Firmware*** for detailed instructions on performing the upgrade procedure.

Query:	**gntprootfs**
Unison response:	**BOOT_IMAGE=UnisonGPS_1**

gntpstat

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

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

Where:

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

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

TFOM = ? A detailed explanation of TFOM is in ***Appendix E - Time Figure-of-Merit***. Briefly, TFOM indicates clock accuracy where:

- 3 time error is < 100 ns
- 4 time error is < 1 us
- 5 time error is < 10 us
- 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 GPS.

YEAR is the year of the UTC timestamp of most recent NTP polling request received by the GPS 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 GPS Subsystem from the NTP reference clock driver.

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

LS is the current number of leap seconds difference between the UTC and GPS timescales (13 at the time of this writing).

Query: **gntpstat**
Unison response:
LOCKED TO GPS, Offset = +0.000024, TFOM = 4 @ 2001 092 06:03:10.904312858 13

gntptimemode

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

Query: **gntptimemode**
Unison response:
Time Mode = LOCAL
Local Time Offset from UTC = -16 (half hours)
DST Start Month = Apr Sunday = 1st Hour = 02
DST Stop Month = Oct Sunday = Last Hour = 02

gntptimemodeconfig

This command starts an interactive shell script that will allow the user to configure the time mode of of any optional AM Code Output (time code) or Serial Time Output. Possible time modes are UTC, GPS, and LOCAL. *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 with an offset to UTC of zero and with Daylight Savings Time disabled. If you need to modify this operation, you must run this script as root. Settings made using this command are non-volatile.

Set: **gntptimemodeconfig**
Unison response: Interactive shell script is started.

gntpversion

This command displays the firmware version and build date of the Linux/NTP Subsystem (root file system).

Query: **gntpversion**
Unison response:
Unison GPS 6010-0042-000 v 1.00 Wed Jan 16 22:38:21 UTC 2004

gptpstat (Optional)

This command is only available if the PTP/IEEE-1588 option has been installed. Refer to ***Appendix H - Precision Time Protocol/IEEE-1588*** for more information.

help

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

Query:	**`help`**
Unison response:	Tempux LX commands are displayed.

Query:	**`help gpsstat`**
Unison response:	Information specific to the **`gpsstat`** command is displayed.

inetdconfig

This command starts an interactive shell script that will allow the user to configure the list of protocol servers which are started by the **`inetd`** server daemon running in the Unison. 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 Unison after running this script for the changes to take effect.

Set:	**`inetdconfig`**
Unison response:	Interactive shell script is started.

netconfig

This command starts an interactive shell script that will allow the user to configure the IP network subsystem of the Unison. 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 - 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*. All of these are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot the Unison after running this script for the changes to take effect.

Set:	**`netconfig`**
Unison response:	Interactive shell script is started.

ntpconfig

This command starts an interactive shell script that will allow the user to configure the NTP subsystem of the Unison. 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 2 - Configuring the Network Time Protocol*** 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 Unison after running this script for the changes to take effect.

Set:	**ntpconfig**
Unison response:	Interactive shell script is started.

ptpconfig and ptp2config (Optional)

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

ptpversionconfig (Optional)

This command is only available if the PTP/IEEE-1588 option has been installed. Refer to ***Appendix H - Precision Time Protocol/IEEE-1588*** for more information.

setantfltmask

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

Set:	**antfltmask MASKED**
Unison response:	**Antenna Fault Mask set to MASKED**

setgpsdynmode

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

Set:	**setgpsdynmode ON**
Unison response:	**GPS Dynamic Mode is ON.**

setgpsrefpos

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

In addition to setting a new accurate, reference position, the user can also invalidate an existing one. This will force the Unison to re-establish a new reference position using the GPS satellite constellation.

Set:	**setgpsrefpos**
Unison response:	Interactive shell script is started.

setsigfltmask

This command allows the user 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.

Set:	**sigfltmask MASKED**
Unison response:	**Signal Loss Fault Mask set to MASKED**

sigfltmask

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

Query:	**sigfltmask**
Unison response:	**Signal Loss Fault is ENABLED**

updaterootflag

This command allows the user to update the configuration of the Linux bootloader after a new root file system image has been uploaded to the UPGRADE root file system partition, */dev/rootfs_1* of the Unison FLASH disk. It may also be used 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, causing a flag to be set that will indicate 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.

Set:	**updaterootflag 1**
Unison response:	**UPGRADE is the default root file system.**
Query:	**updaterootflag 2**
Unison response:	**UPGRADE is the default root file system.**

upgradegps

This script allows the user to upgrade the GPS Subsystem firmware. It requires one argument: the path to the binary file to be uploaded to the GPS Subsystem. It issues the commands over the serial port to the GPS Subsystem that are needed to start the X-modem file transfer, and then displays the responses from the GPS Subsystem to the console. When the X-modem 'C' character appears, indicating that the GPS Subsystem is ready to receive the file, you must hit the <ENTER> key, and the transfer will begin. After about one minute, it should complete, at which point you should see the GPS Subsystem boot messages appear on the console. From these, you will be able to verify that the firmware was successfully upgraded.

In the example console output below, lines which begin with "---" are generated by the **upgradegps** script. All other lines are from the GPS Subsystem, with the exception of the shell message indicating that the process **cat < /dev/arm_user** has been terminated, which is normal. In this example, the 'C' character was received three times before the user hit the <ENTER> key to begin the transfer. The last three lines are the boot messages that are sent by the GPS Subsystem as it comes up. The firmware version should match that of the binary file that was uploaded. See ***Performing the GPS Upgrade*** in ***Appendix B - Upgrading the Firmware*** for more information.

Set: **upgradegps /tmp/6010-0020-000.bin**

Unison response:

```
---When you see the `C` character, hit <enter> to begin the upload.

Waiting for download using XMODEM 128 or XMODEM 1K (both with CRC).
Control X will abort download.
CCC
---Starting file upload, should take about 90 seconds...

/sbin/upgradegps: line 26: 27618 Terminated            cat </dev/arm_user

---You should see the GPS subsystem startup message now.  If not, you
---may need to check your binary file and re-perform the procedure.

Tempus Bootloader 6010-0050-000 v 1.00 - May 28 2004 17:31:05
FW 6010-0020-000 v 1.00 - Aug 18 2004 10:47:41
FPGA 6020-0005-000 v 0202
```

upgradekernel

This script allows the user to change the Linux kernel firmware. It requires one argument: the path to the file to be uploaded to the Unison. Changing the Linux kernel firmware will enable IPv6 operation and should only be done if you have a requirement for IPv6. See ***Chapter 6 - IPv6 Information*** and ***Performing the Linux Kernel Upgrade*** in ***Appendix B - Upgrading the Firmware*** for more information.

Set **upgradekernel /tmp/newkernelimage**

Unison response: Interactive shell script is started.

RS-232 Serial I/O Port Signal Definitions

The RS-232 DB9M connector on the rear panel of the Unison is wired as shown below. In order to connect the Unison to another computer, a null-modem adapter must be used. The serial cable provided with the shipment is wired as a null-modem adapter and can be used to connect the Unison to your computer.

Unison DB9M Pin	Signal Name
1	Not Connected
2	Receive Data (RX)
3	Transmit Data (TX)
4	Data Terminal Ready (DTR)
5	Ground
6	Data Set Ready (DSR)
7	Request To Send (RTS)
8	Clear To Send (RTS)
9	Not Connected

Chapter*Six*

IPv6 Information

EndRun Technologies understands that IPv6 is still in the experimental stage with essentially no mainstream deployment. Customers who are not interested in IPv6 need not burden your system with it. You have a choice of an IPv4-only kernel (recommended) or the IPv4/IPv6-kernel. You may freely change this at any time with an easy software download from our website.

To determine which kernel resides in your Unison check the firmware version using console port command **`cat /proc/version`**.

An IPv4-only kernel will have a part number and version similar to:

6010-0041-000 ver 2.4.31-IPv4

An IPv4/IPv6 kernel will have a part number and version similar to:

6010-0041-100 ver 2.4.31-IPv6

If you want to change your kernel please refer to ***Appendix B - Upgrading The Firmware*** for instructions. The following text refers to products with the IPv4/IPv6 kernel.

Enabling New IPv6 Capabilities

The presence of an IPv6-capable kernel will automatically enable most of the new IPv6 capabilities. By default, autoconfiguration of the ethernet interface via IPv6 Router Advertisements is enabled. To disable acceptance of Router Advertisements, or to configure a static IPv6 address and default IPv6 gateway, you must either run the interactive **`netconfig`** script. This will allow you to configure your ethernet interface for both IPv4 and IPv6 operation. Using the **`netconfig`** script has the advantage that you can also configure the hostname and domainname for the unit, and any nameservers you may want it to have access to.

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/rc.d/rc.inet2* startup script, where **`sshd`** is started, and then copying it to */boot/etc/rc.d*.

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.local* and modifying the agent address argument passed to **`snmpd`** at start-up, and then copying it to */boot/etc/rc.d*.

IPv6-Capable syslog-ng

To enable remote syslogging to an IPv6 host, you will need to edit the new */etc/syslog-ng.conf* file and copy it to */boot/etc*. At boot time, the presence of both the **`syslog-ng`** daemon and the *boot/etc/syslog-ng.conf* file will cause the new IPv6-capable **`syslog-ng`** daemon to be started instead of the previous **`syslogd/klogd`** pair of daemons. These two files remain on the system for backward compatibility with customers' existing */etc/syslog.conf* setups, but they are not IPv6 capable. If you are not currently directing your system logs to a remote host, or you are not using IPv6, then there is little or need or benefit to changing to **`syslog-ng`**.

IPv4-Only Protocols

There are several protocols which are not IPv6-capable: **`telnet`** (client and server), **`http`**, **`ftp`** and **`dhcpcd`**. Due to their intrinsic insecurity, **`telnet`** and **`ftp`** are repidly being deprecated, and probably have little business running over an IPv6 network. The address autoconfiguration capabilities of IPv6 make the DHCP protocol less important, however it is likely that the new **`dhcpv6`** capability will appear in a future upgrade.

Chapter *Seven*

HTTP Interface

This chapter briefly describes the HTTP interface that resides on the Unison GPS Time Server. The HTTP interface to the Unison is a fast and easy-to-use graphical interface that is compliant with your standard web browser. Simply point your browser to the IP address of the Unison and login securely with HTTP. Security-conscious customers may disable the HTTP interface (see the end of this appendix for instructions). Note: The HTTP interface is not IPv6-compatible.

The HTTP interface is not available in older Unison models. If you have an older model you may want to contact EndRun for information on how to upgrade your Unison to be HTTP-capable. The older models have a Linux Subsystem root file system (RFS) number of 6010-0042-000. To see the number enter the **`gntpversion`** command via the network/serial port. The newer Unison models have (or can have) the HTTP interface capability. These models have a Linux Subsystem RFS number of 6010-0044-000.

The HTTP implementation in the Unison uses HTTPS (HTTP over SSL). Secure Socket Layer (SSL) is a sublayer under regular HTTP. HTTPS enhances security because it encrypts and decrypts the requested and returned pages from the server.

The HTTP implementation is built from the standard Apache/1.3.33 distribution from:

http://httpd.apache.org

See ***Appendix A - Security*** for information on changing the default HTTP configuration and SSL certificates.

IMPORTANT

The domain name server IP address is required by the Apache web server. When using **`netconfig`** (see ***Chapter 5 - Control and Status Command***s) to configure the TCP/IP parameters be sure to configure the name server. Only one name server is required, two gives some redundancy. The HTTP Interface will not start if this is configured incorrectly.

HTTP Interface Description

For security reasons the web pages on the Unison show status information only. You cannot reconfigure the Unison except for upgrading firmware, which is done with several security measures in place. To reconfigure the Unison you will need to use the network or serial port command line interface.

NOTE

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

To get started with the web interface simply point your browser to the IP address of the Unison and log in securely with HTTP. For example:

http://192.168.1.1

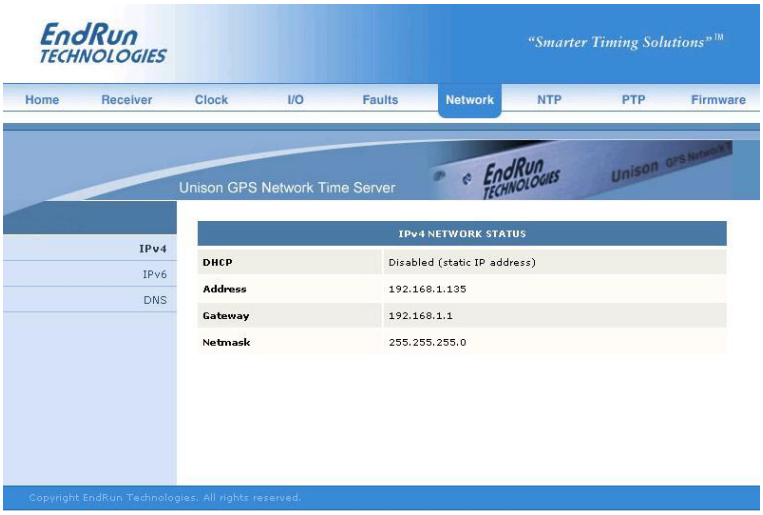
A warning dialog page will be presented for the certificate. Acknowledge the dialog page and the server will continue to load, protected by SSL. The browser should display the "Lock" icon, indicating that the page is protected by SSL. To maximize security you should replace the SSL Certificate. See ***Appendix A - Security, HTTP*** 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 Unison while links on the lefthand side of each webpage provide subcategory navigation.

For example, in the page below the main menu tabs are: Home, Receiver, Clock, I/O, Faults, Network, NTP, PTP and Firmware. The subcategory links on this particular page are: IPv4, IPv6 and DNS. IPv4 is selected.



The top-hand tabs and left-side links are logically arranged for easy navigation. The following table defines this relationship:

Tab	Information	Links
Home	Overall Unison Status Information	Login, Logout
Receiver	GPS Receiver Status	Receiver, Oscillator
Clock	Clock Status	
I/O	I/O Status (Options)	
Faults	Fault Status	
Network	IPv4 Network Status	IPv4, IPv6, DNS
NTP	NTP Status	
PTP	PTP/IEEE-1588 Status (Option)	
Firmware	Firmware Information	Firmware Status, Linux Subsystem Upgrade, GPS Subsystem Upgrade, Reboot

Page Descriptions

Home Page

This page contains general status information. Data fields are:

UTC Time

Shows the current hours, minutes and seconds in UTC.

Date

Shows the current UTC date.

Receiver

Shows whether the GPS receiver is locked or not.

TFOM
Shows the current TFOM value. See ***Appendix E - Time Figure of Merit*** for more information.

System Status
Shows if any system fault is present. If a system fault exists, go to the Faults Page to see which fault it is.

Receiver Page

This page contains information related to the GPS Receiver. Data fields are:

State
Shows whether the GPS receiver is locked or not.

TFOM
Shows the current TFOM value. See ***Appendix E - Time Figure of Merit*** for more information.

Satellite ID
This field lists the satellites that are currently being tracked. Up to 8 may be tracked at a time.

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

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

Reference Position Source
The source of the reference position can be Unknown, Dynamic, User-Entered or Average (24-hour average of GPS fixes). To change the reference position source use the **`gpsrefpos`** command.

Reference Position Latitute, Longitude and WGS-84 Height
The WGS-84 latitude and longitude in degrees, minutes, seconds format and the height above the WGS-84 reference ellipsoid in meters is shown. Refer to ***Appendix D - GPS Reference Position*** for details.

Last Position Fix Latitute, Longitude and WGS-84 Height
This field shows information for the most recent position fix. The WGS-84 latitude and longitude in degrees, minutes, seconds format and the height above the WGS-84 reference ellipsoid in meters is shown.

Antenna Fault Mask
This field shows the current setting for the Antenna Fault Mask. When the antenna fault is masked this will prevent the antenna fault from creating an alarm condition. Some installations may need to mask this fault due to special antenna situations like splitters. To change the Antenna Fault Mask use the **`setantfltmask`** command.

Signal Fault Mask
This field shows the current setting for the Signal Alarm Mask. When the signal alarm is masked it 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. To change the signal alarm mask use the **`setsigfltmask`** command.

Receiver (Oscillator) Page

This page shows receiver oscillator control information such as:

Oscillator Type
This field shows the oscillator type that is installed in the Unison. It will be either a TCXO or a MS-OCXO. The standard oscillator is the TCXO. If you purchase an oscillator upgrade this field will show MS-OCXO.

DAC
Is the upper 16 bits of the oscillator voltage control DAC word, 0 to 65535, with larger numbers implying higher oscillator frequency. Typical range is 20000 to 38000.

Clock Page

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

Time Mode
This field shows the current time mode setting. Possible settings are UTC, GPS and Local. Since NTP always uses UTC, this setting only affects any optional Time Code Output or Serial Time Output. For example, if your Unison has a Time Code Output and this field shows Local, then the time contained in the Time Code Output will be Local time but NTP will remain at UTC time. To change the time mode setting use the **`gntptimemodeconfig`** command via the network/serial port.

Local Time Offset
This field shows the offset from UTC and is only valid when the Time Mode is Local. A positive Local Time Offset implies a longitude east of the Greenwich meridian. To change the local offset use the **`gntptimemodeconfig`** command.

Daylight Savings Time (DST), DST Start, DST End
The DST fields show whether DST is enabled and if so, what the DST Start and End Times are. 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 **`gntptimemodeconfig`** command.

I/O Page

This page shows any installed CPU Options and their settings. These are optional outputs that are generated from the CPU Module in the Unison. A basic Unison has no CPU Options installed. Possible options are a 1PPS Output, an AM Code Output (time code), a Programmable TTL Output and a Serial Time Output. Use commands **`cpuoptsconfig`** and **`cpusertimeconfig`** via the network/serial port to change the settings of the CPU Options.

Faults Page

This page lists all possible fault conditions of the GPS Subsystem. The various faults are described below:

FLASH
This fault indicates that the microprocessor was unable to verify a write to the FLASH non-volatile parameter storage area. This should not ever occur under normal operation. The unit should be returned to the factory for repair.

FPGA
This fault indicates that the microprocessor was unable to configure the FPGA. This would be a fatal fault and the unit should be returned to the factory for repair .

Signal
This fault indicates that the unit has not been able to acquire a GPS signal for one hour while the Time Figure of Merit has been 9, the unsynchronized condition. This could be due to a variety of reasons. If there are no other faults that could explain the inability to receive a signal, then there could be an or antenna failure or blockage. If the condition persists indefinitely, and a problem with the antenna is not evident, the unit may need to be returned to the factory for repair.

DAC
This fault indicates that the electronic frequency control DAC for the oscillator has reached either the high (55000) or low (10000) limit while locked to the GPS signal. Unless the unit is being subjected to out-of-specification environmental conditions, this would indicate that the oscillator frequency has drifted near to the end of life region. This should normally only occur after about ten years of operation. The unit will continue to function until the oscillator frequency finally reaches one of the actual DAC endpoints. The unit should be returned to the factory for oscillator replacement at the your convenience.

Antenna
This fault indicates that the GPS antenna or downlead cable has a fault. It indicates either an over or under current condition. Usually it means that the antenna downlead cable is not plugged into the connector on the rear of the Unison. If the condition persists after checking the antenna/downlead for obvious faults, this is a fatal fault and the unit should be returned to the factory for repair.

Polling Events
This fault indicates that the GPS Subsystem is not receiving polling request from the Linux Subsystem. This could be due to a hardware or software failure. If the condition persists after cycling the power to the unit, this is a fatal fault and the unit should be returned to the factory for repair.

Time Reference
This fault indicates that the microprocessor received an erroneous time input from the GPS Subsystem. If the condition persists please report it to the factory (1-877-749-3878).

GPS Engine
This fault that the microprocessor is unable to establish communications with the GPS Subsystem engine. Please report this fault condition to the factory (1-877-749-3878).

Network Page

This page shows the IPv4 network configuration. Fields are:

DHCP
By default, the Unison 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 network/serial 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 netmask. To change these settings use the **`netconfig`** command via the network/serial port.

Network (IPv6) Page

This page shows information related to the IPv6 network parameters. If your Unison does not have IPv6 then there will be no fields on this page. For more information on IPv6 see ***Chapter 6 - IPv6 Information***.

Network (DNS) Page

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

NTP Page

The NTP Status page shows all information related to NTP operation. Fields are:

Status
The stratum field has three possible values:

Stratum 1:	The server is fully synchronized and accurate.
Stratum 2:	The server is synchronized to a Stratum 1 server.
Stratum 16:	The server is unsynchronized. NTP clients will not use a Stratum 16 server.

Source
This field will show the source of time which is usually GPS. If the Unison is configured as a Stratum 2 server then it will show the IP address of the upstream server.

Offset
This field shows the offset in seconds between the NTP system clock and the GPS Subsystem clock. Positive implies that the NTP system clock is ahead of the GPS Subsystem clock.

Leap Indicator Bits
This field shows whether a leap second is pending. Leap seconds occur every 2-3 years. Possible values for this field are: NONE, INSERT, DELETE or FAULT.

NONE:	No fault and no pending leap second.
INSERT	No fault and a leap second insertion is pending.
DELETE	No fault and a leap second deletion is pending.
FAULT	Unsynchronized fault condition exists.

PTP Page

The fields on this page show the status for the optional PTP/IEEE-1588 protocol. If your Unison does not have PTP then there will be no information on this page. The data shown will depend on whether PTPv1 or PTPv2 has been selected. For more information on PTP and an explanation of the data fields on this page see ***Appendix H - Precision Time Protocol (PTP) IEEE-1588***.

Firmware Page

The firmware status page shows part numbers and versions of the Linux Subsystem firmware (root file system and kernel) and the GPS Subsystem firmware.

Linux Subsystem Upgrade, GPS Subsystem Upgrade

These pages are used for upgrading the firmware. You must be logged in as "root" in order to have access to these pages. The latest released versions of Unison firmware are freely available on the EndRun website. For detailed information on how to perform the upgrade either via the network port, the serial port, or the HTTP interface see ***Appendix B - Upgrading The Firmware***. Only the Linux Subsystem root file system (RFS) and GPS Subsystem can be upgraded via the HTTP Interface. To upgrade the Linux Subsystem kernel see ***Appendix B - Upgrading The Firmware, Performing the Linux Kernel Upgrade***.

Reboot

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

Disabling The HTTP Protocol

To disable HTTP you need to edit a system start-up script called */etc/rc.d/rc.local*. This script starts several daemons. You can either remove the line that lists HTTP or you can place a **#** character at the beginning of the line so that it will not be executed. (A very compact editor is available on the system for this purpose: **`edit`**. If you start **`edit`** without giving it a file name to open, it will display its help screen, showing the supported keystrokes.)

IMPORTANT

After editing ***/etc/rc.d/rc.local***, 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.

Appendix *A*

Security

Your Unison 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 Unison. Others are provided by the additional protocol servers selected for inclusion in your Unison, 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, encyrpted 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 appendix 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 **`gntppasswd`** command. To change the passwords/community strings for SNMP see ***Appendix C - SNMP***.

By default all users are allowed access via SSH, Telnet and SNMP. To restrict access via these protocols, use the **`accessconfig`** command or edit /etc/hosts.allow and /etc/hosts.deny. All users are allowed access via HTTP as well. To restrict access via HTTP, edit /etc/apache/httpd.conf to set up access by specific hosts.

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

Linux Operating System

The embedded Linux operating system running in the Unison is based on kernel version 2.4.31 and version 10 of the Slackware Linux distribution. As such it 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 Unison.

- HTTP may be completely disabled by configuration of */etc/rc/.d/rc.local*.

- Access via SNMP 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 ***Appendix C – Simple Network Management Protocol*** which is dedicated to configuration of SNMP for details.

- Individual host access to protocol server daemons such as **in.telnetd, snmpd** or **sshd** may be controlled by the **tcpd** daemon and directives contained in the files */etc/hosts.allow* and */etc/hosts.deny.*

- Risky protocols like TIME, DAYTIME and TELNET may be completely disabled by configuration of the **inetd** super-server daemon.

The last two topics are supported on the Unison by a pair of shell scripts which ease configuration for the inexperienced user of Unix-like operating systems. These are **accessconfig** and **inetdconfig**.

Using Edit

A very compact editor is available on the system for editing files: **edit**. If you start **edit** without giving it a file name to open, it will display its help screen, showing all supported keystrokes.

Limiting Access

By default, the unit is configured to allow access by all users via Telnet, SSH and SNMP. To ensure security you should restrict access by using the **accessconfig** command.

accessconfig modifies two files which are used by **tcpd** and the standalone daemons, **snmpd** and **sshd**, to determine whether or not to grant access to a requesting host: */etc/hosts.allow* and */etc/hosts/deny*. These two files may contain configuration information for a number of protocol servers, but in the Unison 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 the user runs **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** and **sshd** to all hosts not listed in the */etc/hosts.allow* file. The **snmpd** and **sshd** daemons also parse this file prior to granting access to a requesting host. Then the user is 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.l68.1.3

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 ***Using Edit*** above.) Be careful to maintain the proper ownership and access permissions by using **`cp -p`** when copying the files.

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

```
# Controls who can get stuff from this server.
#
    Order allow,deny
    Allow from all
</Directory>
```

To restrict access to a specific host with IP address xxx.xxx.xxx.xxx, you would modify the directives as so:

```
# Controls who can get stuff from this server.
#
    Order allow,deny
    Deny from all
    Allow from xxx.xxx.xxx.xxx
</Directory>
```

Disabling Protocols

You may completely disable any of the following protocols: Telnet, TIME, DAYTIME, SSH, SNMP and HTTP.

Disable Telnet, TIME and DAYTIME

To disable Telnet, TIME and DAYTIME use the **`inetdconfig`** command. **`inetdconfig`** modifies the */etc/inetd.conf* file which is read by **`inetd`** to start-up various protocol server daemons when requests from remote hosts are received. Currently, three servers are configurable via **`inetdconfig`**: TIME and DAYTIME, whose daemons 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 and HTTP

To disable SNMP and HTTP, edit a system start-up script called */etc/rc.d/rc.local*. This script starts several of the daemons running on the system. You should follow the instructions contained in comments in the file for disabling the **`snmpd`** and **`httpd`** daemons. Placing a **`#`** character at the beginning of a line makes it a comment line so that it will not be executed. (See ***Using Edit*** above.)

Disable SSH

To disable SSH, edit a system start-up script called */etc/rc.d/rc.inet2*. This script starts several of the daemons running on the system. You should follow the instructions contained in comments in the file for disabling the **sshd** daemon. Placing a **#** character at the beginning of a line makes it a comment line so that it will not be executed. (See ***Using Edit*** above.)

IMPORTANT

After editing ***/etc/rc.d/rc.local and/or /etc/rc.d/rc.inet2***, you must copy them to the ***/boot/etc/rc.d*** directory and reboot the system. It is very important to retain the access mode for these files, 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.

OpenSSH

The secure shell protocol server running in the Unison is based on the portable OpenSSH for Linux. As such it supports both SSH1 and SSH2 protocol versions. By default, only SSH2 is enabled due to security issues with SSH1. For more information about this protocol 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 available from O'Reilley & Associates:

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

In the interest of conserving scarce system memory resources, only the secure shell server daemon, **sshd** and the secure copy utility, **scp**, are implemented in the Unison. This means that users on remote hosts may log in to the Unison via an **ssh** client, but users logged in on the Unison are unable to log in to a remote host via **ssh**. Since **scp** runs in concert with an **ssh** client, the same limitations exist for its use, i.e. users on remote hosts may transfer files to and from the Unison via **scp** over **ssh** but users logged in on the Unison are unable to transfer files to and from a remote host via **scp** over **ssh**.

The factory configuration contains a complete set of security keys for both SSH1 and SSH2 versions of the protocol. RSA keys are supported by both versions, and DSA keys are supported when using the SSH2 version.

In addition, the Unison is factory configured with a set of public keys for passwordless, public key authentication of the root user. To use this capability, the corresponding set of private keys for each of the two SSH versions are provided in the */boot/root* directory of the Unison. Three files contain these keys: *identity* (SSH1), *id_rsa* (SSH2) and *id_dsa* (SSH2). These must be copied to the user's *root/.ssh* directory on their remote computer. (Be careful to maintain the proper ownership and access permissions by using **cp -p** when copying the files. They MUST be readable only by *root*.) The corresponding public keys are by factory default resident in the */root/.ssh* directory of the Unison. Two files contain these keys: *authorized_keys* (SSH1) and *authorized_keys2* (SSH2).

Since the provided private keys are not passphrase protected, the user should create a new set of keys after verifying operation with the factory default key sets. After creating the new keys, the public

keys should be copied to the */boot/root/.ssh* directory of the Unison. At boot time, the Unison will copy these to the actual */root/.ssh* directory of the system ramdisk, thereby replacing the factory default set of public keys.

Advanced users wishing to modify the configuration of the **sshd** daemon should edit the */etc/sshd_config* file and then copy it to the */boot/etc* directory of the Unison. 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* directory of the system ramdisk, thereby replacing the factory default configuration file.

To disable SSH, see ***Disable SSH*** above.

Network Time Protocol

The NTP implementation in the Unison is built from the standard distribution from the http://www.ntp.org site. By factory default, remote control of the NTP daemon **ntpd** is disabled. Query-only operation is supported from 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

This line eliminates control access from ALL hosts. Query access is not affected by this restriction. Knowledgable NTP users who would like to customize the security aspects of the configuration of the NTP daemon in the Unison 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 restrict query access to a specific remote host with IP address 192.168.1.10 while also allowing processes running on the Unison to have query access as well:

```
restrict default noquery nomodify
restrict localhost nomodify
restrict 192.168.1.10 nomodify
```

HTTP

The HTTP server in the Unison is built from the standard Apache/1.3.33 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.

HTTP and SSL use two files for the default configuration located in */etc/apache*. These are *httpd.conf* and *ssl.conf*. Advanced users who need to modify the default configuration will need to edit these two files and copy them to the */boot/etc/apache* directory. (See ***Using Edit*** above.)

For SSL it is recommended that new certificates are generated and installed on the Apache web server with mod_ssl. The current certificates included are located in */etc/apache/ssl.ctr*, */etc/apache/ssl.csr*, and */etc/apache/ssl.key*. New certificates, CSRs, and private keys will need to be saved in */boot/etc/apache/ssl.crt*, */boot/etc/apache/ssl.csr*, and */boot/etc/apache/ssl.key* directories.

By default, the Apache server configuration file httpd.conf for httpd is factory-configured. It contains the configuration directives that give the server its instructions. Although not required, the directives may be changed by editing */etc/apache/httpd.conf*, and then copying it to */boot/etc/apache*. Do not attempt to change the directives unless you have a real need to do so.

An excellent book which describes operation and configuration of the various HTTP directives and SSL configuration is:

Professional Apache, Wainwright, Wrox Press, 1999.

To disable HTTP, see ***Disable SNMP and HTTP*** above.

Appendix *B*

Upgrading the Firmware

Periodically, EndRun Technologies will make bug fixes and enhancements to our products available for download from our website. All such downloads are freely available to our customers, without charge. You may securely upgrade your Unison firmware via the HTTP interface, the network port, or the serial port. Software upgrades for the Unison are available at this link:

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

Upgrade Via The HTTP Interface

The HTTP interface is not available in the older Unison models. These models have a Linux Subsystem root file system (RFS) number of 6010-0042-000. To see the number enter the **`gntpversion`** command via the network/serial port. If you have one of the older Unison models please proceed to the next section - ***Upgrade Via The Network/Serial Port***.

The newer Unison models have (or can have) the HTTP interface capability. These models have a Linux Subsystem RFS number of 6010-0044-000. The HTTP interface was introduced at version 5.50 of the Linux Subsystem software. If you have one of the newer Unison models and your current software version is at least 5.50, you may upgrade firmware via the HTTP interface or the network/serial port.

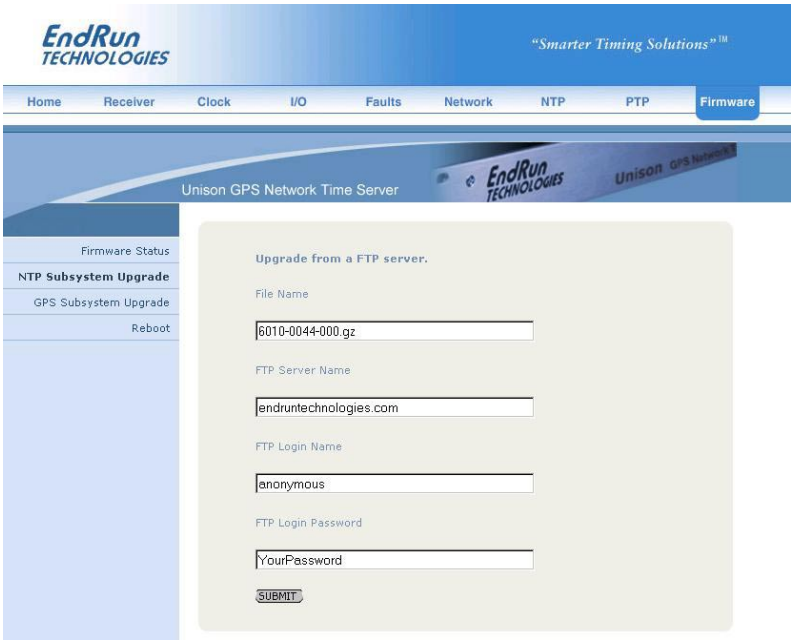
Software upgrades via the HTTP interface are simple, with your choice of two methods:

1. If your Unison has access to the internet, the HTTP interface can automatically retrieve the appropriate files from the FTP server at endruntechnologies.com to temporary locations on the Unison. You will need to authenticate the root user name and password, and follow the prompts from the HTTP interface to complete each upgrade, one for the Linux Subsystem and the other for the GPS Subsystem.

IMPORTANT

The domain name server IP address is required by the Apache web server. When using **`netconfig`** (see ***Chapter 5 - Control and Status Command***s) to configure the TCP/IP parameters be sure to configure the name server. Only one name server is required, two gives some redundancy. The HTTP Interface will not start if this is configured incorrectly.

The following picture shows the Linux Subsystem RFS Upgrade page. All fields are filled in with default values to download the appropriate software 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 Unison does not have access to the internet, you must first download the appropriate files from the endruntechnologies.com website to the computer that you will be using later to access the Unison via its HTTP interface. Use the link shown above to get the files. After saving the files, use the Unison HTTP interface to select the previously saved files for upload to the Unison. One for the Linux Subsystem and the other for the GPS Subsystem. Then follow the remaining prompts from the HTTP interface to complete the upgrades. (You will need to authenticate the root user name and password.)

Upgrade Via The Network/Serial Port

In order to upgrade via the network or serial ports you will need to first download the appropriate FLASH binary image file from the EndRun website. After you have done this you are ready to upgrade your Unison. The firmware consists of two FLASH binary image files. One of these is the firmware for the Unison Linux/NTP Subsystem. This firmware executes on the IBM-compatible CPU and contains the embedded Linux operating system and NTP specific application software. The other file is the firmware for the GPS Subsystem. Each of these files may be upgraded independently, although some upgrades require both images to be modified together.

You will need to use **ftp** or **scp** to transfer the binary image file(s) to the Unison. This means that you must place the previously downloaded file(s) in a place on your network which is accessible to the Unison.

Performing the Linux/NTP Subsystem Upgrade

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 devices. To protect the factory root file system from accidental erasure or over-writing, the device node has been deleted. The upgrade FLASH disk partition is accessed via */dev/rootfs_1*. When performing an upgrade, you will be copying the new image to this device.

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.

To perform the upgrade, log in as the *root* user to the Unison using the local console serial I/O port, **telnet** or **ssh** and perform these operations:

First erase the upgrade partition by issuing this command at the shell prompt:

```
eraserootfs_1
```

If you are using **ftp** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to */dev/rootfs_1* on your Unison using FTP. The root file system image will be named with the software part number and version like: *6010-004x-000_3.00.gz*. When following the instructions below, substitute the name of the actual root file system image that you are installing for *6010-004x-000_3.00.gz*. Issue these commands from the console of your Unison:

```
ftp remote_host                          {perform ftp login on remote host}
bin                                      {set transfer mode to binary}
get 6010-004x-000_3.00.gz /dev/rootfs_1  {transfer the file}
quit                                     {close the ftp session after transfer }
```

If you are using **ssh**, you may open a command window on the remote computer and securely transfer the root file system image using **scp** from the remote computer to your Unison. A command like

this should be used:

```
scp -p 6010-004x-000_3.00.gz root@gntp.your.domain:/dev/rootfs_1
```

Update the default file system partition by issuing this command on your Unison.

```
updaterootflag 1
```

You should see this line displayed:

```
UPGRADE is the default root file system.
```

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

```
shutdown -r now
```

Wait about 90 seconds for the system to shutdown and reboot. Then log in to the Unison 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 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

```
gntpversion
```

which will cause the system 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:

```
gntprootfs
```

Which should cause this to be printed to the console:

```
BOOT_IMAGE=UnisonGPS_1
```

If so, and your unit seems to be operating normally, you have successfully completed the 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 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 Unison.

Recovering from a Failed Upgrade

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

Pay close attention to the terminal window while the unit is rebooting. After the Linux bootloader displays the message

```
To override and boot the FACTORY partition 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 upgrade and re-perform it.

Performing the Linux Kernel Upgrade

The Unison is shipped from the factory with a kernel that is IPv4-only capable only. If you want to upgrade your kernel to the IPv4/IPv6-capable one then you must first be sure that your root file system is version 2.60 or later. To see the root file system version type **gntpversion** at the network/serial port.

To upgrade your kernel, log in as the *root* user to the Unison using the local console serial I/O port, **telnet** or **ssh** and perform these operations:

If you are using **ftp** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to a temporary location on your Unison using FTP. The IPv6 kernel image will be named with the software part number like: *6010-0041-100.bzimage*. When following the instructions below, substitute the name of the actual kernel image that you are installing for *6010-0041-100.bzimage*. Issue these commands from the console of your Unison:

```
ftp remote_host                          {perform ftp login on remote host}
bin                                      {set transfer mode to binary}
get 6010-0041-100.bzimage /tmp           {transfer the file}
quit                                     {close the ftp session after transfer }
```

If you are using **ssh**, you may open a command window on the remote computer and securely transfer the root file system image using **scp** from the remote computer to your Unison. A command like this should be used:

```
scp -p 6010-0041-100.bzimage root@gntp.your.domain:/tmp
```

The kernel upgrade utility is executed with a single argument passed on the command line: the path to the previously uploaded kernel image file. For example:

```
upgradekernel /tmp/6010-0041-100.bzimage
```

The kernel upgrade utility verifies the integrity of the file, reads the kernel version information, presents it to you and asks you to verify before replacing the old kernel image. If you verify, it will then erase the old image and write the new one in its place. The erase and write operation takes about 10 seconds.

CAUTION

A power failure during the kernel erase and write operation would render your unit unbootable. It is highly advisable to plug your unit into a UPS while performing the kernel upgrade.

Performing the GPS Subsystem Upgrade

To perform this upgrade, log in as the *root* user to the Unison using either the local console serial I/O port, **telnet** or **ssh** and perform these operations:

Change the working directory to the */tmp* directory:

```
cd /tmp
```

If you are using **ftp** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to the working directory, */tmp*. The GPS Subsystem image will be named with the software part number and version like: *6010-0020-000_3.01.bin*. When following the instructions below, substitute the name of the actual GPS Subsystem image that you are installing for *6010-0020-000_3.01.bin*:

```
ftp remote_host                 {perform ftp login on remote host}
bin                             {set transfer mode to binary}
get 6010-0020-000_3.01.bin      {transfer the file}
quit                            {close the ftp session after the transfer }
```

If you are using **ssh**, you may open another command window on the remote computer and securely transfer the GPS Subsystem image to the */tmp* directory using **scp** from the remote computer. A command like this could be used:

```
scp -p 6010-0020-000_3.01.bin root@gntp.your.domain:/tmp
```

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

```
upgradegps /tmp/6010-0020-000_3.01.bin
```

This command is a script that performs the file transfer to the GPS engine. It first tells the GPS engine to enter the 'waiting for download' mode, and then prompts you with this line

```
---When you see the `C` character, hit <enter> to begin the upload.
```

Then it echos the serial port characters sent by the GPS engine to the console. You should next see this message from the GPS engine:

```
Waiting for download using XMODEM 128 or XMODEM 1K (both with CRC).
Control X will abort download.
```

After about 3 seconds, you should see a capital 'C' character appear. When you do, hit the <enter> key. Now the script will initiate the XMODEM file transfer and display this message to the console:

```
---Starting file upload, should take about 90 seconds...
```

After about one minute you should see this message from the script:

```
/sbin/upgradegps: line 26: 27618 Terminated       cat </dev/arm_user

---You should see the GPS sub-system startup message now.  If not, you
---may need to check your binary file and re-perform the procedure.
```

The first message should be ignored. It is only reporting that one of the intermediate processes of the script execution has been terminated. The next message informs you that the GPS engine file transfer

has completed, and that its start-up messages should appear. First the bootloader message will appear:

```
Tempus Bootloader 6010-0050-000 v 1.00 - May 28 2004 17:31:05
```

In about ten seconds, the GPS engine application start-up messages should appear:

```
FW 6010-0020-000 v 1.00 - Aug 18 2004 10:47:41
FPGA 6020-0005-000 v 0202
```

The firmware version should match that of the binary file that you uploaded. At this point, the **upgradegps** script terminates its execution, and you will again have the standard Unison console prompt.

After about one minute, you should query the GPS firmware version using the command:

```
gpsversion
```

The upgraded version information should be displayed.

Problems with the GPS Subsystem Upgrade

Should you have difficulties with the upgrade due to a corrupt file, power failure during upload, or other accident, do not be alarmed. Even though you may have lost the existing application program, the GPS engine bootloader program will remain intact. On boot up, it will check to see if a valid application program is in the FLASH memory. If there is not, it will immediately go into the 'waiting for download' mode. You may verify this by issuing this command:

```
cat < /dev/arm_user
```

You should now see the 'C' character being received every three seconds. This is the character that the GPS engine bootloader sends to indicate to the XMODEM utility that it is wating for a download. You may now retry the upload procedure, assuming that you have corrected any original problem with the binary file. First kill the **cat** command by typing CTRL-C. You should see a command prompt. Now issue this command to re-transfer the binary file:

```
upgradegps /tmp/6010-0020-000_3.01.bin
```

Recover Command

Sometimes a user will attempt to download the wrong file to the GPS Subsystem. When this happens the recovery method above will not work. After issuing the **cat** command above you will not see a series of "C" characters, but instead you will see the bootloader message being output every few seconds. In this case you need to use a different recovery procedure.

First make sure the above **cat** command is killed by typing CTRL-C. Then enter a new **cat** command as:

```
cat < /dev/arm_user &
```

You should again be seeing the bootloader message every few seconds:

```
Tempus Bootloader 6010-0050-000 v 1.00 - May 28 2004 17:31:05
```

Please type the following command but do not press enter:

```
echo -e "recover\r" > /dev/arm_user
```

Now wait until you see another bootloader message come out and then press enter. You will then see the "C" come out every 3 seconds. You then kill the previous **cat** command by entering:

```
kill $!
```

You should see a command prompt. Now issue this command to re-transfer the correct binary file:

```
upgradegps /tmp/6010-0020-000_3.01.bin
```

Appendix C

Simple Network Management Protocol (SNMP)

Your Unison includes the (NET)-SNMP version 5.3.1 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:

TEMPUSLXUNISON-MIB

Which is located on your Unison in this ASCII file:

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

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

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

Invocation of the SNMP daemon

The SNMP daemon, **snmpd** is started from the */etc/rc.d/rc.local* system start-up script with this line:

```
snmpd -m "$MIBNAME" -Ls d -c /etc/snmpd.conf
```

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 by adding **-p port** to the end of this line, where **port** is the number of the port you would like for the agent to listen on. If you would like to disable starting of the **snmpd** daemon altogether, you can either remove this line or place a **#** character at the beginning of the line so that it will not be executed. (A very compact editor with WordStar command keystrokes is available on the system for this purpose: **edit**. If you start **edit** without giving it a file name to open, it will display its help screen, showing the supported keystrokes.)

IMPORTANT

After editing ***/etc/rc.d/rc.local***, 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 TEMPUSLXUNISON-MIB file on your SNMP management system and access the variables defined therein. The factory default community names are "TempusLX-Unison" 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)

To ensure security, you should change the default community names by editing */etc/snmpd.conf* and modifying these two lines:

```
rwcommunity   endrun_1
rocommunity   TempusLXUnison
```

Configuring SNMPv1 Trap Generation

To have your Unison 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 Unison. 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 each destination, the enterprise trap generation mechanism of the Unison will only send a trap to the last declared **trapsink** in the file.

Configuring SNMPv2c Notifications and Informs

To have your Unison 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 Unison. 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 agent will recognize multiple **trap2sink** or **informsink** lines within */etc/snmpd.conf* and send the generic SNMP coldStart or authenticationFailure notifications and informs to each destination, the enterprise notification/inform generation mechanism of the Unison 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 Unison 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 Unison, 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 Tempus_0
```

The first line will cause the agent, **`snmpd`** to create a user *root* who may be authenticated via Message Digest Algorithm 5 (MD5) with password *endrun_1* and may use the Data Encryption Standard (DES) to encrypt the session data with passphrase *endrun_1*. The second line will cause a user *ntpuser* to be created who may be authenticated using the Secure Hash Algorithm (SHA) with password

Tempus_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`** process prior to editing, ***/boot/net-snmp/snmpd.conf***. Otherwise, the secret key creation may not complete properly. Issue the command **`ps -e`** to have the operating system display the list of running processes. Look for the PID of the **`snmpd`** process and issue the kill command to stop it. For example, if the PID listed for the **`snmpd`** process is 53, then you would issue this command: **`kill 53`**. You can verify that the process was terminated by re-issuing the **`ps -e`** command.

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.

Disabling The SNMP Protocol

To disable SNMP you need to edit a system start-up script called */etc/rc.d/rc.local*. This script starts several daemons. You can either remove the line that lists SNMP or you can place a **#** character at the beginning of the line so that it will not be executed. (A very compact editor is available on the Unison system called **`edit`**. If you start **`edit`** without giving it a file name to open, it will display its help screen, showing all supported editing keystrokes.)

IMPORTANT

After editing ***/etc/rc.d/rc.local***, 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.

Appendix *D*

GPS Reference Position

Your Unison is capable of operation from either an automatically determined GPS reference position or a manually entered GPS reference position. If your Unison is unable to automatically determine this information itself, this appendix describes the needed background information and procedures for determining an acceptably accurate GPS reference position in the proper ***World Geodetic Survey of 1984 (WGS-84) geodetic datum****.*

Obtaining Reference Positions

If you need to provide an accurate (< 100 meter error) reference position to your Unison because you are using a window-mounted antenna with inadequate satellite visibility, there are two good ways to do it: 1) use a handheld GPS receiver to obtain a position near the location of your Unison antenna or 2) reference a geodetic database to obtain a position for your street address.

Using a Handheld GPS Receiver

Obtain an inexpensive, handheld GPS receiver. Use it outside of the building to determine a position that is within 100 meters of the installed Unison antenna. Make sure that the handheld GPS receiver is configured to report its positions in the WGS-84 datum. Record the position and then make any adjustments to the height that might be necessary if the antenna is installed in a high-rise building. Input it to the Unison via the **`setgpsrefpos`** command.

Using the Internet

Reasonably accurate position information can be obtained from various websites on the Internet. Using your favorite search engine, type in a search term such as: “street gps position”. Many of the websites displayed will give you the ability to type in your location and provide your GPS position coordinates. Record the position and then make any adjustments to the height that might be necessary if the antenna is installed in a high-rise building. Input it to the Unison via the **`setgpsrefpos`** command.

Using “Indirect GPS”

There are some locations where using a GPS window-mount installation is not practical, either because of metallic films on the window, or the view from the window is blocked, or the window is facing away from the equator. In these cases we have an alternative product that uses CDMA cell phone signals for time synchronization. We call it “indirect GPS”. CDMA is not available worldwide, but if you work in an area with CDMA cell phone service then you will be able to mount your antenna on top of your equipment rack inside your data center. Contact EndRun Sales or Support for more information.

Appendix *E*

Time Figure-of-Merit (TFOM)

This appendix describes the Time Figure of Merit (TFOM) number. The Unison displays this number in the time-of-day fields printed by the Unison **gpsstat** *and* **gntpstat** *commands (see Chapter 5). The TFOM number indicates the level of accuracy that should be included in the interpretation of the time-of-day and ranges from 3 to 9:*

3	time error is < 100 nanoseconds
4	time error is < 1 microseconds
5	time error is < 10 microseconds
6	time error is < 100 microseconds
7	time error is < 1 milliseconds
8	time error is < 10 milliseconds
9	time error is > 10 milliseconds, unsynchronized state if never locked to GPS

In all cases, the Unison reports this value as accurately as possible, even during periods of GPS signal outage where the Unison is unable to directly measure the relationship of its timing outputs to UTC. During these GPS outage periods, assuming that the Unison had been synchronized prior to the outage, the Unison extrapolates the expected drift of the Unison timing signals based on its knowledge of the characteristics of the internal Temperature Compensated Crystal Oscillator (TCXO), Oven Controlled Crystal Oscillator (OCXO) or Rubidium oscillator. The extrapolated TFOM is based on a conservative estimate of the performance of the oscillator and should be considered 'worst case' for a typical benign ambient temperature environment.

Due to this extrapolation behavior, after initial synchronization, brief periods without GPS satellite visibility will not induce an immediate alarm condition. (Removal of the antenna to simulate this will induce an immediate alarm, however.) If the condition persists for long enough periods, you should see the TFOM character change to indicate a gradually deteriorating accuracy of the timing outputs. If the signal loss condition persists longer, then the final, unsynchronized state will eventually be reached. If the Unison is unable to achieve re-synchronization within one hour after reaching this state, the red LED will illuminate. The fault status field returned in either of the **gpsstat** or **gntpstat** commands will have the appropriate bit set to indicate a loss-of-signal time-out condition.

If the GPS Subsystem reaches the unsynchronized TFOM state, the NTP daemon will cease to use the timing information returned by the GPS 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.

Appendix *F*

Third-Party Software

The Unison 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
Copyright (C) 1989,1991 Free Software Foundation, Inc.,
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.

END OF TERMS AND CONDITIONS

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 Unison is covered 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:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
```

```
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. The end-user documentation included with the redistribution,
*    if any, must include the following acknowledgment:
*       "This product includes software developed by the
*        Apache Software Foundation (http://www.apache.org/)."
*    Alternately, this acknowledgment may appear in the software itself,
*    if and wherever such third-party acknowledgments normally appear.
*
* 4. The names "Apache" and "Apache Software Foundation" must
*    not be used to endorse or promote products derived from this
*    software without prior written permission. For written
*    permission, please contact apache@apache.org.
*
* 5. Products derived from this software may not be called "Apache",
*    nor may "Apache" appear in their name, without prior written
*    permission of the Apache Software Foundation.
*
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
* DISCLAIMED.  IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
* ====================================================================
*
* This software consists of voluntary contributions made by many
* individuals on behalf of the Apache Software Foundation.  For more
* information on the Apache Software Foundation, please see
* <http://www.apache.org/>.
*
* Portions of this software are based upon public domain software
* originally written at the National Center for Supercomputing Applications,
* University of Illinois, Urbana-Champaign.
*/
```

PTP Software License

The PTP/IEEE-1588 option as implemented in the Unison is coverd by patents and copyrights.

See the IEEE Standards Association at: http://standards.ieee.org/db/patents/pat1390.html for patents that pertain the the Std No 1588.

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 each file.

Copyright (c) 2005-2008 Kendall Correll, Aidan Williams

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Appendix G

Serial Time Output

This option is provided on a second RS-232 (or RS-422) serial port. It is a serial time string output that provides a once-per-second sequence of ASCII characters indicating the current time. The "on-time" character is transmitted at the very beginning of each second, with the leading edge of the start bit transmitted during the first 100 microseconds. This output starts automatically at power-up. See ***Appendix J - Specifications*** *for pinout.*

To configure this output use the **`cpusertime`** and **`cpusertimeconfig`** commands (see ***Chapter 5 - Control and Status Commands).***

There are several different formats for this string. The format, baud rate and parity can all be changed via console command **`cpusertimeconfig`**. 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.

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 the string is UTC and it 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.
<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 Unison. (See **`gntptimemodeconfig`** in ***Chapter 5 - Control and Status Commands***.) 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 Unison. For example, if you want the time in this string to be UTC, then set the time mode of the Unison to UTC. (**`gntptimemodeconfig`** in ***Chapter 5 - Control and Status Commands***.) 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 (TFOM) character described in ***Appendix E - TFOM.*** This is the "on-time" character.
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 (TFOM) character described in ***Appendix E - TFOM***. This is the "on-time" character.
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.
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 United States 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. This is the "on-time" character.
^	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. This is the "on-time" character.
^	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. This is the "on-time" character.
^	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 Unison conform to NMEA-0183 Specification Version 3.01 and are GGA, GLL, GSA, RMC, VTG and ZDA. Your Unison can output one, two, or three of these sentences per second.

You can select which NMEA sentences to output by using the **`cpusertime`** and **`cpusertimeconfig`** commands (see ***Chapter 5 - Control and Status Commands).***

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

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 leading edge of the start bit of the "on-time" character is transmitted within 100 microseconds of the beginning of the second.

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

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

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

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

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

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

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

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

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

RMC (Recommended Minimum Specific GPS Data)
The RMC sentence identifies the UTC time of fix, status, latitude, longitude, and date. Examples are below:

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

Msg ID	$GPRMC	
Field 1	173831.00	UTC time of fix (hhmmss.ss)
Field 2	A	GPS receiver warning (A=data valid, V=data not valid)
Field 3	3827.030	Latitude in ddmm.mmm
Field 4	N	Direction of latitude (N=north, S=south)
Field 5	12244.020	Longitude in dddmm.mmm
Field 6	W	Direction of longitude (W=west, E=east)
Field 7	0.08	Speed over ground, knots
Field 8	158.14	Course made good, degrees True
Field 9	200508	Date of fix (ddmmyy)
Field 10	empty field	Magnetic variation
Field 11	empty field	Direction of magnetic variation
Field 12	A	A=autonomous mode, N=data not valid
Checksum	*0D	
Msg End	<CR><LF>	

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

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

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

ZDA (Time and Date)

The ZDA sentence identifies the time associated with the current 1PPS pulse. Each sentence is transmitted within 500 milliseconds after the 1PPS pulse is output and tells the time of the pulse that just occurred. If the Unison 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 zone hour, offset from UTC (- for east longitude)
Field 6	00	Local zone minutes, offset from UTC
Checksum	*69	
Msg End	<CR><LF>	

Appendix *H*

Precision Time Protocol (PTP) IEEE-1588

This appendix contains the configuration and status information for the optional Precision Time Protocol. Both PTP version 1 and PTP version 2 are available. The PTPv2 protocol running on the Unison is a full Grandmaster Clock (default profile) implementation of the IEEE-1588-2008 standard. The PTPv1 protocol is a full Grandmaster Clock implementation of the IEEE-1588 2002 standard. The PTP version is user-selectable and once configured, the Unison operates as a PTP Grandmaster Version 1 OR Version 2.

About PTP

The PTP implementation in the Unison is built from the distribution at the PTPd website: http://ptpd.sourceforge.net.

The PTP daemon status and configuration is supported from two PTP companion utilities **`gptpstat`** or **`gptp2stat`** and **`ptpconfig`** or **`ptp2config`**. The following table shows the Unison utilities that pertain to PTPv1 and PTPv2:

	Daemon	Status	Configuration
PTPv1	**`ptpd`**	**`gptpstat`**	**`ptpconfig`**
PTPv2	**`ptp2d`**	**`gptp2stat`**	**`ptp2config`**

For more information about **`ptpd`** 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-1.00.tar.gz* if using PTPv1 or *ptpd-2.1.0.tar.gz* if using PTPv2.

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://ieee1588.nist.gov.

Version PTPv2 or PTPv1

In the Unison, you may use the PTPv1 protocol or the PTPv2 protocol. PTPv2 is the default. In order to change the selection from PTPv2 to PTPv1 you need to use the **ptpversionconfig** command.

The following is a transcript of the question and answer configuration utility provided by **ptpversionconfig**.

```
Unison GPS(root@endrun:~)-> ptpversionconfig

*******************************************************************************
***********Precision Time Protocol IEEE-1588 Version Configuration*************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure PTP Version 1 or 2                *
*                                                                             *
*                                                                             *
*   The changes you make now will not take effect until you re-boot the       *
*   Unison GPS.  If you make a mistake, just re-run ptpversionconfig prior    *
*   to re-booting.                                                            *
*                                                                             *
*   You will now be prompted for the necessary set up parameters.             *
*                                                                             *
*******************************************************************************
*******************************************************************************

---PTP Version Configuration


Set the PTP Version (1 or 2) 2

Configuring PTP to start as Version 2...

*******************************************************************************
*******************************************************************************
*                                                                             *
*  The Unison GPS Precision Time Protocol IEEE-1588 Version 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:

```
shutdown -r now
```

PTPv2 Configuration and Status

The default PTPv2 configuration settings in the Unison are shown below. If you need to modify these settings then you will need to reconfigure the PTPv2 subsystem. You may perform the configuration from either a **telnet** or **ssh** session, or the local RS-232 console. Default PTPv2 settings are:

Sync Interval:	1 second
Announce Interval:	2 seconds
Priority 1:	128
Priority 2:	128
Delay Mechanism:	E2E
Domain:	0
PTP Time Mode:	UTC
PTP TTL:	1

PTPv2 Configuration Using the Network or Serial Port

The **ptp2config** command starts an interactive shell script that will allow you to configure the PTPv2 subsystem of the Unison. You will be prompted to set PTPv2 parameters as follows:

Sync Interval:	1 or 2
Announce Interval:	1, 2, 3, 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

One file is modified, */etc/ptp2.conf*. This is a non-volatile stored file in the FLASH disk */boot/etc* directory. You must reboot the Unison after running this script for the changes to take effect.

The following is a transcript of the question and answer configuration utility provided by ptp2config. The user-entered parameters are underlined:

Unison GPS(root@cntp)-> ptp2config

```
*******************************************************************************
************Precision Time Protocol IEEE-1588 V2 Configuration***************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure the ptp2.conf file                *
*   that controls the PTP V2 daemon operation.                                *
*                                                                             *
*   You will be able to configure the PTP sync interval, announce interval,   *
*   priority1, priority2, delay mechanism , ptp domain, time mode, and ttl.   *
*                                                                             *
*   The changes you make now will not take effect until you re-boot the       *
*   Unison GPS.  If you make a mistake, just re-run ptp2config 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 seconds (1 or 2) 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) UTC

---PTP TTL Configuration

Set the PTP TTL value (1-255) 1

*******************************************************************************
*******************************************************************************
*                                                                             *
*  The Unison GPS 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:

```
shutdown -r now
```

PTPv2 Status Using the Network or Serial Port

The **gptp2stat** command allows you to query the status of the PTPv2 subsystem. The ptp2d daemon running on the system updates the */var/log/ptp.monitor* every five seconds under normal operation. This logfile is parsed and formated to provide the status string having these fields:

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

Where:

V	is the IEEE-1588 version 2 for the 2008 standard.
SI	is the PTP sync interval, either 1 or 2 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 ttl in a range from 1 to 255.
CLASS	is the PTP clock class either SYNCHRONIZED, HOLDOVER, or UNLOCKED.
SCALE	is the PTP timescale either PTP or ARB.
STATE	is the PTP port state either MASTER, PASSIVE, or LISTENING.
CLKID	is the PTP clock source either GPS, or OSC.
UTC	is the PTP utc offset in seconds.
UTCV	is the PTP utc offset valid, either TRUE or FALSE.
CA	is the PTP clock accuracy either 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.

PTPv2 Operation

The Unison 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 Unison will begin to transmit PTP Sync messages after it is locked.

The PTP Sync Interval is user configured, either 1 or 2 seconds is transmitted as a multicast. The packet is only transmitted when the clock is fully synchronized or in holdover. The delay interval is 2 seconds.

The PTP Announce Interval is user configured, either 1, 2, 4, 8, or 16 seconds is transmitted as a multicast. The packet is only transmitted when the clock is fully synchronized or in holdover. The Announce Interval must be no shorter than the Sync Interval.

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, then 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 either E2E or P2P. E2E uses the delay request-response mechanism. 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, 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 appendix for more information.

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

PTP Clock Class either SYNCHRONIZED, HOLDOVER, or UNLOCKED. The Clock Class is SYNCHRONIZED when the TFOM level is at 3. The Clock Class is HOLDOVER when the TFOM level is greater than 3 and less than 9. The Clock Class is UNLOCKED when the 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 either 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 either GPS, or OSC. The PTP Clock Source is GPS if the Clock Class is Synchronized, otherwise it is OSC based on the internal oscillator.

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

The PTP UTC Offset Valid either TRUE or FALSE. The PTP UTC Offset Valid is TRUE if the current PTP 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:

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

The PTP Leap 59 second indicator, 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, 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, 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, either TRUE or FALSE. The Frequency Traceable is TRUE if the Time Traceable is TRUE, otherwise it is FALSE.

PTPv1 Configuration and Status

The default PTPv1 configuration settings in the Unison are shown below. If you need to modify these settings then you will need to reconfigure the PTPv1 subsystem. You may perform the configuration from either a **`telnet`** or **`ssh`** session, or the local RS-232 console. Default PTPv1 settings are:

PTP Preferred:	TRUE
PTP Sync Interval:	Two seconds
PTP Subdomain Name:	DFLT
PTP Time Mode	UTC
PTP TTL	1

PTPv1 Configuration Using the Network or Serial Port

The **`ptpconfig`** command starts an interactive shell script that will allow you to configure the PTPv1 subsystem of the Unison. You will be prompted to set the PTPv1 parameters as follows:

Preferred State:	TRUE or FALSE
Sync Interval:	1,2,8,16, or 64 seconds
Subdomain Name:	DFLT, ALT1, ALT2, or ALT3

PTP Time Mode:	UTC or PTP
PTP TTL:	1-255

One file is modified, */etc/ptp.conf*. This is a non-volatile stored file in the FLASH disk */boot/etc* directory. You must reboot the Unison after running this script for the changes to take effect.

The following is a transcript of the question and answer configuration utility provided by ptpconfig. The user entered parameters are underlined:

Unison GPS(root@cntp)-> ptpconfig

```
*************************************************************************
******************** Precision Time Protocol Configuration ***************
*************************************************************************
*
*    This script will allow you to configure the ptp.conf file
*    that controls the PTP daemon operation.
*
*    You will be able to configure the PTP sync_interval, preferred state,
*    subdomain_name, and time_mode.
*
*    The changes you make now will not take effect until you re-boot the
*    Unison . If you make a mistake, just re-run ptpconfig prior to
*    re-booting.
*
*    You will now be prompted for the necessary set up parameters.
*
*************************************************************************

---PTP preferred Configuration

Set PTP preferred (TRUE, FALSE) TRUE

---PTP sync_interval Configuration

Set the PTP sync_interval in seconds (1,2,8,16,64) 2

---PTP subdomain_name Configuration

Set the PTP subdomain_name (DFLT, ALT1, ALT2, ALT3) DFLT

---PTP time_mode configuration

Set the PTP time_mode (UTC or PTP) PTP

---PTP ttl configuration

Set the PTP ttl value (1-255) 1


*************************************************************************
*
*    The Unison Precision Time Protocol IEEE-1588 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:

```
shutdown -r  now
```

PTPv1 Status Using the Network or Serial Port

The **gptpstat** command allows the user to query the status of the PTPv1 subsystem. The ptpd daemon running on the system updates the */var/log/ptp.monitor* every five seconds under normal operation. This logfile is parsed and formated to provide the status string having these fields:

```
PTPMODE CKID Stratum SSS PPPPP SDOM II LL TMD V TTL
```

Where:

PTPMODE	is the PTP port state, either Master or Passive.
CKID	is the sync identifier, either ATOM or GPS.
SSS	is the PTP stratum, either 1, 2, 3 or 255, where 1 implies an error of < 25 ns, 2 implies < 100 ns, 3 implies > 100 ns, and 255 is the unsynchronized state.
PPPPP	is the PTP preferred master setting, either True or False.
SDOM	is the PTP subdomain, one of DFLT, ALT1, ALT2 or ALT3.
II	is the PTP sync update interval, one of 1,2,8,16, or 64, in seconds.
LL	is the PTP leap second setting, one of 59, 60, or 61, where 59 implies that the last minute of the current day will have 59 seconds (leap second deletion), and 61 implies that the last minute of the current day will have 61 seconds (leap second insertion).
TMD	is the PTP time epoch either PTP or UTC.
V	is the PTP protocol version, only version 1 is implemented.
TTL	is the PTP multicast TTL, 1-255.

PTPv1 Operation

The Unison is configured as an IEEE-1588 Grandmaster Clock. Verify that the network settings have been configured and tested using **netconfig**. Once the network has been configured the Unison will begin to transmit PTP Sync messages to the slave clocks.

The PTP sync message and status report from the Unison is dependent on the status of the clock configuration including the oscillator type and GPS Subsystem.

The Port State will report either MASTER or PASSIVE. MASTER is reported when the clock is locked to GPS and the best master clock algorithm (BMC) designates this clock as the MASTER.

The port_state will report PASSIVE if the clock has never locked to GPS or if the BMC designates this clock as anything other than the MASTER.

The Sync Identifier will report either GPS, or ATOM. GPS is reported when the system starts and when locked to GPS. ATOM is only reported when the oscillator type in the Unison is a Rubidium.

The PTP Stratum will report either 1, 2, 3 or 255. The identifier and the calculated offset to UTC determines the PTP Stratum as shown below:

Identifier	PTP Stratum	Offset to UTC
GPS or ATOM	1	< 25 nanosecs
GPS or ATOM	2	< 100 nanosecs
GPS or ATOM	3	> 100 nanosecs
GPS or ATOM	255	Never locked

The PTP leap_59 and leap_61 report either TRUE or FALSE. FALSE is reported when no leap insertion or deletion is pending. The leap_61 reports TRUE on the day of a leap second insertion. The leap_59 is TRUE on the day of a leap second deletion.

The PTP Time Mode is user configured, either UTC or PTP. When UTC time mode is configured the clock transmits the UTC epoch. When the time mode is PTP the clock transmits the PTP epoch (TAI). See ***About the PTP Second and UTC Time*** below for more information.

The PTP Multicast TTL value is factory set to the IEEE-1588 standard that defines TTL=1. The TTL value may be set to any value from 1-255. When set to any value other than 1, you must also configure the PTP Slave accordingly.

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 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.

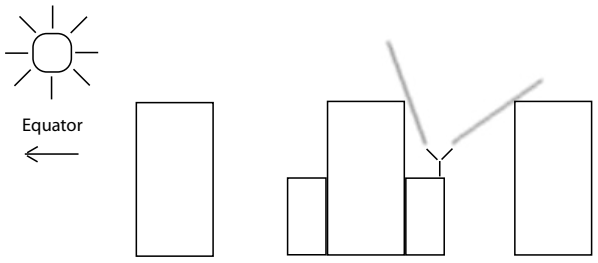
Appendix *I*

Installing the GPS Antenna

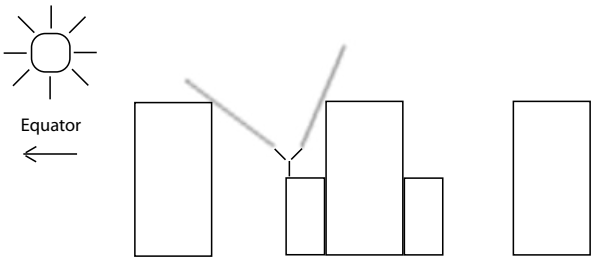
This appendix contains guidelines for installing the GPS antenna. The majority of this appendix is devoted to rooftop installations. The last section contains information on a window-mount installation.

Antenna Location

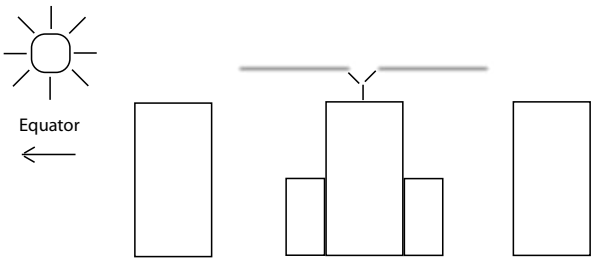
The location of the antenna must be chosen based on having as clear a view of the sky as possible. Any obstructions such as buildings, large metal objects or other antennas, and even trees, will limit the performance of the GPS antenna. The antenna should also be located away from overhead power lines or circuits, for safety reasons. The illustration below shows some examples of good and bad antenna mounting locations.



POOR ANTENNA LOCATION - blocked view of the sky plus it is on the side of the building facing away from the equator.



BETTER ANTENNA LOCATION - blocked view of the sky but it is on the side of the building facing the equator.



BEST ANTENNA LOCATION - full view of the sky.

GPS Antenna Kit

The time server ships with a free GPS Antenna Kit which includes 50 feet (15 meters) of antenna cable. This amount of cable is sufficient for the majority of GPS antenna installations. Longer cable runs can also be accommodated. Below is a list of the items in a typical GPS Antenna Kit, part number 0610-0007-001:

- GPS Antenna (part #0502-0012-000)
- Antenna Mounting Adaptor (part #0602-0035-000)
- PVC Mounting Pipe (part #0100-0009-018)
- Hose Clamps (part #0100-0008-000)
- 50 feet of RG-59U (Belden 9104) Cable/TNC Male (part #0600-0013-050)
- GPS Antenna Inside Window Mount Kit (part #0608-0002-001)

Following is the Installation Guide for a rooftop mount that is included with the antenna kit.

INSTALLATION GUIDE

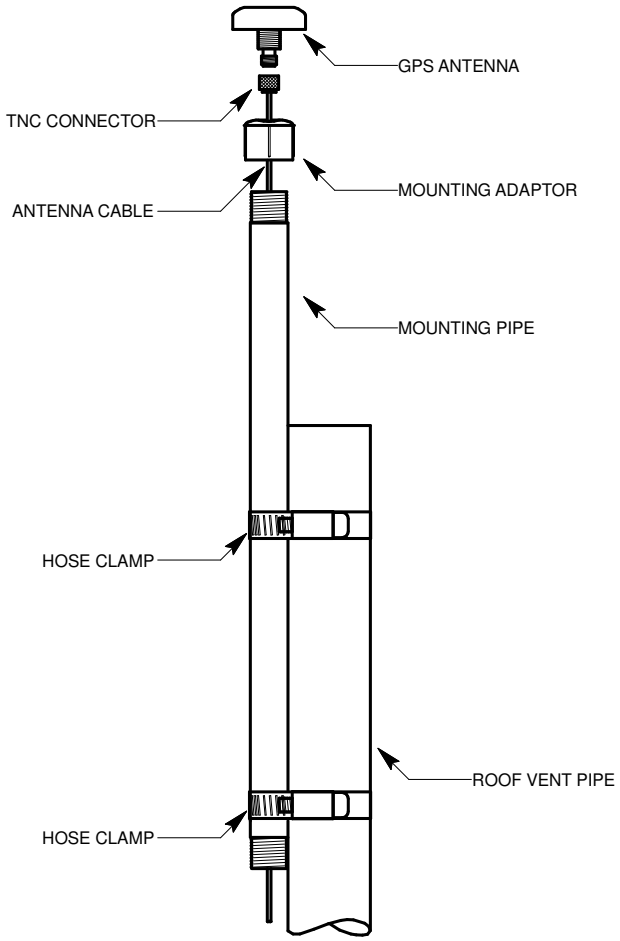
GPS Antenna Rooftop Mounting Guidelines

Locating Mounting Site

Most ideal mounting location is one with unobstructed clear view of the sky. If mounted on building side, locate on side closest to earth equator (South if in Northern Hemisphere). Mount as close to vertical as possible. Mount away from other radiating antennas if possible.

Antenna Installation Using Supplied Mounting Kit

The ¾-16 nuts and metal flat washer are not used with this mounting method -- remove from antenna, if present. Run cable-end through the mounting pipe and through the mounting adaptor as shown. Connect cable TNC connector to antenna connector. Thread the mounting adaptor onto the mounting pipe and thread the base of the antenna into the mounting adaptor. Tighten firmly against rubber gasket on bottom of antenna. Excessive force is not necessary and may damage threads. Do not use thread-locking compound. Secure mounting pipe to available pipe or roof structure using hose clamps as shown. Run the antenna cable into the building and connect to instrument GPS antenna connector.



5050-0015-000 1 of 1 18Dec2007

Long Cable Runs

Most GPS Time Servers are installed with only 50 feet (15 meters) of antenna cable. However, there are many circumstances where 50 feet is inadequate. EndRun can accommodate a cable length of up to 1000 feet using a combination of low-loss cable and preamplifiers.

Recommended Cable

The factory-supplied GPS cable is RG-59 Belden 9104 or Belden 1505A, depending on length. If you are responsible for the GPS installation and you are supplying the cable then you need to make sure it is comparable with less than 10 dB of loss at 1.5 GHz. Choosing a cable type that is different can cause a myriad of GPS reception problems. If the cable length is less than 700 feet then Belden 9104 is appropriate. If the cable length is greater than 700 feet then Belden 1505A is the cable of choice. You will also need preamplifiers if the cable length is greater than 250 feet. See the chart below for details.

Using GPS Preamplifiers

EndRun produces a GPS Preamplifier which is a very high-performance, low-noise, inline amplifier for difficult GPS signal environments and long cable runs (greater than 250 feet of factory-supplied cable). The following table shows the number of preamplifers we recommend for each GPS antenna installation using our GPS receiver and our factory-supplied cable. Installations using other cable types may have different preamplifer requirements.

Cable Length	Cable Type	Number of Preamplifiers
Up to 250 feet (76 meters)	RG-59 Belden 9104	0
251 to 500 feet (77 to 152 meters)	RG-59 Belden 9104	1
501 to 700 feet (153 to 213 meters)	RG-59 Belden 9104	2
701 to 750 feet (214 to 228 meters)	RG-59 Belden 1505A	2
751 to 1000 feet (229 to 305 meters)	RG-59 Belden 1505A	3

The following two pages show the Installation Guide for installing a rooftop-mounted antenna with GPS preamplifer.

INSTALLATION GUIDE

GPS Antenna Rooftop Mounting Guidelines
(with In-Line Amplifier)

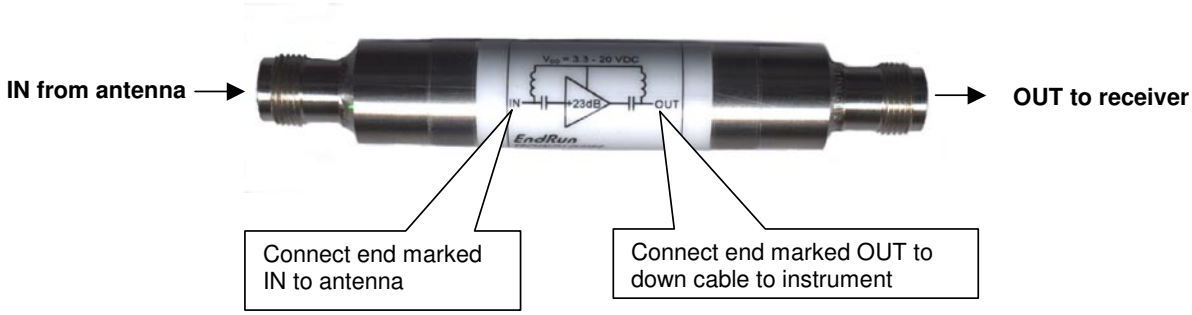
Locating Mounting Site

Most ideal mounting location is one with unobstructed clear view of the sky. If mounted on building side, locate on side closest to earth equator (South if in Northern Hemisphere). Mount as close to vertical as possible. Mount away from other radiating antennas if possible.

Antenna Cable and Mast Installation

Locate end of antenna cable with TNC connector. Run this end through the antenna mast and connect to the in-line amplifier (end marked output). Connect short cable (12 inches long) between in-line amplifier (end marked input) to the base of the antenna as shown. Thread the antenna mast into the base of the antenna. Excessive force is not necessary and may damage threads. Do not use thread locking compound. Secure the antenna mast to available pipe or roof structure using hose clamps as shown. Run the antenna cable into your building and connect to the rear of the instrument TNC connector identified as GPS Antenna.

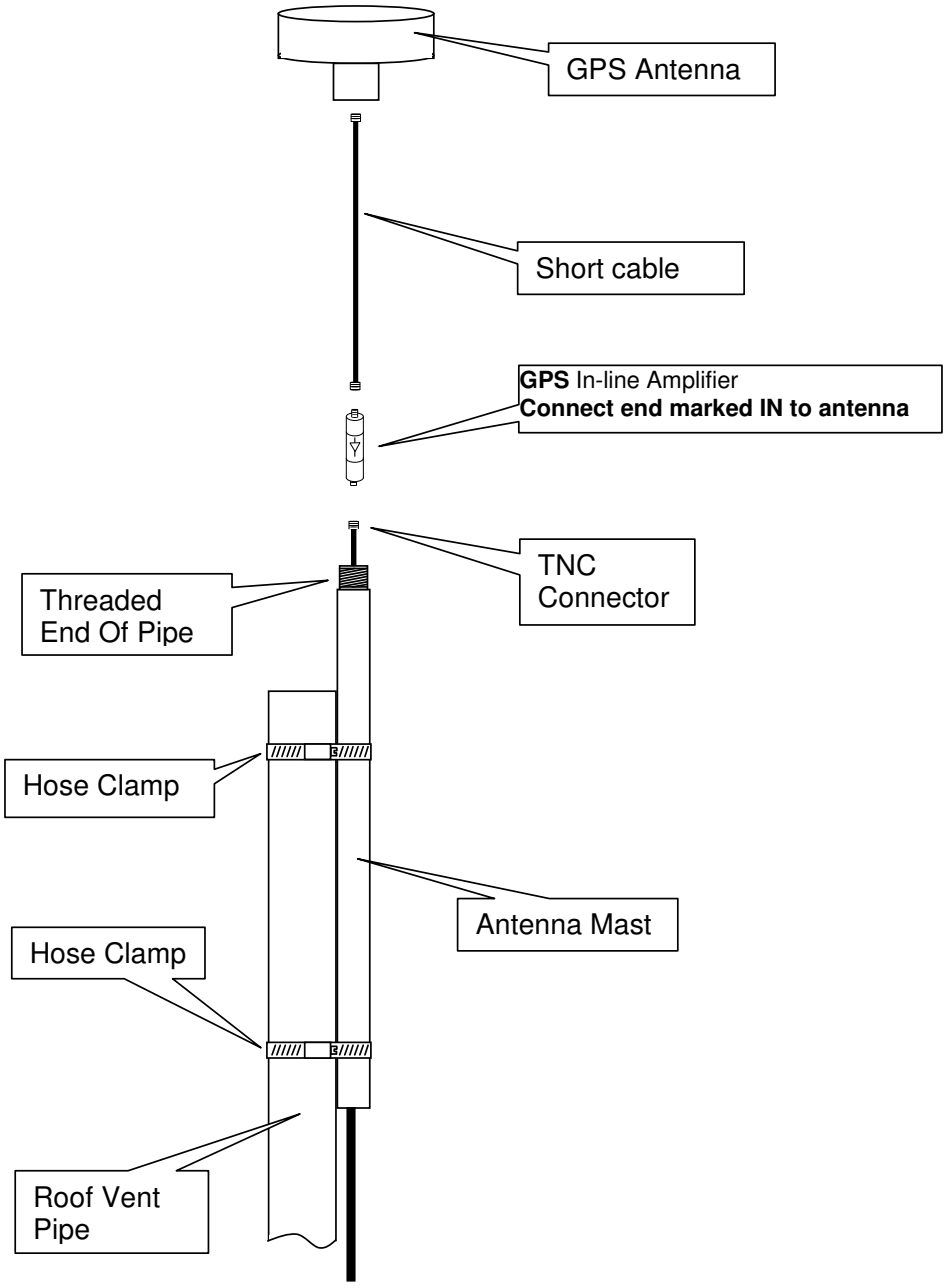
IMPORTANT! Observe polarity when connecting the GLna in-line amplifier. Connect as illustrated below:



5050-0004-000 1 of 1 05FEB2010

INSTALLATION GUIDE

GPS Antenna Rooftop Mounting Guidelines
(with In-Line Amplifier)



5050-0004-000 2 of 2 05FEB2010

Other Accessories

Lightning Arrestor

A lightning arrestor helps protect your GPS installation from damage due to lightning strikes. It is designed to pass the DC voltage that is needed to power the antenna and/or preamps without degrading the GPS signal. It is installed between the antenna and the receiver where the cable enters the building, near an earth-ground. You need to bond the lightning arrestor to the earth-ground.

Splitters

Splitters are used when two time servers are sharing one antenna installation. The smart GPS Splitter supplied by EndRun is a one-input, two-output device. In the normal configuration, one of the splitter RF outputs (J1) passes DC from the connected GPS receiver through the splitter to the antenna, allowing the GPS receiver to power both the antenna and the splitter amplifier. The other RF output (J2) is DC loaded with a 200-ohm resistor to simulate the antenna current draw.

When installing a splitter keep these points in mind:

1. The splitter must be DC-blocked on one leg. The GPS receivers in the two time servers output 5 VDC up the coax to power the GPS antenna's build-in preamp. You do not want these power sources tied together.

2. The DC block leg should have DC load to mimic a GPS antenna load. This way you will not get a false alarm from the receiver's antenna load sensor. You can prevent this false alarm from causing a system fault in the time server by using the **`setantfltmask`** and **`antfltmask`** commands. See information in ***Chapter 5 - Control and Status Commands***.

3. The splitter supplied by EndRun has a built-in preamplifier to compensate for signal loss through the splitter. If using a splitter other than the one supplied by EndRun you may need to compensate for splitter signal loss by using a separate GPS preamplifier.

Mounting Inside A Window

For GPS time servers, it is possible to mount the GPS antenna inside a window and have it perform adequately. Avoid windows with metallic film coating that will inhibit GPS signals and ensure that the window has a good view of the sky. If you are in the Northern Hemisphere then a south-facing window is best and vice-versa for the Southern Hemisphere.

Your Unison needs to calculate its position in order to operate properly. It only needs to do this once and needs to be able to see four satellites all at the same time. If your Unison has a limited view of the sky it may not be able to see the required four satellites so you will need to manually enter your position. See ***Appendix D - GPS Reference Position*** for instructions.

Because of the reduced sky visibility that goes with a window-mount installation, your time server may go through many hours without locking to a GPS signal. This is fine as long as it locks at least once every 24 hours. If the time server goes longer than 24 hours without locking then it will stop serving Stratum 1 time. An OCXO upgrade will allow the time server to go for much longer than 24 hours without receiving a GPS signal and is extra insurance for window-mount installations.

The following page shows the Installation Guide for window-mounting the antenna..

INSTALLATION GUIDE

GPS Antenna Inside-Window Mounting Guidelines

The double-sided tape supplied in this kit can be used to mount the GPS antenna to the inside of a window. There is enough tape included in the kit to try up to three different mounting locations (The tape is not typically reusable.). Note that the tape does not exhibit full adhesive strength until pressed between two flat surfaces. It can be removed by firmly twisting the antenna clockwise and/or counter-clockwise to break the seal. Once the surfaces are separated, the tape can be removed by lifting one end and slowly peeling it back with a steady force.

STEP 1

Separate antenna from outside-mounting kit. The ¾-16 nuts and metal flat washer are not used with this mounting method -- remove from antenna, if present.

STEP 2

Cut off two strips of tape, each approximately 1" long. Note clear backing on one side of tape.

STEP 3

Press non-backed side onto flat surface of antenna approximately as shown in Figure 1.

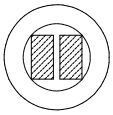


FIGURE 1

STEP 4

Remove backing from tape and position antenna in front of mounting location. Firmly press antenna, seating exposed tape against dust-free window surface.

STEP 5

Re-connect cable to antenna. Route cable to prevent kinking, avoiding sharp bends and providing adequate strain relief. Figures 2 and 3 illustrate possible installation methods using materials supplied with this kit. To mount cable-tie holder on window, remove self-adhesive and backing, exposing nylon surface of holder. Use 1" length of double-sided tape to attach holder to window or aluminum frame as shown in Figure 3. Use of the double-sided tape provides a sun/heat-resistant, removable mounting method. To mount holder on rough frame or wall surface, use the self-adhesive as-is by simply removing the backing.

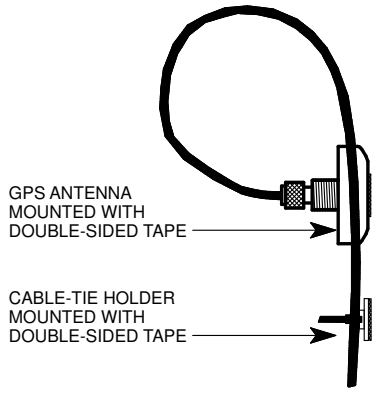


FIGURE 2

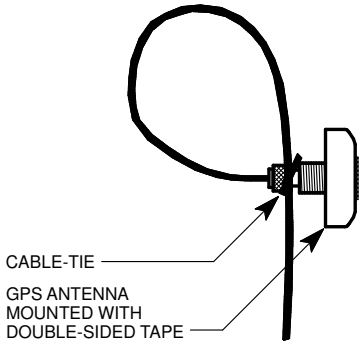


FIGURE 3

5050-0016-000 1 of 1 20Dec2007

Appendix J

Specifications

GPS Receiver:
L1 Band – 1575.42 MHz
8 Channels, C/A Code

Antenna:
TNC jack on rear panel, Z_{in} = 50Ω
Integral +35 dB gain LNA with bandpass filter for out-of-band interference rejection.
Rugged, all-weather housing capable of operation over –40°C to +85°C temperature extremes.
Mounting via 18" long, ¾" PVC pipe with stainless steel clamps.
50' low-loss RG-59 downlead cable standard.
Extension cables and low noise pre-amplifiers are available as options.

Local Oscillator:
TCXO is standard ($2.5x10^{-6}$ over -20° to 70°C).
Option: Medium-Stability OCXO ($4x10^{-9}$ over 0 to 70°C).
Stratum 1 Holdover Performance: 24 Hours - TCXO
35 Days - MS-OCXO

Time to Lock:
< 5 minutes, typical (TCXO).
< 10 minutes, typical (MS-OCXO).

Network I/O:
Rear panel RJ-45 jack
AMD PC-Net Fast III 10/100Base-T ethernet

System Status Indicator:
Sync LED: Green LED pulses to indicate GPS acquisition and lock status.
Network LED: Amber LED indicates network activity.
Alarm LED: Red LED indicates a fault condition.

Maintenance Console:
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". Pinout is shown below.
Note: For operational details see ***Chapter 5 - Control and Status Commands***.

Unison DB9M Pin	Signal Name
1	Not Connected
2	Receive Data (RX)
3	Transmit Data (TX)
4	Data Terminal Ready (DTR)
5	Ground
6	Data Set Ready (DSR)
7	Request To Send (RTS)
8	Clear To Send (RTS)
9	Not Connected

Synchronization Accuracy:

GPS Receiver Accuracy: <30 nanoseconds to GPS Time when locked.*
NTP Timestamp Accuracy: <10 microseconds @ 200 packets/second (200,000 clients).
NTP Client Synchronization Accuracy: Network factors can limit LAN synchronization accuracy to 1/2 to 2 milliseconds, typical.
* <100 nanoseconds to UTC. Constraints in the official GPS specification prohibit claiming an accuracy to UTC better than 100 nanoseconds.

Supported IPv4 Protocols:

SNTP, NTP v2, v3, v4 and broadcast/multicast mode; MD5 authentication and autokey
SSH 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
HTTP

Supported IPv6 Protocols:

SNTP, NTP v2, v3, v4 and broadcast/multicast mode; MD5 authentication and autokey
SSH server with “secure copy” utility, SCP
SNMP v1, v2c, v3 with Enterprise MIB
TIME and DAYTIME server
SYSLOG
Note: See ***Chapter 6 - IPv6 Information*** for details.

Optional PTP/IEEE-1588 Grandmaster:

IEEE-1588-2008 (v2) and IEEE-1588-2002 (v1)
PTP Timestamp Resolution: 1 microsecond.
PTP Slave Synchronization Accuracy to the Grandmaster: 10 microseconds, typical, network topology dependent.
Note: See ***Appendix H - Precision Time Protocol*** for more information.

Power:
90-264 VAC, 47-63 Hz, 0.5 A Max. @ 120 VAC, 0.25 A Max. @ 240 VAC
110-370 VDC, 0.5A Max @ 120 VDC
3-Pin IEC 320 on rear panel, 2 meter line cord is included.

DC Power (option):
38-72 Vdc, 1.5A 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.)

Size:

Chassis:	1.75"H x 17.0"W x 10.75"D
Antenna:	3.5" Dia. x 2.5" H
Weight:	< 5 lb. (2.70 kg.)

Environmental:

Operating Temperature:	0° to +50°C
Operating Humidity:	0 to 95%, non-condensing
Storage Temperature:	-40° to +85°C
Antenna Operating Temperature:	-40° to +85°C

Optional Outputs:
See ***Chapter 2 - Physical Description*** for more information on these outputs.

1 PPS: Positive TTL pulse @ 50Ω or RS-422 levels.
Width: User-selectable to 20 us, 1 ms, 100 ms, 500 ms.
Accuracy: < 30 nanoseconds to GPS Time when locked.*
Stability: TDEV < 20 ns, $\tau < 10^5$ seconds.
Connector (TTL): Rear-panel BNC jack labeled "1 PPS".
Connector (RS-422): Rear-panel DB-9M jack labeled "1PPS RS-422".
Pinout (RS-422): Pin 3 is +signal. Pin 6 is -signal. Pin 5 is GND.
* <100 nanoseconds to UTC. Constraints in the official GPS specification prohibit claiming an accuracy to UTC better than 100 nanoseconds.
Note: To change the pulse width refer to the **`cpuopts`** and **`cpuoptsconfig`** commands in ***Chapter 5- Control and Status Commands***.

AM Code: 1 Vrms @ 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 "AM CODE".
Note: To change the time code format refer to the **`cpuopts`** and **`cpuoptsconfig`** commands in ***Chapter 5 - Control and Status Commands***.

Prog TTL Pulse Rate: Positive TTL pulse @ 50Ω on BNC jack.
User-Selectable Output Type: On-time pulse rate, a digital time code or synthesized rate.
Pulse Rate: User selectable to 1, 10, 100, 1K, 10K, 100K, 1M, 5M, 10M PPS, 1PPM, 1PP2S.
Duty Cycle: 50% except 1PPS which mimics the standard 1PPS Output.
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^2$ seconds, $\sigma_y(\tau) < 10^{-7}/\tau$ for $\tau > 10^2$ seconds.
Synthesized Rate (option): 1PPS to 10 MPPS in 1PPS steps with optional DDS upgrade.
Connector: Rear-panel BNC jack labeled "PROG TTL".
Note: To change the output selection refer to the **`cpuopts`** and **`cpuoptsconfig`** commands in ***Chapter 5 - Control and Status Commands***.

Alarm: 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 strip labeled "ALARM".

Serial Time: Output only port at RS-232 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.
Connector: Rear-panel DB-9M connector labeled "SERIAL TIME".
Pinout (RS-232): Pin 3 is Transmit Data. Pin 5 is GND.
Pinout (RS-422): Pin 3 is +Transmit Data. Pin 6 is -Transmit Data. Pin 5 is GND.
Note: See ***Appendix G - Serial Time Output*** for more information.

Fixed Rate: Positive TTL pulse @ 50Ω.
Rate: Preset at Factory and cannot be changed.
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Stability: $\sigma_y(\tau) < 10^{-9}$ for $\tau < 10^2$ seconds, $\sigma_y(\tau) < 10^{-7}/\tau$ for $\tau > 10^2$ seconds.
Connector: Rear-panel BNC jack labeled with appropriate rate such as "10MPPS".

CE/FCC Compliance:

RTTE Directive 99/5/EC
Low Voltage Directive 73/23/EC
EMC Directive 89/336/EC
With Amendment 93/68/EC

Supplementary Compliance Data:

- **Safety:** EN 60950;1992, A1,A2: 1993, A3: 1995, A4: 1997, A11:1998
- **EMC:** EN 55024:1998 w/ A1:2000 and A2:2003, EN61000-3-2:2000, EN61000-3-3:1995 w/ A1:2001, EN55022:1998 Class A, VCCI (April 2004) Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A.

DECLARATION OF CONFORMITY

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

Manufacturer's Name: **EndRun Technologies**

EndRun TECHNOLOGIES

Manufacturer's Address: **1360 North Dutton Avenue, Suite 200**
Santa Rosa, CA 95401, U.S.A.

DECLARES THAT THE PRODUCT

Product Name: **(1) Network Time Servers and (2) Time & Frequency Standards**

Model Number: **(1) Tempus LX GPS, Tempus LX CDMA, Unison GPS, Unison CDMA; and (2) Tycho GPS, Tycho CDMA**

CONFORMS TO THE FOLLOWING EUROPEAN DIRECTIVES

RTTE Directive 99 / 5 / EC
Low Voltage Directive 73 / 23 / EC
EMC Directive 89 / 336 / EC
With Amendment 93 / 68 / EC

Supplementary Information:

Safety : **EN 60950: 1992, A1,A2: 1993, A3: 1995, A4: 1997, A11:1998**

EMC: **EN 55024:1998 w/ A1:2000 and A2:2003, EN61000-3-2:2000, EN61000-3-3:1995 w/ A1: 2001, EN55022:1998 Class A, VCCI (April 2004) Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A**

Year Mark First Applied: **2004**

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

Place: Santa Rosa, California USA

Signature:

Date: December 22, 2004

Full Name: David J. Lobsinger

Position: V. P. Hardware Engineering

Special Modifications

Changes for Customer Requirements

From time to time EndRun Technologies will customize the standard Unison Network 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.

EndRun TECHNOLOGIES
"Smarter Timing Solutions"
2270 Northpoint Parkway
Santa Rosa, CA 95407
TEL 1-877-749-3878
FAX 707-573-8619
www.endruntechnologies.com