Smarter
Timing
Solutions

EndRun TECHNOLOGIES

Tempus Gntp Network Time Server

User's Manual

Tempus Gntp Network Time Server

User's Manual

1360 North Dutton Avenue #200
Santa Rosa, California USA 95401
Phone 707-573-8633 • Fax 707-573-8619

Preface

Thank you for purchasing the Tempus Gntp 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 Tempus Gntp 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 base stations, and calibration laboratories.

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

About this manual

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

Introduction – The Tempus Gntp, how it works, where to use it, its main features.
Basic Installation – How to connect, configure and test your Tempus Gntp with your network.
Client Set-Up – Two sections; one for Unix-like platforms and one for Windows NT/2000.

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.

Trademark acknowledgements

Tempus Gntp User's Manual **Revision 2**

Part No. USM3012-0000-000 **Sept 2003**

Warranty

This product, manufactured by EndRun Technologies, is warranted against defects in material and workmanship for a period of two 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 EndRun Technologies and EndRun Technologies shall pay shipping charges to return the product to Buyer. However, Buyer shall pay all shipping charges, duties, and taxes for products returned to EndRun Technologies from another country.

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 standard warranty may be extended beyond the standard two-year period. A record of warranty extensions is documented on the sales order for the product purchased. All other conditions of the standard warranty apply for the extended period.

Limitation of Warranty

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

NO OTHER WARRANTY IS EXPRESSED OR IMPLIED. ENDRUN TECHNOLOGIES SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND 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 fix or 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.

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.

Table of Contents

Introduction 1

GPS Timing–How it Works 1

Where to Use It 2

Main Features 3

Basic Installation 5

Tempus Gntp Physical Description 6

Installing the Tempus Gntp 8

Mount the Tempus Gntp 8
Connecting DC Power (option) 9
Connecting and Configuring Ethernet 9
Configuring Ethernet with the Front-Panel Keypad 9
Configuring Ethernet with the Serial Port 10
Connect the RS-232 Serial I/O Port 10
Test the Serial Port 10
Using netconfig to Set Up Your IP 13
Verify Network Configuration 15
Check Network Operation 16
Using Telnet 17
Using SSH 18

Configuring the Network Time Protocol 18

Configuring NTP Using the Front-Panel Keypad 19
Configuring NTP Using the Network Interface or Serial Port 19

Setting Up NTP Clients on Unix-like Platforms 21

Basic NTP Client Setup 22

Configure NTP 22

MD5 Authenticated NTP Client Setup 23

Create the ntp.keys file 23
Configure NTP 24

Broadcast/Multicast NTP Client Setup 25

Configure NTP 25

Setting Up NTP Clients on Windows NT 4.0/2000 27

Basic NTP Client Setup 28

Configure NTP 28

MD5 Authenticated NTP Client Setup 29

Create the ntp.keys file 29
Configure NTP 30

Broadcast/Multicast NTP Client Setup 31

Configure NTP 32

Front-Panel Keypad and Display 35

Display Description 35

Keypad Description 35
Display and Keypad Operation 36
Traversing the Display Structure 36
Editing 36
Keypad EDIT Lockout 37
Using Help 37
Detailed Display Descriptions 37
Time/Status 37
Main Menu 38
Receiver Status 39
Reference Position 40
GPS Dynamic Mode 41
Clock Menu 41
Time Mode 41
Local Offset 41
Hours Display 41
Daylight Savings Time (DST) 42
Display 42
Network 43
NTP Menu 44
NTP Status 44
NTP Setup 44
Firmware 45
About 46
Shortcut Menu 46
Control and Status Commands 47
General Linux Shell Operation 47
Available User Commands 48
Detailed Command Descriptions 49
accessconfig 49
gntpenableupgrade 50
gntphwaddr 50
gntposctype 50
gntppasswd 50
gntprootfs 50
gntpstat 51
gntptimemode 52
gntptimemodeconfig 52
gntpversion 53
gpsdynmode 53
gpsrefpos 53
gpsstat 54
gpstrkstat 57
gpsversion 57
inetdconfig 57
kplockstat 57
lockoutkp 58
netconfig 58
ntpconfig 58
setgpsdynmode 59
setgpsrefpos 59
unlockkp 59
updatelilo 60
Null Modem Adapter Cable 61
Security 63
Linux Operating System 63

OpenSSH 65
Network Time Protocol 66
Upgrading the Firmware 67
What You Need To Perform the Upgrade 67
Performing the Tempus Gntp Upgrade 67
Recovering from a Failed Upgrade 70
Performing the GPS Upgrade 70
Problems with the GPS Upgrade 71
Simple Network Management Protocol 73
SNMPv3 Security 73
Enterprise Management Information Base (MIB) 74
Invocation of the SNMP daemon 74
Quick Start Configuration – SNMPv1/v2c 75
Configuring SNMPv1 Trap Generation 75
Configuring SNMPv2c Notifications and Informs 76
Configuration of SNMPv3 76
GPS Reference Position 79
Obtaining Reference Positions 79
Using a Handheld GPS Receiver 79
Using Geodetic Databases 79
Geodesy 80
WGS-84 Positions 81
Procedure 81
Lithium Battery Replacement 85
Time Figure of Merit (TFOM) 87
Specifications 89

Chapter 1

Introduction

The Tempus Gntp 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 Tempus Gntp is composed of a Praecis Gntp Global Positioning System (GPS) time and frequency engine, an IBM-PC compatible single board computer with fanless, convection-cooled 133 MHz CPU with integral ethernet interface, a graphic vacuum-fluorescent display, a keypad, and a power supply. Non-volatile storage of the embedded Linux operating system and the Tempus Gntp application software on the single board computer is via a solid state FLASH disk.

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

GPS satellite transmissions must be synchronized.

The time and frequency engine in the Tempus Gntp 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-ar-

rival 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.

GPS time is based on an ensemble of cesium beam atomic frequency standards.

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 contains redundant cesium beam or rubidium vapor atomic frequency standards.

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.

Spread spectrum modulation allows near perfect extraction of the timing information.

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 Tempus Gntp does just that.

Where to Use It

GPS is globally available.

Since signals from the GPS satellites are available at all locations on the globe, you may deploy the Tempus Gntp 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 Tempus Gntp can maintain acceptable network synchronization accuracy for about a day without GPS reception, by flywheeling on its standard temperature compensated crystal oscillator.

Just about any computer network using TCP/IP can use the Tempus Gntp.

Because the Tempus Gntp 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 Tempus Gntp 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 Præcis Gntp 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 Præcis products available to our customers free of charge.

Chapter 2

Basic Installation

This chapter will guide you through the most basic checkout and physical installation of your Tempus Gntp. 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 Tempus Gntp 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

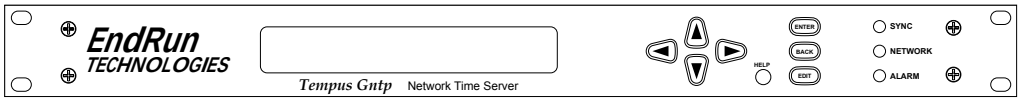
Unpack and check all the items using the following check list. Contact the factory if anything is missing or damaged.

The Tempus Gntp Hardware Pack (part # 4008-0000-000 or # 4008-variant) contains:

- Tempus Gntp (part # 3012-0000-000 or # 3012- variant)
- Tempus Gntp User's Manual (part # USM3012-0000-000)
- IEC 320 AC Power Cord (part # 0501-0003-000)
  (This part will not be present if using the DC power option.)
- DB-9F to DB-9F Null Modem Serial I/O Cable (part # 0501-0002-000)
- RJ-45 to RJ-45 CAT-5 patch cable, 2 meters (part # 0501-0002-000)
- Antenna/cable assembly (part # 0501-0000-000)

Tempus Gntp Physical Description

Front Panel

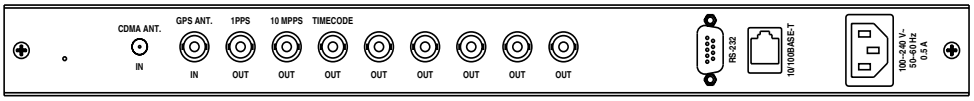


Sync Status LED — This green LED flashes to indicate synchronization status.

Network Status LED — This amber LED illuminates when the 10/100Base-T RJ-45 connector is connected to the network and flashes when receiving or transmitting packets..

Alarm Status LED — This red LED illuminates briefly at power-up, and thereafter whenever a serious fault condition exists.

Rear Panel



GPS ANT. Jack — This BNC connector mates with the downlead cable from the external antenna.

1PPS Jack — This BNC connector provides the optional 1PPS TTL output.

10 MPPS Jack — This BNC connector provides the optional 10 MPPS TTL output.

Timecode Jack — This BNC connector provides the optional IRIG-B time code output.

10 MHz, 5 MHz, 1 MHz, 5 MPPS, 1 MPPS, Time Code TTL Jacks — These BNC connectors are additional optional outputs and may or may not be present on your unit.

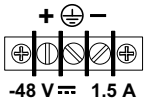
RS-232 Serial I/O Jack — This DB-9M connector provides the RS-232 serial I/O console interface to the Tempus Gntp. This console allows the user to initialize and maintain the Tempus Gntp. A null modem adapter is required to connect

this port to another computer.

10/100Base-T Jack — This RJ-45 connector mates with the ethernet twisted pair cable from the network.

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 Tempus Gntp will work in your desired location:

1. Screw the BNC plug on the end of the antenna cable onto the BNC antenna input jack on the chassis rear panel of the Tempus Gntp.

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 Tempus Gntp.

NOTE

After power is applied, the front-panel display will remain blank for approximately 60 seconds while the Tempus Cntp is initializing.

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.

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 procede 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 Tempus Gntp may be damaged and should be returned to the factory for repair or exchange.

Installing the Tempus Gntp

Mount the Tempus Gntp

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

Connecting 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 Tempus Cntp has a "floating" internal power supply, therefore either the positive or negative output of the DC power source can be referenced to earth ground.

CAUTION

Reverse connection at "+" and "-" power terminals can cause severe damage to power supply.

Connecting and Configuring Ethernet

Connect one end of the CAT-5 patch cable supplied with your Tempus Gntp 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 Tempus Gntp will attempt to configure the ethernet interface automatically via the Dynamic Host Configuration Protocol (DHCP). The Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp 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 either the front-panel keypad or the RS-232 serial I/O port. The following sections contain brief descriptions on how to do that.

Configuring Ethernet with the Front-Panel Keypad

Configuring your ethernet interface with the front-panel keypad is quite simple. After the unit has powered on, press the ENTER key once or twice until you see a display called Main Menu. Now press the RIGHT arrow key until the "Network" selection is highlighted. Press ENTER again. You will see the IP address, gateway and netmask settings displayed here. Press the EDIT key to modify these settings. The sequence of edit displays will guide you through the setup process. Press the HELP key at any time

to view context-sensitive help information. When you are finished the unit will reset. Skip to the section called "Check Network Operation" later in this chapter to continue with the basic installation procedures.

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 **`ash`** 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 Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp. To test serial communications with the Tempus Gntp 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 Tempus Gntp.

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

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 6 – *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 Tempus Gntp 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 Tempus Gntp. After about 20 seconds, your terminal should display a sequence of boot messages similar to these:

```
LILO
Low memory: 0262 Kb
boot:
```

These three lines are the Linux Loader (LILO) boot prompt. This prompt will timeout after 5 seconds and the Linux kernel and the factory default Tempus Gntp root file system will be loaded. When the Linux kernel is loaded from the FLASH disk into RAM a long list of kernel-generated, informational messages is displayed as the kernel begins execution and the various device drivers are initialized:

```
Loading TempusGntp_1.....................................................
Linux version 2.2.13-DOC (root@endrun1) (gcc version egcs-2.91.66 19990314/Linux
(egcs-1.1.2 release)) #14 Fri Jun 21 10:53:55 PDT 2002
Calibrating delay loop... 52.63 BogoMIPS
Memory: 28288k/32768k available (580k kernel code, 440k reserved, 532k data, 32k
init)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
CPU: Cyrix Cx486DX2
Checking 386/387 coupling... OK, FPU using exception 16 error reporting.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
PCI: PCI BIOS revision 2.10 entry at 0xfb180
PCI: Probing PCI hardware
Linux NET4.0 for Linux 2.2
Based upon Swansea University Computer Society NET3.039
NET4: Unix domain sockets 1.0 for Linux NET4.0.
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP
Starting kswapd v 1.5
Serial driver version 4.27 with no serial options enabled
ttyS00 at 0x03f8 (irq = 4) is a 16550A
ttyS01 at 0x02f8 (irq = 3) is a 16550A
ttyS03 at 0x02e8 (irq = 0) is a 16550A
RAM disk driver initialized:  16 RAM disks of 8192K size
Flash disk driver for DiskOnChip2000
Copyright (C) 1998,2000 M-Systems Flash Disk Pioneers Ltd.
Copyright (C) 2000 Lineo
DOC device(s) found: 1
Fat Filter Enabled
rtl8139.c:v1.07 5/6/99 Donald Becker http://cesdis.gsfc.nasa.gov/linux/drivers/
rtl8139.html
eth0: RealTek RTL8139 Fast Ethernet at 0xe400, IRQ 11, 00:d0:c9:91:c8:6f.
fl_geninit: registered device at major: 100
partition: 0: start_sect: 0, nr_sects: 3e30 Fl_blk_size[]: 1f18kb
partition: 1: start_sect: 0, nr_sects: 0 Fl_blk_size[]: 0kb
Partition check:
 fla: fla1 fla2 fla3 fla4
RAMDISK: Compressed image found at block 0
VFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 32k freed
```

```
INIT: version 2.76 booting
Parallelizing fsck version 1.15 (18-Jul-1999)
ext2fs_check_if_mount: No such file or directory while determining whether
/dev/msys/fla1 is mounted.
/dev/msys/fla1: clean, 35/80 files, 559/639 blocks
ext2fs_check_if_mount: No such file or directory while determining whether
/dev/msys/fla2 is mounted.
/dev/msys/fla2: clean, 15/32 files, 99/240 blocks
 fla: fla1 fla2 fla3 fla4
/dev/msys/fla1 o fla:n /boot type ext fla12 (rw)
 fla2 fla3 fla4
/dev/msys/fla2 on /logs type ext2 (rw)
/proc on /proc type proc (rw)
hwclock: Can't open /dev/tty1, errno=19: No such device.
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:

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

Then these messages are printed, in either case.

```
Activating 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!
PCM9340 CPU
Starting Keypad/Display Process
```

During this process, the factory default TempusGntp_0 root file system is loaded from FLASH disk to an 8MB ramdisk and the remainder of the boot process completes. At this point, the Tempus Gntp login prompt is displayed:

```
*******************************************************************************
*           Welcome to Tempus Gntp 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 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 Tempus Gntp and shows the software part number, version and build date:

```
Tempus Gntp 6010-0003-000 v 1.00 Wed May  9 14:17:44 UTC 2002
Tempus Gntp->
```

This last line is the standard Tempus Gntp shell prompt. The Tempus Gntp uses the **ash** shell, which is a reduced functionality, **bash**-compatible 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 6 – *RS-232 Serial I/O Port Signal Definitions* for the signal connections for the Tempus Gntp.

NOTE

You must use a null-modem cable or adapter if you are connecting the Tempus Gntp 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 Tempus Gntp, you may procede to configuring the network parameters. Then you can communicate with the Tempus Gntp over the network using **telnet** or **ssh** and synchronize your network computers to UTC using NTP.

Using netconfig to Set Up Your IP

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:

```
Tempus Gntp-> netconfig

*******************************************************************************
******************** Tempus Gntp Network Configuration  ***********************
*******************************************************************************
*                                                                             *
*   This script will configure the TCP/IP network parameters for your         *
*   Tempus Gntp. 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     *
*   Tempus Gntp, so if you make a mistake, just re-run this script before     *
*   re-booting.                                                               *
*                                                                             *
*   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 Tempus Gntp. 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 Tempus Gntp. 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 Tempus Gntp's current IP address, full hostname, and base hostname:
192.168.1.245       gntp.your.domain    gntp

---DOMAIN NAMESERVER(S) address setting

Will your Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp network configuration has been updated.            *
*                                                                             *
*             Please re-boot 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 Tempus Gntp and re-boot it. There are two ways to do this:

1. Cycle power to the Tempus Gntp.

2. Issue the shutdown with re-boot command at the shell prompt:

```
Tempus Gntp-> shutdown –r now
```

If you are using the RS-232 serial I/O port to communicate with the Tempus Gntp, you will be able to see the kernel generated boot messages when the unit re-boots. 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 Tempus Gntp 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 Tempus Gntp 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:**

```
Tempus Gntp-> ifconfig

eth0      Link encap:Ethernet  HWaddr 00:D0:C9:11:33:41
          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**:

```
Tempus 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 Tempus Gntp has been successfully configured to operate on your network and you are ready to check operation of the Tempus Gntp over the network. If not, you should re-check 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:

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

Once you have successfully established network communications with the Tempus Gntp, you may perform all maintenance and monitoring activities via **telnet** and **ftp**.

The Tempus Gntp provides both client and server operation using **telnet.** For security reasons as well as to reduce the memory footprint in the Tempus Gntp, only client operation is supported using **ftp**.

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 Tempus Gntp. Both of these protocols are supported in the Tempus Gntp via the OpenSSH implementations for Linux. Refer to Appendix A – *Security* for more information about the *secure shell* protocol and its configuration.

Using Telnet

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

```
**************************************************************************
*          Welcome to Tempus Gntp 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 Tempus Gntp and shows the software part number, version and build date:

```
Tempus Gntp 6010-0004-000 v 1.00 Wed May 16 14:17:44 UTC 2002
Tempus Gntp->
```

This last line is the standard Tempus Gntp shell prompt. The Tempus Gntp uses the **ash** shell, which is a reduced functionality, **bash**-compatible 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:

```
Tempus 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 Tempus Gntp, logging in directly as *root* is permitted. When you log in as *root* via a **ssh** session with the Tempus Gntp, this banner will be displayed:

```
*******************************************************************************
*            Welcome to Tempus Gntp 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 Tempus Gntp and shows the software part number, version and build date:

```
Tempus Gntp 6010-0003-000 v 1.00 Wed Jan 02 14:17:44 UTC 2002
Tempus Gntp->
```

This last line is the standard Tempus Gntp shell prompt. The Tempus Gntp uses the **ash** shell, which is a reduced functionality, **bash**-compatible 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.

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 Tempus Gntp 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 Tempus Gntp. If you need to modify the factory default Tempus Gntp MD5 keys (recommended) or set up broadcast/multicast operation, then you will need to re-configure the NTP subsystem.

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.

You may perform the configuration from either a **telnet** or **ssh** session, the front-panel keypad, or the local RS-232 console.

Configuring NTP Using the Front-Panel Keypad

To configure NTP using the front-panel keypad go to the Main Menu display. Press the RIGHT arrow key until the "NTP" selection is highlighted. Press ENTER again. Press the RIGHT arrow key to highlight "Setup" and press ENTER. From this display you can configure broadcast/multicast mode. You can also select previously configured MD5 authentication keys from this display. However, to configure new keys you will need to run **ntpconfig**.

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:

```
Tempus Gntp-> ntpconfig


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

---MD5 Keyfile Configuration

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

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

MD5 keys may contain from 1 to 31 ASCII characters.  They may not contain
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_Gntp

Writing key number: 2 and Key: Tempus_Gntp 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 Tempus Gntp.  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 Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp Network Time Protocol configuration has been updated.    *
*                                                                             *
*              Please re-boot now for the changes to take effect.             *
*                                                                             *
*******************************************************************************
*******************************************************************************
```

Chapter 3

Setting Up NTP Clients on Unix-like Platforms

To configure your Unix-like computer to use your Tempus Gntp, 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 Tempus Gntp 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

Although all the information is available at the above site, the following are excellent tutorials on setting up NTP and are easier to understand:

http://www.sun.com/solutions/blueprints/0701/NTP.pdf

http://www.sun.com/solutions/blueprints/0801/NTPpt2.pdf

http://www.sun.com/solutions/blueprints/0901/NTPpt3.pdf

Many problems may also be solved by the helpful people who participate in the Internet news group devoted to NTP:

news://*your_news_server*/comp.protocols.time.ntp

Three methods of using the Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp 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.

Re-start **ntpd** to have it begin using the Tempus Gntp server. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Tempus Gntp. 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 Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp on your network.
- Your Tempus Gntp has been configured to perform authentication either by factory default, or by running the **`ntpconfig`** shell script. The example Tempus Gntp 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 Tempus Gntp. You can **`telnet`** into your Tempus Gntp and start an **`ftp`** session with your client computer to send the Tempus Gntp'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 Tempus Gntp server using one of the trusted keys, in this case key # 1:

```
server 192.168.1.245 key 1
```

Re-start **ntpd** to have it begin using the Tempus Gntp server with MD5 authentication. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Tempus Gntp. 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 Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp on your network.
- Your Tempus Gntp has been configured to perform broadcasts or multicasts via the front-panel keypad or 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 Tempus Gntp 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 Tempus Gntp 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

You must edit the *ntp.conf* file which **ntpd**, the NTP daemon, looks for by default in the the */etc* directory. Assuming that your Tempus Gntp 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
```

If you are using multicast instead of broadcast mode, you would replace the **broadcastclient** keyword with the **multicastclient** keyword. 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
```

Re-start **ntpd** to have it begin using the Tempus Gntp as a broadcast or multicast server. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Tempus Gntp. 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 Tempus Gntp 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 Tempus Gntp 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 4

Setting Up NTP Clients on Windows NT 4.0/2000

To configure your Windows NT 4.0/2000 computer to use your Tempus Gntp, 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 Tempus Gntp 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

Although all the information is available at the above site, the following are excellent tutorials on setting up NTP and are easier to understand:

http://www.sun.com/solutions/blueprints/0701/NTP.pdf

http://www.sun.com/solutions/blueprints/0801/NTPpt2.pdf

http://www.sun.com/solutions/blueprints/0901/NTPpt3.pdf

Many problems may also be solved by the helpful people who participate in the Internet news group devoted to NTP:

news://*your_news_server*/comp.protocols.time.ntp

Three methods of using the Tempus Gntp 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 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 Tempus Gntp 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 Tempus Gntp 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. 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.

Re-start **ntpd.exe** to have it begin using the Tempus Gntp 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 re-start it.

Use the NTP utility **ntpq.exe** to check that **ntpd.exe** is able to communicate with the Tempus Gntp. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT partition. From a console window, 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 Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp on your network.
- Your Tempus Gntp has been configured to perform authentication either by factory default, or by running the **ntpconfig** shell script. The example Tempus Gntp 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. It must be a copy of the one residing in the */etc* directory of your Tempus Gntp. You can **telnet** into your Tempus Gntp and start an **ftp** session with your client computer to send the Tempus Gntp */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 Tempus Gntp 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 */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 it's 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. 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 Tempus Gntp server using one of the trusted keys, in this case key # 1:

```
server 192.168.1.245 key 1
```

Re-start **ntpd.exe** to have it begin using the Tempus Gntp 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 re-start it.

Use the NTP utility **ntpq.exe** to check that **ntpd.exe** is able to communicate with the Tempus Gntp. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT partition. From a console window, 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 Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp on your network.
- Your Tempus Gntp has been configured to perform broadcasts or multicasts via the front-panel keypad or 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 Tempus Gntp 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 Tempus Gntp 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

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. Assuming that your Tempus Gntp 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
```

If you are using multicast instead of broadcast mode, you would replace the **broadcastclient** keyword with the **multicastclient** keyword. 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
```

Re-start **ntpd.exe** to have it begin using the Tempus Gntp 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 re-start it.

Use the NTP utility **ntpq.exe** to check that **ntpd.exe** is able to communicate with the Tempus Gntp. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT partition. 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 Tempus Gntp 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 Tempus Gntp 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 5

Front-Panel Keypad and Display

This section describes the Tempus Gntp front-panel user interface which consists of a graphic vacuum-fluorescent display (VFD) and keypad. The keypad and display provide a convenient interface that allows the user to quickly check the operation of the instrument and setup many control parameters. If desired, the Network Administrator can disable the keypad EDIT key to prevent unauthorized tampering with the instrument setup. Even when disabled, all status and control parameters are available for reading only.

Display Description

The display consists of a graphic 16 x 280 dot-matrix vacuum-fluorescent array. The VFD technology offers very readable, bright alphanumeric characters with variable font sizes. Time information is readable at distances in excess of 15 feet. The keypad consists of an eight-key switch assembly designed to allow easy parameter selection and control.

NOTE

After power is applied, the front-panel display will remain blank for approximately 60 seconds while the Tempus Cntp is initializing.

Keypad Description

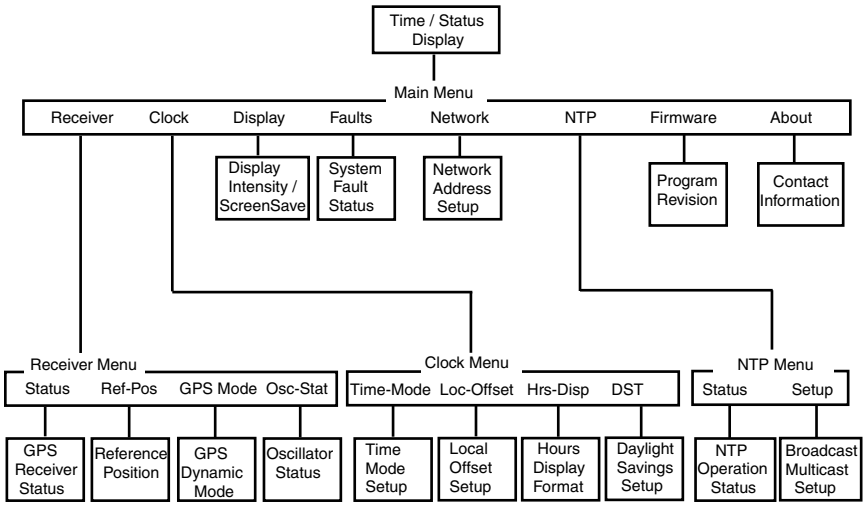
The front-panel keypad consists of eight switch keys identified as follows:

ENTER: Select a menu item or load a parameter when editing.
BACK: Return to previous display or abort an edit process.
EDIT: Edit the parameter currently in view.
HELP: Display context-sensitive help information.
LEFT arrow: Select a new item to the left.

RIGHT arrow: Select a new item to the right.
DOWN arrow: Scroll through parameter values in edit displays or through help lines in help displays. In all other displays this key has a secondary function where it will operate like the ENTER key to select menu items.
UP arrow: Scroll through parameter values in edit displays or through help lines in help displays. In all other displays this key has a secondary function where it will operate like the BACK key to return to the previous display.

Display and Keypad Operation

The display is organized like the inverted tree structure shown below.



Traversing the Display Structure

After power initialization the welcome message will appear. Press any key to go to the Time/Status display, which is described under the heading "Detailed Display Descriptions". From the Time/Status display, press ENTER (or DOWN arrow) to go to the Main Menu. As illustrated in the diagram above, several status and setup displays are accessible from the Main Menu. To traverse downward through the tree use the RIGHT and LEFT arrow keys to highlight a selection and then press ENTER. To traverse back up the tree press BACK (or UP arrow) to return to the previous display.

Editing

To modify a parameter, traverse to the appropriate display and push EDIT. This will cause the edit display to appear. Within the edit display, the modifiable parameter value is highlighted. Use UP and DOWN to scroll through all the possible parameter values. When editing a sequence of numbers, use LEFT and RIGHT to select other digits. When the parameter is correct, press ENTER to load the new value. All entered values

are stored in non-volatile FLASH and restored after a power cycle. If you wish to abort the edit process, press BACK. This operation returns you to the previous display and the parameter will remain unchanged.

Keypad EDIT Lockout

As a security feature, the Network Administrator can disable all editing processes done through the front-panel keypad. This action should be performed to prevent unauthorized modification of the instrument. The lockout feature will prevent editing only, the displays are always available for viewing. When the EDIT key has been disabled, the following message will display whenever a user attempts to edit a parameter.

Using Help

Press HELP at any time to read the context-sensitive help messages. Most Help messages have much more information than can be viewed within the two-line display. Use UP and DOWN to scroll through the help message. Press the HELP key a second time to exit Help (or press BACK).

Detailed Display Descriptions

Time/Status

The Time/Status display provides all the information necessary to determine that the instrument is working correctly.

Time-of-Day: The large numeric digits shown on the left side of the display indicate the current time-of-day.

Time Mode: The indicator next to the time digits identifies the time mode as being UTC, GPS or LOC (for local time). If the user selects local time in the 12-hour mode, an AM or PM indicator will appear instead of LOC.

Date: Current month, day and year.

Stratum: The stratum field has three possible values:

Stratum 1:	The server is fully synchronized and accurate.
Stratum 11:	The server is synchronized to its local CPU clock with undependable accuracy. NTP clients will not use a Stratum 11 server.
Stratum 16:	The server is unsynchronized. NTP clients will not use a Stratum 16 server.

Receiver Status: GPS receiver status as follows:

Acquire: Searching for a signal.
Locking: Locking to the PN Code (spread-spectrum of carrier).
Locked: Synchronized to signal.

System Status: Indicates either OK or flashing FAULT. A fault status indicates that one or more of the built-in fault checking processes has detected an error condition. See Faults section for more information.

Main Menu

Press ENTER from the Time/Status display to select the Main Menu display. The Main Menu provides access to the following items: Receiver Menu, Clock Menu, Display, Faults, Network, NTP Menu, Firmware, and About. To select one of these items use the RIGHT and LEFT keys to highlight it. Then push ENTER to select the highlighted item. These displays are described in detail below.

Receiver Menu

The Receiver Menu provides access to the receiver status and oscillator status displays described below. These are status displays only and cannot be edited.

Receiver Status

This display provides information associated with the operation of the GPS receiver. Press DOWN to scroll through all the information.

Receiver State: This shows the current state of the GPS receiver subsystem. The state may be: acquire, locking, or locked. When locked, the GPS receiver is synchronized to the signal and it is disciplining the internal oscillator to remove frequency and time errors.

Time Figure-of-Merit (TFOM): A detailed explanation of TFOM is in Appendix F. Briefly, TFOM indicates clock accuracy where:

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 the unit has never been locked to GPS.

Carrier-to-Noise: The carrier-to-noise ratio ratio is an indicator of the GPS signal quality. This number typically ranges from 30 to 45 dB when the instrument is locked.

Satellite ID#: This field lists the satellites that are currently being tracked.

Reference Position

This display shows the current GPS position and allows you to enter a position, if necessary. The GPS reference position is the position of the GPS receiver antenna. Accurate position is necessary to generate precise time and frequency outputs.

Source: The source field indicates the source of the position information. Possible values are unknown, average and user. When first installed, the position source will be unknown and change to average after the receiver has computed the position average. Computation requires that a minimum of 4 or more satellites be in view. The position is shown as latitude, longitude and elevation. Latitude and longitude are shown as hemisphere (North, South, East, West), degrees, minutes and seconds. Elevation is shown in meters.

With a roof-top antenna installation that has an unobscured view of the sky, the instrument will determine position automatically. Once determined, the position information is saved in non-volatile FLASH and will be restored after a power outage. After position has been determined, the instrument can achieve time lock with only one satellite.

In some situations, visibility of the sky is limited and the unit may 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 either through the serial interface or via the front panel. In addition to loading a new accurate reference position, the user can also invalidate an existing one by setting the position source to unknown. This will force the instrument to re-establish a new reference position using the GPS satellite constellation.

Push the EDIT key to start the process. First, select the reference position source:

Unknown:	Selecting "unknown" will cause the CALCULATE NEW POSITION AVERAGE confirmation display to appear. Select YES. The front panel will return to the GPS Reference Position display. This action will force the unit to re-establish a new reference position. Once the receiver has computed a new accurate reference position the position source will change from "unknown" to "average".
Source:	Selecting "user" will allow you to enter a position. It is very important that the new reference position be accurate. Refer to Appendix D for detailed instructions on how to obtain an accurate reference position for your location.

GPS Dynamic Mode

The GPS dynamic mode setting affects the position value used by the system to derive accurate time synchronization. Set the mode to "static" when the instrument is in a static installation. Set the mode to "dynamic" if the instrument is installed on a moving platform such as a ship or aircraft.

Oscillator Status

This display provides the oscillator time base status and type. The oscillator control setting (DAC) value indicates the frequency control setting. The system automatically sets this value to remove frequency errors. Values may range from 0 to 65,535. Values less than 10,000 or greater than 55,000 will set the DAC fault flag that will appear in the fault status display. The Time/Status display will also indicate a fault condition.

The oscillator type indicates the oscillator that is installed. Possible oscillator types are:

Temperature-compensated crystal oscillator (TCXO)
Medium-stability oven oscillator (MS-OCXO)
High-stability oven oscillator (HS-OCXO)
Rubidium oscillator (Rb)

Clock Menu

The Clock Menu provides access to the parameters related to timekeeping. These are Time Mode, Local Offset, Hours Format, Leap Seconds, and Daylight Savings Time (DST). These displays are all described below.

Time Mode

Time mode defines the time format used for the front-panel time display and, if installed, the optional time code output. The time mode does not affect the NTP output, which is always UTC. Possible values for the time mode are GPS, UTC, and local time. GPS time is derived from the GPS satellite system. UTC is GPS time minus the current leap second correction. Local time is UTC plus local offset and Daylight Savings Time (DST). The local offset and daylight savings time displays are described below.

Local Offset

Local offset is used in calculating the current local time when the time mode is set to local (see time mode above). Press the EDIT key to change the value by pressing. Enter a negative offset for time zones west of Greenwich and a positive offset for time zones to the east. If enabled, DST will add an additional hour.

Hours Display

The hours-display format affects the front-panel time display and is active only when the time mode is set to local time. Hours-display selections are either 12-hour format (1-12 hours with AM/PM indicator) or 24-hour format (0-23 hours).

Daylight Savings Time (DST)

DST is used in calculating the current local time when the time mode is set to local. When the time mode is local this display will allow the user to enable or disable DST by pressing EDIT. If DST is disabled then any previously set start and stop times will be ignored. If DST is enabled then the start and stop times can be set by pressing the arrow keys to scroll and then ENTER. DST is active within the start-stop interval and adds one hour to the local time. If DST is active the display will show an active indicator.

Display

This display contains parameters related to the functioning of the front-panel vacuum-fluorescent display. There are two parameters -- an intensity setting and a screensaver setting. The intensity setting allows you to set the brightness level of the vacuum-fluorescent display. Display intensity ranges from 12% to 100%. The screensaver capability allows you to increase the usable life of the display beyond the rated 100,000 hours. When the screensaver capability is enabled, then the intensity will be reduced to half of its normal operating intensity when the unit has not detected a keypress for one hour. Press EDIT to modify the intensity and screensaver settings.

Faults

This display provides system fault information. When a particular fault condition is asserted it will be followed by a flashing indicator. Otherwise the fault condition is followed by an "ok" indicator. The fault display and various fault conditions are described below:

FLASH - FLASH Write Fault — 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. This fault would cause erratic operation at the next power cycling since important parameters could be corrupt. The unit should be returned to the factory for repair.

FPGA - 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 .

SIG - 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 a antenna blockage. If the condition persists indefinitely, the unit may need to be returned to the factory for repair.

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.

ANT - Antenna Cable

This fault indicates that the GPS antenna cable is either shorted or open-circuit. Check all antenna connections and cable integrity if this fault should occur.

POLL - No Polling Events

This fault indicates that the GPS timing subsystem is not receiving polling request from the NTP 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.

Network

This display provides the ability to view and modify the network settings. The parameters include Dynamic Host Configuration Protocol (DHCP), IP address, gateway and netmask settings. Enable DHCP to allow automatic system configuration of the network interface. When DHCP is disabled the user must provide address information.

NTP Menu

The NTP Menu provides access to the NTP Status and NTP Setup displays described below:

NTP Status

This display provides information associated with the NTP subsystem.

Source: The synchronization source is named here. For the Tempus Gntp the source is GPS, CPU or none.

Stratum: This stratum field has three possible values:

Stratum 1:	The server is fully synchronized and accurate.
Stratum 11:	The server is synchronized to its local CPU clock with undependable accuracy. NTP clients will not use a Stratum 11 server.
Stratum 16:	The server is unsynchronized. NTP clients will not use a Stratum 16 server.

Offset: The NTP offset indicates the accuracy of the NTP system clock relative to the GPS subsystem clock. Immediately after power-up the NTP system clock free runs using its internal crystal which is likely to be inaccurate. Initially, if the offset between the NTP system clock and the GPS subsystem clock is large the display will indicate "not available". After the GPS subsystem locks, the NTP clock will synchronize to the GPS subsystem. Once synchronization is complete, the typical offsets will range over approximately ± 10 microseconds.

Leap Indicator: Shows the status of the leap indicator bits as sent by the Tempus Gntp time server to the clients in the NTP reply packets. Descriptions of the leap indicator are:

None: No fault and no pending leap second.
Leap Insertion: No fault and a leap second insertion is pending.
Leap Deletion No fault and a leap second deletion is pending.
Fault: Unsynchronized fault condition exists.

NTP Setup

This display provides access to the NTP broadcast and multicast settings.

This display provides the user with a convenient means of checking the current configuration and allows limited setup. You may also perform a more complete broadcast/multicast configuration via a **`telnet`** or **`ssh`** session or the local RS-232 console using the **`ntpconfig`** utility. This utility provides a more secure means of setup and so is more complete. It will allow you to select keys and identify trusted keys.

This display will indicate that the unit is either in broadcast, multicast, or disabled. It allows either broadcast or multicast configuration with selection of the broadcast address, multicast time-to-live (TTL) and trusted key for MD5 authentication. The broadcast/multicast configuration may also be disabled.

Broadcast Mode:	In this mode the broadcast address is displayed. If MD5 authentication is selected the trusted key number will also be display.
Multicast Mode:	The multicast address must be 224.0.1.1. The TTL value is the number of router hops that multicast traffic is permitted to pass through before expiring on the network. Multicast may also use MD5 authentication. If selected, the trusted key number will also be displayed.

Press EDIT to change the broadcast/multicast settings. Each of the edit windows has help information available to guide you through the setup process. Note that changing the NTP multicast/broadcast settings does not take effect until the system reboots. The new parameters are loaded to the ntp.conf file in the */boot/etc/* directory. Only the broadcast line in the ntp.conf file is modified. The final display in the edit sequence requires confirmation of your intent to change the instrument settings. Once confirmation takes place, the instrument will reboot.

Firmware

The Firmware display provides version information for the application software running on the GPS subsystem and the NTP subsystem (Linux OS). Use UP and DOWN to toggle between the two information windows.

About

The About display provides contact information about EndRun Technologies. The website and toll-free phone number are listed.

Shortcut Menu

The Shortcut Menu allows the user quick access to particular displays from the Time/Status display. The displays available through the Shortcut Menu are the Receiver Status display, the Faults display, and the NTP Status display. While viewing the Time/Status display press ENTER for one second to select the Shortcut Menu.

Chapter 6

Control and Status Commands

This chapter describes the Tempus Gntp control and status commands. In addition to a subset of the standard Linux shell commands/utilities, the Tempus Gntp supports several application-specific commands for performing initialization/setup and for monitoring the performance and status of the NTP and GPS subsystems. The standard Linux commands are not documented here. A wealth of information is available from a variety of sources on those. Only the Tempus Gntp specific commands will be described here. The serial I/O port physical and electrical characteristics are defined as well.

General Linux Shell Operation

The command shell used by the Tempus Gntp is a **bash** equivalent that is known as **ash**. **ash** offers good compatibility in running shell scripts written for **bash**, but lacks some of the niceties of **bash**. In particular, it lacks command line editing. 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 Tempus Gntp you should consult either the web

www.linuxdoc.org

or good Linux reference books like:

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

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

to learn the ins and out of the Linux command console.

Available User Commands

COMMAND	FUNCTION
accessconfig	Interactive shell script that guides the user in configuring **`telnet, ssh`** and **`snmpd`** access to the Tempus Gntp 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.
gntpenableupgrade	Enables a firmware upgrade by mounting the FLASH disk partitions that hold compressed root file system images.
gntphwaddr	Prints the ethernet hardware address, if the ethernet has been configured.
gntposctype	Prints the installed oscillator type, which is one of: TCXO, DIP-OCXO, MS-OCXO, HS-OCXO or Rubidium.
gntppasswd	Allows the *root* user to change the password for the two configured users on the Tempus Gntp: *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 0 (factory default) or 1 (field upgrade) which is running in the Tempus Gntp 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 timecode output or optional front panel vacuum fluorescent display.
gntptimemodeconfig	Interactive shell script that guides the user in configuring the time mode settings for any optional timecode output or front panel vacuum fluorescent display. 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 Tempus Gntp application software version information to the console.
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.
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 Tempus Gntp.
kplockstat	Prints the front-panel keypad lockout status.
lockoutkp	Locks out access to the front-panel keypad EDIT key.
netconfig	Interactive shell script that allows the user to configure the IP network subsystem of the Tempus Gntp.
ntpconfig	Interactive shell script that guides the user in configuring the Tempus Gntp NTP subsystem. Allows configuration of MD5 authentication and broadcast/multicast mode. All parameters are retained in non-volatile FLASH disk storage.
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.
unlockkp	Unlocks access to the front-panel keypad EDIT key.
updatelilo	Shell script that must be run to update the Linux Loader (LILO) so that it will boot a new root file system image. **gntpenableupgrade** must have been previously executed in order to run this command.

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 Tempus Gntp. 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 re-boot the Tempus Gntp after running this script for the changes to take effect.

Usage:

Set:	**accessconfig**
Tempus Gntp response:	***Interactive shell script is started.***

gntpenableupgrade

This command mounts the two FLASH disk root file system partitions as part of the firmware upgrade procedure. Refer to Appendix B – *Upgrading the Firmware* for detailed instructions for performing the upgrade procedure.

Usage:

Set:	**gntpenableupgrade**
Tempus Gntp response:	**Mounting root file system partitions.**

gntphwaddr

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

Usage:

Query:	**gntphwaddr**
Tempus Gntp response:	**00:D0:C9:25:78:59**

gntposctype

This command displays the installed oscillator type. It is one of TCXO, DIP-OCXO, MS-OCXO, HS-OCXO or Rubidium. The standard oscillator is the TCXO.

Usage:

Query:	**gntposctype**
Tempus Gntp 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.

Usage:

Query:	**gntppasswd gntpuser**
Tempus Gntp response:	***Passwd interactive utility is started.***

gntprootfs

This command displays the currently booted root file system image. It can be either

TempusGntp_0 (factory image) or TempusGntp_1 (field upgrade image). Refer to Appendix B – *Upgrading the Firmware* for detailed instructions for performing the upgrade procedure.

Usage:

Query:	**gntprootfs**
Tempus Gntp response:	**BOOT_IMAGE=TempusGntp_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 timing 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 engine, 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 = ? shows the Time Figure of Merit (TFOM) of the GPS engine's internal timebase. ? may take values ranging from 4 to 9:

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 been locked to GPS

Refer to *Time Figure of Merit* in Appendix F for a detailed description of the meaning of this number.

YEAR is the year of the UTC timestamp of most recent NTP polling request received by the GPS engine 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 engine 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 engine 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).

Usage:

Query: **gntpstat**

Tempus Gntp 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 timecode outputs or the front panel vacuum fluorescent display. 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.

Usage:

Query: **gntptimemode**

Tempus Gntp response:

```
Time Mode = UTC
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 operation of any optional timecode outputs or front panel vacuum fluorescent display of the Tempus Gntp. *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 LOCAL 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.

Usage:

Set: **gntptimemodeconfig**

Tempus Gntp response: ***Interactive shell script is started.***

gntpversion

This command displays the firmware version and build date of the Tempus Gntp.

Usage:

Query: **gntpversion**

Tempus Gntp response:

Tempus Gntp 6010-0003-000 v 1.00 Wed Jan 16 22:38:21 UTC 2002

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 Tempus Gntp is installed on a moving platform. When it is OFF, it is assumed that the Tempus Gntp is installed in a stationary location.

When the dynamic mode is OFF, the Tempus Gntp 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.

Usage:

Query: **gpsdynmode**

Tempus Gntp 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.

Usage:

Query: **gpsrefpos**

Tempus Gntp response:

CURRENT REFERENCE POSITION = AVG N38d26m36.1s W122d42m56.5s +00032 meters

gpsstat

This command allows the user to query the status of the GPS timing subsystem. During normal operation, the NTP daemon polls the GPS timing 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 SN.R FLTS
```

Where:

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

TFOM = ? shows the Time Figure of Merit (TFOM) of the GPS engine's internal timebase. ? may take values ranging from 6 to 9:

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 been locked to GPS.

Refer to *Time Figure of Merit* in Appendix F for a detailed description of the meaning of this number.

YEAR is the year of the UTC timestamp of the most recent NTP polling request received by the GPS engine 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 engine 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 engine 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 oscillator Voltage Control DAC word, 0 to 65535 with larger numbers implying higher oscillator frequency. Typical range is 20000 to 38000.

SN.R — 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 timing 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:

Hex Character	Bit 3	Bit 2	Bit 1	Bit 0
0	FLASH Write Fault	FPGA Config Fault	No Signal Time-Out	DAC Control Over-Range
1	Antenna Fault	No Polling Events	Not Used	Not Used
2	Not Used	Not Used	Not Used	Not Used
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. This fault would cause erratic operation at the next power cycling since important parameters could be corrupt. The unit should be returned to the factory for repair.
No Polling Events	This bit indicates that the GPS timing subsystem is not receiving polling request from the NTP 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 Tempus Gntp. 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.

Usage:

Query: **gpsstat**

Tempus Gntp 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.

Usage:

Query: **gpstrkstat**

Tempus Gntp 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.

Usage:

Query: **gpsversion**

Tempus Gntp response: **F/W 2.00 FPGA 06**

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 Tempus Gntp. Four protocol servers may be configured: TIME, DAYTIME, TELNET and SSH. 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 re-boot the Tempus Gntp after running this script for the changes to take effect.

Usage:

Set: **inetdconfig**

Tempus Gntp response: ***Interactive shell script is started.***

kplockstat

This command prints the status, either locked or unlocked, of the front-panel keypad EDIT key. When the EDIT key is locked, it will prevent unauthorized tampering with the unit. All other keys are still enabled so you may continue to read the status and current settings of the Tempus Gntp. Refer to the **lockoutkp** and **unlockkp** commands.

Usage:

Set:	**kplockstat**
Tempus Gntp response:	***LOCKED or UNLOCKED***

lockoutkp

This command locks out access to the front-panel keypad EDIT key. When the EDIT key is locked, it will prevent unauthorized tampering with the unit. All other keys are still enabled so you may continue to read the status and current settings of the Tempus Gntp. Refer to the **kplockstat** and **unlockkp** commands.

Usage:

Set:	**lockoutkp**
Tempus Gntp response:	***Front-panel keypad EDIT key disabled.***

netconfig

This command starts an interactive shell script that will allow the user to configure the IP network subsystem of the Tempus Gntp. 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 re-boot the Tempus Gntp after running this script for the changes to take effect.

Usage:

Set:	**netconfig**
Tempus Gntp 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 Tempus Gntp. 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 re-boot the Tempus Gntp after running this script for the changes to take effect.

Usage:

Set: **ntpconfig**

Tempus Gntp response: ***Interactive shell script is started.***

setgpsdynmode

This command accepts a single argument: ON or OFF to allow the user to set the dynamic mode of operation of the Tempus Gntp GPS subsystem. By default, the unit is configured for static operation, so this setting is OFF. If the Tempus Gntp 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.

Usage:

Set: **setgpsdynmode ON**

Tempus Gntp 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 Tempus Gntp. 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 Tempus Gntp to re-establish a new reference position using the GPS satellite constellation.

Usage:

Set: **setgpsrefpos**

Tempus Gntp response: ***Interactive shell script is started.***

unlockkp

This command unlocks out access to the front-panel keypad EDIT key. When the EDIT key is locked, it will prevent unauthorized tampering with the unit. All other keys are still enabled so you may continue to read the status and current settings of the Tempus Gntp. Refer to the **kplockstat** and **lockoutkp** commands.

Usage:

Set: **unlockkp**

Tempus Gntp response: ***Front-panel keypad EDIT key enabled.***

updatelilo

This command allows the user to update the configuration of the Linux Loader (LILO) after a new root file system image has been uploaded to the upgrade root file system partition, */rootfs_1* of the Tempus Gntp FLASH disk. Refer to Appendix B – *Upgrading the Firmware* for detailed instructions for performing the upgrade procedure. Two arguments are accepted, first either 0 or 1 to tell LILO which root file system image should be made the default, second the file name of the new compressed root file system image. If no arguments or any value other than 1 is given for the first argument, the default root file system is set to TempusGntp_0. If the first argument is 1, then the second argument is read and LILO is re-configured to make the default root file system TempusGntp_1.

Upon completion, the root file system partitions are unmounted.

Usage:

Set: **`/boot/updatelilo 1 rootfs1.01.gz`**

Tempus Gntp response:

```
Added TempusGntp_0
Added TempusGntp_1 *

Unmounting root file system partitions now.  Run Gntpenableupgrade
again to remount them, should you need to re-run updatelilo.
```

The trailing asterisk '*' character indicates that the default root file system is set to TempusGntp_1.

RS-232 Serial I/O Port Signal Definitions

DB9M Pin on Tempus Gntp	Signal Name
1	Data Carrier Detect (DCD)
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 (CTS)
9	Ring Indicator (RI)

Null Modem Adapter Cable

In order to connect the Tempus Gntp to another computer, a null modem adapter must be used. The provided adapter cable is wired this way:

DB9F Pin on Adapter	DB9F Pin on Adapter
1	4
2	3
3	2
4	1
5	5
7	8
8	7
9	9

Pin 6 is not connected.

Appendix A

Security

Your Tempus Gntp 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 Tempus Gntp. Others are provided by the additional protocol servers selected for inclusion in your Tempus Gntp, 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 UCD-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.

Linux Operating System

The embedded Linux operating system running in the Tempus Gntp is based on kernel version 2.2.13 and version 7 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 Tempus Gntp

- 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 */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 Tempus Gntp by a pair of shell scripts which ease configuration for the inexperienced user of Unix-like operating systems. These are **accessconfig** and **inetdconfig**.

accessconfig modifies two files which are used by **tcpd** and the standalone daemon, **snmpd** 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 Tempus Gntp 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** daemon also parses this file itself 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. (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.) Be careful to maintain the proper ownership and access permissions by using **cp -p** when copying the files.

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, four servers are configurable via **inetdconfig**: TIME and DAYTIME, whose daemons are contained within the **inetd** daemon itself, and **in.telnetd** and **sshd**. Any one or all of these may be enabled or disabled for start-up.

OpenSSH

The secure shell protocol server running in the Tempus Gntp is based on the portable OpenSSH version 3.4p1 for Linux. As such it supports both SSH1 and SSH2 protocol versions. For more information about this protocol and to obtain client software, refer to the OpenSSH website:

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 Tempus Gntp. This means that users on remote hosts may log in to the Tempus Gntp via an **ssh** client, but users logged in on the Tempus Gntp 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 Tempus Gntp via **scp** over **ssh** but users logged in on the Tempus Gntp 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 Tempus Gntp 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 Tempus Gntp. Three files contain these keys: *identity* (SSH1), *id_rsa* (SSH2) and *id_dsa* (SSH2). These must be copied to the user's ~/*.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 Tempus Gntp. 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 Tempus Gntp. At boot time, the Tempus Gntp 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 Tempus Gntp. 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.

Network Time Protocol

The NTP implementation in the Tempus Gntp is built from version 4.1.1c-rc2 of the standard distribution from the 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 notrust 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 Tempus Gntp 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.

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. After you have downloaded the appropriate FLASH binary image file from the EndRun Technologies website, you are ready to perform the upgrade to your Tempus Gntp.

The firmware consists of two FLASH binary image files. One of these is the firmware for the Tempus Gntp itself. This firmware executes on the IBM-compatible single board computer and contains the embedded Linux operating system and NTP specific application software. The other file is the firmware for the GPS time and frequency subsystem. This firmware executes in the Tempus Gntp GPS time and frequency engine. Each of these files may be upgraded independently.

What You Need To Perform the Upgrade

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

Performing the Tempus Gntp Upgrade

There are two FLASH disk partitions which hold the compressed root file system images. These are normally unmounted. When an upgrade is to be performed they are mounted at */rootfs_0* and */rootfs_1*. The factory shipped image is always stored in the first of these partitions as */rootfs_0/rootfsX.XX.gz*. Where *X.XX* is the factory shipped version. It is stored with the immutable attribute set so that even *root* cannot inadvertently delete it or overwrite it. When performing an upgrade, you will be copying the new image to the partition that will be mounted on */rootfs_1*.

CAUTION

Some browsers will automatically unzip the gzip file when downloading from the website. Please make sure that the gzip file is less than 3M in size before proceeding. Upgrading the partition with a too-large file size can cause serious problems and the unit may have to be returned to the factory for repair.

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

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

```
gntpenableupgrade
```

This command will mount the FLASH disk root file system partitions. Now change the working directory to the upgrade partition:

```
cd /rootfs_1
```

Now remove any previously installed root file system image that may be on the upgrade partition:

```
rm /rootfs_1/*.gz
```

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, */rootfs_1* using FTP (substitute the name of the root file system image that you are installing for *rootfsupgrade.gz*):

```
ftp remote_host      {perform ftp login on remote host}
bin                  {set transfer mode to binary}
get rootfsupgrade.gz {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 root file system image using **scp** from the remote computer. A command like this could be used:

```
scp -p rootfsupgrade.gz root@gntp.your.domain:/rootfs_1
```

Now you must leave the */rootfs_1* directory in order to execute the **updatelilo** command and complete the upgrade:

```
cd /root
```

Update the LILO configuration by executing this shell script (substitute the name of the

root file system image that your are installing for *rootfsupgrade.gz*):

```
/boot/updatelilo 1 rootfsupgrade.gz
```

You should see these lines displayed if the update is successful:

```
Added TempusGntp_0
Added TempusGntp_1 *

Unmounting root file system partitions now.  Run gntpenableupgrade
again to remount them, should you need to re-run updatelilo.
```

The trailing asterisk following the second line indicates that the LILO configuration file is set to default to the new TempusGntp_1 root file system that you just installed on */rootfs_1*. Now reboot the system by issuing this command at the shell prompt:

```
shutdown -r now
```

Wait about 30 seconds for the system to shutdown and re-boot. Then log in to the Tempus Gntp 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=TempusGntp_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 30 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 Tempus Gntp.

Recovering from a Failed Upgrade

To restore your Tempus Gntp to a bootable state using the factory root file system, you must use the serial I/O port and re-boot the Tempus Gntp by cycling the power. Refer to Chapter 1 – *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 Tempus Gntp.

Pay close attention to the terminal window while the unit is re-booting. When the LILO prompt is displayed, you must press the ESC key once on your keyboard within five seconds to let LILO know that you are going to enter the name of a root file system label that it should boot in place of the default. Now type

```
TempusGntp_0
```

This tells LILO to boot the factory root file system. Now watch the rest of the boot process to make sure that you have successfully recovered from the failed upgrade. If the system boots normally, then you should resolve the problems with the previous upgrade and re-perform it.

Performing the GPS Upgrade

To perform this upgrade, log in as the *root* user to the Tempus Gntp 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* (substitute the name of the GPS subsystem image that your are installing for *gpsupgrade.bin*):

```
ftp remote_host      {perform ftp login on remote host}
bin                  {set transfer mode to binary}
get gpsupgrade.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 gpsupgrade.bin root@gntp.your.domain:/tmp
```

Now issue the following command to the Tempus Gntp GPS engine to initiate the upload:

```
echo –e "upload\r" > /dev/ttyS0
```

This command tells the Tempus Gntp GPS engine to enter the 'waiting for download' mode. Now issue this command to start the transfer of the binary file using the XMODEM protocol:

```
lsz –Xk gpsupgrade.bin < /dev/ttyS0 > /dev/ttyS0 2>&1
```

After issuing this command you will have to wait for about one minute for the transfer to complete before the prompt will be re-displayed. There will be no diagnostic error messages displayed if the upload is successful. Following a successful upload, you will see the front panel ALARM and LOCK LEDs go through the start-up sequence.

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

```
gpsversion
```

The new version information should be displayed.

Problems with the GPS 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 Tempus Gntp GPS engine boot loader 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/ttyS0
```

You should now see the 'C' character being received every three seconds. This is the character that the Tempus Gntp GPS engine boot loader sends to indicate to the XMODEM utility that it is wating for a download. You may now re-try 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 start the transfer of the binary file using the XMODEM protocol:

```
lsz –Xk gpsupgrade.bin < /dev/ttyS0 > /dev/ttyS0 2>&1
```

Appendix C

Simple Network Management Protocol

Your Tempus Gntp includes the University of California at Davis (UCD)-SNMP version 4.2.5 implementation of a 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 UCD-SNMP project has its roots in the Carnegie-Mellon University SNMP implementation. For more detailed information about the UCD-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 UCD-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:

TEMPUS-MIB

Which is located on your Tempus Gntp in this ASCII file:

/usr/local/share/snmp/mibs/TEMPUS-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 -s -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 key-strokes.)

IMPORTANT

After editing */etc/rc.d/rc.local*, you must copy it to the */boot/etc/rc.d* directory and re-boot 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 over written.

Quick Start Configuration – SNMPv1/v2c

You should be able to compile the TEMPUS-MIB file on your SNMP management system and access the variables defined therein. The factory default community names are "Tempus" 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. You can, and should, change the default community names by editing */etc/snmpd.conf* and modifying these two lines:

```
rwcommunity   endrun_1
rocommunity   Tempus
```

Configuring SNMPv1 Trap Generation

To have your Tempus Gntp 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 Tempus Gntp. 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 Tempus Gntp will only send a trap to the last declared `trapsink` in the file.

Configuring SNMPv2c Notifications and Informs

To have your Tempus Gntp 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 Tempus Gntp. 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 Tempus Gntp 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 re-boot the system. It is very important to retain the access mode for the file (i.e. 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 over written.

Configuration of SNMPv3

If you are planning to use SNMPv3, you should definitely make use of the two resources mentioned previously (UCD-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 Tempus Gntp via v3 of SNMP, you will have to configure two files:

/etc/snmpd.conf
/boot/ucd-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 Tempus Gntp, 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/ucd-snmp/snmpd.conf* like these for each user:

```
createUser root    MD5 endrun_1 DES endrun_1
createUser ntpuser SHA Tempus0
```

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/ucd-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 re-booting, the agent will read the */boot/ucd-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

The encryption algorithms used by the agent are dependent upon the IP address of the Tempus Gntp. Because of this, new keys must be generated anytime your Tempus Gntp's IP address is changed. It also means that you cannot use the same */boot/ucd-snmp/snmpd.conf* file with multiple Tempus Gntp units. To generate new keys, stop the **`snmpd`** process, delete the existing **`usmUser`** key lines from the file and then add new **`createUser`** lines. Then re-boot 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.

Appendix D

GPS Reference Position

Your Tempus Gntp is capable of operation from either an automatically determined GPS reference position or a manually entered GPS reference position. If your Tempus Gntp 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*. Refer to the *Geodesy* and *WGS-84 Positions* sections of this appendix for details on some of the jargon contained herein.

Obtaining Reference Positions

If you need to provide an accurate (< 100 meter error) reference position to your Tempus Gntp 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 Tempus Gntp antenna or 2) reference a geodetic database to obtain a position for your street address. The first way is the easiest and probably the best:

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 Tempus Gntp 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 Tempus Gntp via the **`setgpsrefpos`** command.

Using Geodetic Databases

Many users will not feel confident in determining their own reference position via this technique. For those users, EndRun Technologies technical support will be happy to assist you. We are familiar with the procedure and can convert your street address and

zipcode information to the proper WGS-84 coordinates for you. The following provides the necessary background information needed to interpret the geodetic database and then describes the procedure:

Geodesy

Geodesy is the science of mathematically describing the earth's surface. To do this, a model or *geodetic datum* is used to fit the shape of the earth. These models are flattened spheres called *ellipsoids*. The earth's shape is accurately modeled using such an ellipsoid, with the equator being a circle around the fattest part and with the north and south poles corresponding to the compressed top and bottom of the ellipsoid. Some of these models are intended only for localized regions of the earth's surface. The GPS uses a model that is called the WGS-84 ellipsoid. It is intended to model the entire earth, and is currently the best global model available.

What these ellipsoids are actually attempting to approximate is the *geoid*. The geoid is a gravitationally equipotential surface surrounding the earth that is everywhere perpendicular to the gravitational field and approximates the surface of the oceans. The height of the surface of the geoid relative to the surface of the WGS-84 ellipsoid is called the *geoid height* or *separation* and has been determined by literally millions of gravitational measurements performed over its entire surface. Due to variations in the distribution of mass concentration of the earth, the geoid height varies over a range of about 100 meters. The simplicity of the ellipsoid model cannot describe these fluctuations, so the precise, survey-quality description of the geoid height is contained in a very large data base. This database can be accessed via a utility called GEOID99 that is freely available from the NGS/NOAA website. Over most of North America, the geoid height is *negative* which means that it lies *below* the surface of the WGS-84 ellipsoid.

The height above the ellipsoid of a point P is called the ellipsoidal height, h of P. The height above the geoid of a point P is called the orthometric height, H. The orthometric height is also commonly known as the height above mean sea level. The geoid height at point P is referred to as N. h, H and N are related using this equation:

$$h = H + N$$

A wealth of information on this subject, as well as conversion programs and databases are available at the National Geodetic Survey/National Oceanic and Atmospheric Administration and the National Imagery and Mapping Agency (formerly the Defense Mapping Agency) websites:

http://www.ngs.noaa.gov

http://164.214.2.59/GandG/pubs.html

WGS-84 Positions

Internally, GPS receivers perform all of their range measurement calculations using receiver and satellite positions that are kept in a Cartesian, XYZ coordinate system. The center of the earth, as modeled by the WGS-84 ellipsoid, is the origin for the coordinates. The X-axis lies in the equatorial plane and intersects the 0° or Greenwich meridian. The Y-axis also lies in the equatorial plane and intersects the 90° east meridian. The Z-axis is perpendicular to the equatorial plane and is the polar axis. The WGS-84 ellipsoid is simple to describe mathematically and facilitates the calculations that take place in a GPS receiver to convert Cartesian XYZ coordinates to latitude, longitude and height above the WGS-84 ellipsoid.

However, for a lot of reasons WGS-84 is not the geodetic datum that has been universally used by mapmakers and surveyers. That means that to use positions generated by a GPS receiver to find a location on a map, a conversion between the GPS WGS-84 position and the geodetic datum used for making the map must be performed. Sometimes the differences are small, as in using a localized datum known as the North American Datum of 1983 (NAD-83). The positional differences between WGS-84 and NAD-83 are only at the one meter level, so for our purposes you can use NAD-83 and WGS-84 interchangeably. The older North American Datum of 1927 (NAD-27) exhibits much larger differences, mostly in the longitude, that can exceed 100 meters. Many maps and survey benchmarks exist that were created using this datum.

Procedure

Access a mapping database, of which there are several on the Internet, that will convert a street address and zipcode to latitude and longitude. In general, the datum for the latitude and longitude will not be WGS-84. In the United States it will likely be NAD-27. If so, you must convert this to NAD-83 using a utility called NADCON that is freely downloadable from the NGS/NOAA website. NAD-83 is sufficiently close to WGS-84 that we can use coordinates from either geodetic datum interchangeably.

Having the horizontal position coordinates, you now need to determine a height above the WGS-84 ellipsoid for your location. To do that, you need to find a survey benchmark near your location and make the assumption that its height is close to your street height. From the same NGS/NOAA website, you can obtain a list of survey benchmarks that are within a user-specified radius of the NAD-83 latitude and longitude coordinates you previously determined. Of these, some are vertical control points, meaning that they have height data as well as latitude and longitude data. You can select one, or several of these that are closest to your location and download the datasheets for those benchmarks.

Some of these vertical control point datasheets are based on GPS survey measurements and contain the height above the NAD-83 ellipsoid information. If so, then you can use that height directly along with the NAD-83 latitude and longitude coordinates you

previously determined. Other vertical control point datasheets will give only the orthometric height, which is the height above the geoid. Fortunately, the height of the geoid above the WGS-84 ellipsoid is also contained in the datasheet. So, to obtain the height above the ellipsoid you must add the orthometric height and the geoid height together. Make any adjustments to the height that might be necessary if the antenna is installed in a high-rise building. Armed with coordinates in the NAD-83 datum, you can input them to the Tempus Gntp via the **setgpsrefpos** command.

The following is a sample datasheet for a benchmark that is near the EndRun Technologies facility in downtown Santa Rosa, CA:

```
DATABASE = Sybase ,PROGRAM = datasheet, VERSION = 6.57
1        National Geodetic Survey,   Retrieval Date = JANUARY 23, 2002
 JT9450 ***********************************************************************
 JT9450  DESIGNATION -  B 1397
 JT9450  PID         -  JT9450
 JT9450  STATE/COUNTY-  CA/SONOMA
 JT9450  USGS QUAD   -  SANTA ROSA (1994)
 JT9450
 JT9450                        *CURRENT SURVEY CONTROL
 JT9450  ______________________________________________________________________
 JT9450* NAD 83(1986)-  38 26 44.     (N)    122 43 25.     (W)     SCALED
 JT9450* NAVD 88     -        47.270  (meters)     155.09   (feet)  ADJUSTED
 JT9450  ______________________________________________________________________
 JT9450  GEOID HEIGHT-         -31.28  (meters)                     GEOID99
 JT9450  DYNAMIC HT  -          47.241 (meters)     154.99  (feet)  COMP
 JT9450  MODELED GRAV-     980,011.6   (mgal)                       NAVD 88
 JT9450
 JT9450  VERT ORDER  -  FIRST     CLASS II
 JT9450
 JT9450.The horizontal coordinates were scaled from a topographic map and have
 JT9450.an estimated accuracy of +/- 6 seconds.
 JT9450
 JT9450.The orthometric height was determined by differential leveling
 JT9450.and adjusted by the National Geodetic Survey in June 1991.
 JT9450
 JT9450.The geoid height was determined by GEOID99.
 JT9450
 JT9450.The dynamic height is computed by dividing the NAVD 88
 JT9450.geopotential number by the normal gravity value computed on the
 JT9450.Geodetic Reference System of 1980 (GRS 80) ellipsoid at 45
 JT9450.degrees latitude (g = 980.6199 gals.).
 JT9450
 JT9450.The modeled gravity was interpolated from observed gravity values.
 JT9450
 JT9450;                    North         East     Units  Estimated Accuracy
 JT9450;SPC CA 2     -   586,710.    1,936,830.      MT  (+/- 180 meters Scaled)
 JT9450
 JT9450                          SUPERSEDED SURVEY CONTROL
 JT9450
 JT9450  NGVD 29     -        46.412  (m)          152.27   (f) ADJUSTED    1 2
 JT9450
 JT9450.Superseded values are not recommended for survey control.
 JT9450.NGS no longer adjusts projects to the NAD 27 or NGVD 29 datums.
 JT9450.See file dsdata.txt to determine how the superseded data were derived.
 JT9450
 JT9450_MARKER: DB = BENCH MARK DISK
 JT9450_SETTING: 38 = ABUTMENT
 JT9450_STAMPING: B 1397 1987
```

```
JT9450_MARK LOGO: NGS
JT9450_STABILITY: B = PROBABLY HOLD POSITION/ELEVATION WELL
JT9450
JT9450  HISTORY     - Date     Condition        Report By
JT9450  HISTORY     - 1987     MONUMENTED       NGS
JT9450
JT9450                          STATION DESCRIPTION
JT9450
JT9450'DESCRIBED BY NATIONAL GEODETIC SURVEY 1987
JT9450'IN SANTA ROSA.
JT9450'IN SANTA ROSA, AT THE INTERSECTION OF U.S. HIGHWAY 101 AND STATE
JT9450'HIGHWAY 12, SET VERTICALLY IN THE SOUTH FACE OF THE NORTH CONCRETE
JT9450'ABUTMENT OF THE SOUTHBOUND U.S. HIGHWAY OVERPASS OF THE STATE
JT9450'HIGHWAY, 6.7 M (22.0 FT) WEST OF THE CENTER OF THE SOUTHBOUND LANES
JT9450'OF THE U.S. HIGHWAY, 5.6 M (18.4 FT) NORTH OF THE CENTERLINE OF THE
JT9450'WESTBOUND LANES OF THE STATE HIGHWAY, AND 0.3 M (1.0 FT) EAST OF THE
JT9450'WEST END OF THE ABUTMENT.
JT9450'THE MARK IS 1.4 M ABOVE A SIDEWALK.

*** retrieval complete.
Elapsed Time = 00:00:01
```

The height data for this benchmark was not obtained via GPS and so does not directly contain height above the ellipsoid, but we can obtain that information by adding the orthometric height (47.27 meters) to the geoid height (-31.28 meters). In this case, the ellipsoid height of the benchmark is 15.99 meters. This benchmark is .4 miles from the EndRun Technologies facility. The GPS antenna at the facility is located on the rooftop of a three story office building which would place it about 15 meters above the street level. If we add 15 meters to the benchmark height we estimate the antenna height at 30.99 meters.

The GPS receiver actually reports a WGS-84 height of 32 meters, which gives remarkably close agreement. In general, you should not expect results that are this good. Downtown Santa Rosa is located on a very flat plain so that relatively distant survey points give acceptable results. You should exercise some judgment in selecting particular survey points to use for your location. As an example, if you know that the terrain west of your facility rises or falls rapidly you should avoid using benchmarks that are west of your facility.

Appendix E

Lithium Battery Replacement

Your Tempus Gntp incorporates a lithium battery on its IBM-PC compatible single board computer subsystem component. This battery is *not* user servicable and your Tempus Gntp should be returned to the factory should its replacement become necessary.

CAUTION

Danger of explosion if battery is incorrectly replaced..

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Appendix F

Time Figure of Merit (TFOM)

This appendix describes the Time Figure of Merit (TFOM) number. The Tempus Gntp displays this number on the front panel via the Receiver Status display (see Chapter 5). The TFOM is also printed out in the time-of-day fields printed by the Tempus Gntp **`gpsstat`** and **`gntpstat`** commands (see Chapter 6). The TFOM number indicates the level of accuracy that should be included in the interpretation of the time-of-day and ranges from 4 to 9:

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 been locked to GPS

In all cases, the Tempus Gntp reports this value as accurately as possible, even during periods of GPS signal outage where the Tempus Gntp is unable to directly measure the relationship of its timing outputs to UTC. During these GPS outage periods, assuming that the Tempus Gntp had been synchronized prior to the outage, the Tempus Gntp extrapolates the expected drift of the Tempus Gntp 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 Tempus Gntp 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 are receiving synchronization from the Tempus Gntp that it is running at stratum 11. NTP clients will recognize that and cease to use the unsynchronized server.

Appendix G

Specifications

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

Antenna:
- Integral +35 dB gain LNA with dual bandpass filters 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. Other lengths optional.

Local Oscillator: TCXO. OCXO or Rubidium (options).

Time to Lock: < 5 minutes, typical.

Display: Brilliant 16x280 dot-matrix vacuum-fluorescent.

Keypad: Enter, Back, Edit, Right, Left, Up, Down, Help.

Network I/O (rear panel RJ-45 jack)**:**
10/100Base-T ethernet

System Status Indicators (front panel)**:**
- **Sync LED:** green indicator that pulses to indicate the current GPS acquisition and lock status.
- **Network LED:** amber indicator that illuminates when the ethernet connection is up and flashes when packets are received or transmitted.
- **Alarm LED:** red indicator that illuminates when a serious fault condition exists.

Linux Maintenance Console:
RS-232 serial I/O on rear panel DB9M jack for secure, local terminal access. Parameters fixed at 19200 baud, 8 data bits, no parity, 1 stop bit. For communication with another computer, 2 meter DB9F—DB9F null modem adapter cable is included.

NTP Client Synchronization Accuracy:
Network factors can limit NTP client synchronization accuracy to .5-2 ms, typical. Timestamping accuracy is maintained to less than 100 us while processing hundreds of NTP packets per second.

Supported Protocols:
- SNTP, NTP v2, v3, v4 and broadcast/multicast mode; MD5 authentication
- SSH server with "secure copy" utility, SCP (Open SSH version 3.4p1)
- SNMP v1, v2c, v3 with Enterprise MIB
- MD5 authentication
- TIME and DAYTIME server
- TELNET client/server
- FTP client
- DHCP client

Power:
- 85-270 VAC, 47-63 Hz, .5 A Max. @ 120 VAC, .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):
- 40-60 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.)

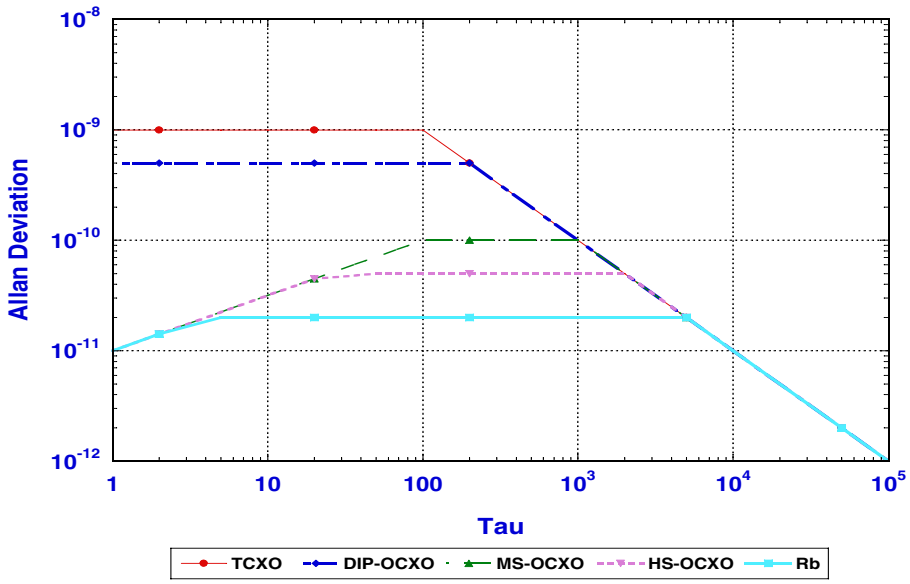
Optional Timing Outputs (rear panel BNC jacks)**:**
- **1 PPS:** 1 ms wide, positive TTL pulse @ 50Ω.
  Accuracy: < 100 nanoseconds to UTC when locked
  Stability: TDEV < 50 ns, $\tau < 10^4$ seconds.
- **Time Code:** 1 Vrms @ 50Ω.
  Format: IRIG-B122

Optional Frequency Output (rear panel BNC jack):

- **10 MPPS:** TTL squarewave @ 50Ω.

  Accuracy: < 10^{-12} to UTC for 24 hour averaging times when locked.

  Stability:



Additional Optional Time/Frequency Outputs (rear panel BNC jacks)**:**

- **10 MHz:** 1Vrms sinewave @ 50Ω, harmonics < -45 dBc
- **5 MHz:** 1Vrms sinewave @ 50Ω, harmonics < -45 dBc
- **1 MHz:** 1Vrms sinewave @ 50Ω, harmonics < -45 dBc
- **5 MPPS:** TTL squarewave @ 50Ω
- **1 MPPS:** TTL squarewave @ 50Ω
- **Time Code TTL:** IRIG-B022 DC-shift TTL @ 50Ω

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:

- **Temperature:** 0° to +50°C
- **Humidity:** 0 to 95%, non-condensing

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), EN61000-3-2 (1995 w/A1 & A2:98),
  EN61000-3-3 (1995 w/A1:98), EN55022 (1998 w/A1:00) Class A,
  VCCI (April 2000) Class A, CISPR 22 (1997) Class A,
  FCC Part 15 Subpart B Section 15.109 Class A,
  ICES-003 Class A (ANSI C63.4 1992),
  AS/NZS 3548 (w/A1 & A2: 97) Class A