EndRun
TECHNOLOGIES
"Smarter Timing Solutions"

Meridian

Precision GPS TimeBase

User Manual

Meridian

Precision GPS TimeBase User Manual

Preface

Thank you for purchasing the Meridian Precision GPS TimeBase. Our goal in developing this product is to bring you a precise time and frequency reference that will quickly, easily and reliably meet or exceed your system requirements. Your new Meridian 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.

The instruments produced by EndRun Technologies have been selected as the timing reference for a variety of industries and applications - computer networks, satellite earth stations, power utilities, test ranges, broadcast and telecommunications systems and more.

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

Trademark Acknowledgements

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

Part No. USM3019-0000-000 Revision 6
December 2007

Copyright © EndRun Technologies 2005-2007

About This Manual

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

Introduction – The Meridian, how it works, where to use it, its main features.
Basic Installation – How to connect, configure and test your Meridian.
Console Port – Description of the Linux console commands for use over the network and serial ports.
Front-Panel Keypad and Display – How to operate the user interface that provides convenient setup and monitoring of the instrument.

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

Warranty

This product, manufactured by EndRun Technologies, is warranted against defects in material and workmanship for a period of 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.

Limitation of Warranty

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

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

Warranty Repair

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

Ship the unit prepaid in the original container or a container of sufficient strength and protection to EndRun Technologies. EndRun will not be responsible for damage incurred during shipping to us. Be sure the RMA number is clearly identified on the shipping container. Our policy is to 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.

EndRun Contact Information

Address:	EndRun Technologies 1360 N. Dutton Avenue #200 Santa Rosa, CA 95401
Phone:	(707)573-8633
Fax:	(707)573-8619
Sales:	1-877-749-3878 or (707)573-8633 sales@endruntechnologies.com
Support:	1-877-749-3878 or (707)573-8633 support@endruntechnologies.com

Table of Contents

Preface i
About EndRun Technologies i
Trademark Acknowledgements i
About This Manual ii
Warranty ii
Limitation of Warranty ii
Warranty Repair iii
Repair After Warranty Expiration iii
Limitation of Liability iii
EndRun Contact Information iii

Chapter One - Introduction 1
Main Features 1
Overview 1
Highly-Reliable, Modular Design 1
Standard Features 2
Secure Network Interface 2
Free FLASH Upgrades 2
GPS Timing-How It Works 2
Where to Use It 3

Chapter Two - Basic Installation 5
Checking and Identifying the Hardware 5
Meridian Physical Description 6
Performing an Initial Site Survey 7
Installing the Meridian 8
Mount the Meridian 8
Connecting the 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 17
Connecting Instruments to the Meridian TimeBase 18

Chapter Three - Front-Panel Keypad and Display 19
Display Description 19
Keypad Description 19
Display and Keypad Operation 20
Traversing the Display Structure 20
Editing 20
Keypad EDIT Lockout 21
Using Help 21
Shortcut Menu 21
Detailed Display Descriptions 21
Time/Status Display 21
Main Menu Display 22
Receiver Menu Display 22
Receiver Status 22
Reference Position 23
Last-Fix Position 24
Oscillator Status 24
Clock Calibration 24
TFOM Fault Level 24
Antenna Fault Mask 25
Signal Loss Fault Mask 25
Clock Menu Display 25
Time Mode 25
Local Offset 25
Hours Display 25

Daylight Savings Time 25
Option I/O Menu Display 25
CPU-I/O Menu Display 26
1PPS Output Setup 26
Timecode Output Setup 26
Programmable TTL Setup 26
Synthesizer (DDS) Setup 26
Serial Time Output Setup 26
Display Setup Display 26
Faults Display 26
Network Setup Display 27
NTP Menu Display 28
NTP Status 28
NTP Setup 28
Firmware Display 29
About Display 29

Chapter Four - Control and Status Commands 31
General Linux Shell Operation 31
Available User Commands 32
Detailed Command Descriptions 34
accessconfig 34
antfltmask 34
cpuoptsconfig 34
eraserootfs_1 35
gpscaldelay 35
gpsdynmode 35
gpsrefpos 35
gpsstat 36
gpstrkstat 38
gpsversion 38
gsyshwaddr 38
gsysosctype 38
gsyspasswd 38

gsysrootfs . . . 38
gsysstat . . . 39
gsystimemode . . . 40
gsystimemodeconfig . . . 40
gsysversion . . . 40
help . . . 40
inetdconfig . . . 40
kplockstat . . . 41
lockoutkp . . . 41
netconfig . . . 41
ntpconfig . . . 41
oscctrlstat . . . 42
pluginopts . . . 42
pluginoptsconfig . . . 42
setantfltmask . . . 43
setgpscaldelay . . . 43
setgpsdynmode . . . 43
setgpsrefpos . . . 43
setsigfltmask . . . 43
settfomfltmask . . . 44
sigfltmask . . . 44
tfomfltlvl . . . 44
unlockkp . . . 44
updaterootflag . . . 44
upgradegps . . . 45
upgradekernel . . . 45
RS-232 Serial I/O Port Signal Definitions . . . 46

Chapter Five - Setting Up the NTP Server . . . 47

Configuring the Network Time Protocol . . . 47
Configuring NTP Using the Front-Panel Keypad . . . 47
Configuring NTP Using the Network Interface or Serial Port . . . 47
Configuring the Meridian as a Stratum 2 Server . . . 50

Chapter Six - Optional Rear-Panel Outputs 51
CPU Module Options 51
Programmable TTL Output 51
Direct Digital Synthesizer (DDS) 51
Fixed Rate TTL Output (10 MPPS, etc.) 52
1 PPS (RS-422) Output 52
Serial Time Output 52
Sysplex Format 52
Truetime Format 53
EndRun Format 53
EndRunX (Extended) Format 54
NENA Format 54
Alarm Output 55
Plug-In Module Options 55
Programmable Digital Buffer Plug-in Module 55
Digital Timecode Formats 55
Direct Digital Synthesizer (DDS) 56
Analog Timecode Buffer Plug-In Module 56
Oscillator/Low Phase Noise Plug-In Module 57
Appendix A - Time Figure-of-Merit (TFOM) 59
Appendix B - Upgrading the Firmware 61
What You Need To Perform the Upgrade 61
Performing the Linux/NTP Upgrade 61
Recovering from a Failed Upgrade 63
Performing the Linux Kernel Upgrade 63
Performing the GPS Upgrade 64
Problems with the GPS Upgrade 65
Appendix C - Simple Network Management Protocol (SNMP) 67
SNMPv3 Security 67
Enterprise Management Information Base (MIB) 67
Invocation of the SNMP daemon 68
Quick Start Configuration -- SNMPv1/v2c 68

Configuring SNMPv1 Trap Generation 69
Configuring SNMPv2c Notifications and Informs 69
Configuration of SNMPv3 69

Appendix D - Security 73
Linux Operating System 73
OpenSSH 74
Network Time Protocol 75

Appendix E - Setting Up NTP Clients on Unix-like Platforms 77
Basic NTP Client Setup 78
Configure NTP 78
MD5 Authenticated NTP Client Setup 78
Create the ntp.keys File 79
Configure NTP 79
Broadcast/Multicast NTP 80
Client Setup 80
Configure NTP 80

Appendix F - Setting Up NTP Clients on Windows NT 4.0/2000/XP 83
Basic NTP Client Setup 84
Configure NTP 84
MD5 Authenticated NTP Client Setup 85
Create the ntp.keys File 85
Configure NTP 85
Broadcast/Multicast NTP Client Setup 86
Configure NTP 87

Appendix G - Timecode Formats 89
IRIG-B122/002 89
IRIG-B123/003 89
IRIG-B120/000 (IEEE-Standard 1344-1995) 89
NASA-36 89
2137 89
IEEE-1344 Bit Definition 90

Appendix H - IPv6 Information 91
Enabling New IPv6 Capabilities 91
OpenSSH 91
Net-SNMP 91
IPv6-Capable syslog-ng 92
IPv4-Only Protocols 92

Appendix I - Third-Party Software 93
GNU General Public License 93
NTP Software License 98

Appendix J - Specifications 99

Appendix K - Software Release Notes for Previous Meridian Users 105
Easy Field-Installable Upgrade 105
If You Are Using DHCP 105
If You Are Operating NTP Without MD5 Authentication 105
Freedom of Choice 105
Performing the Upgrade 106
Enabling New IPv6 Capabilities 106
OpenSSH 106
Net-SNMP 106
New IPv6-Capable 107
syslog-ng 107
Remaining IPv4-Only Protocols 107

Special Modifications - Changes for Customer Requirements 109

Chapter *One*

Introduction

The Meridian Precision GPS TimeBase is a high-performance, full-featured system that provides highly-precise time and frequency outputs. The modular design allows for easy, field-installed upgrades that can satisfy virtually any time and frequency requirement. Advanced packaging techniques, coupled with compact card design, allow for the installation of up to five option boards in a single 1U chassis.

Utilizing a Global Positioning System (GPS) receiver with advanced timing algorithms, the Meridian TimeBase can support operation on static or dynamic platforms. Proprietary, adaptive 3rd order frequency control and TRAIM algorithms maximize the stability and reliability of the output signals. A variety of top-quality quartz and rubidium oscillators are available to handle the full range of holdover, phase noise, and short-term stability requirements.

The Meridian TimeBase utilizes the GPS transmissions to precisely synchronize itself to Universal Coordinated Time (UTC) to the 100-nanoseconds level of accuracy. The frequency of the internal oscillator is disciplined to match the frequency of the UTC timescale to the low parts in 10^{13} level of accuracy over 24-hour observation intervals. The time and frequency outputs are coherent after initial GPS synchronization, and synchronization is maintained via 20-bit DAC frequency control, rather than phase stepping, to provide excellent short-term stability.

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.*

Main Features

Overview

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

Highly-Reliable, Modular Design

The Meridian 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. A complete suite of time and frequency capabilities with an exceptionally high number and variety of outputs are provided in its standard 1U high, 19” rack-mountable chassis. The modular, plug-and-play design of the Meridian TimeBase and a wide range of option cards make it easy to tailor the unit to support your applications.

Standard Features

In addition to sourcing a precision 1PPS timing reference and an IRIG-B timecode output, your Meridian TimeBase includes a network port with high-bandwidth Network Time Protocol (NTP). The Meridian TimeBase incorporates a vibrant 16x280 dot-matrix vacuum-fluorescent display and a user-friendly keypad design for control and status monitoring. The Meridian can also be managed via the network port or a local console on the RS-232 serial port. See ***Chapter 3 - Front-Panel Display and Keypad, Chapter 4 - Control and Status Commands,*** and ***Chapter 5 - NTP*** for more information.

Secure Network Interface

An ethernet port is provided as a standard feature of the Meridian TimeBase with a wide variety of protocols including NTP, SNMP with Enterprise MIB, SSH, TELNET, FTP, and SNTP. Refer to ***Chapter 2 - Basic Installation*** for information to help you set up your network interface. The inclusion of SNMP v3 and SSH provides a very secure network interface and allows you to safely perform monitoring and maintenance activities over the network. Security-conscious users can also disable any or all of the risky protocols such as Telnet, Time and Daytime. In addition, access via SSH, SNMP and Telnet can be restricted to specific hosts. Refer to ***Appendix C - SNMP*** and ***Appendix D - Security*** for further information.

Free FLASH Upgrades

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

GPS Timing-How It Works

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

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

Each satellite in the constellation contains redundant cesium beam or rubidium vapor atomic frequency standards. These provide the timebase for all transmissions from each satellite. These transmissions are monitored from ground stations located around the world and carefully measured relative to GPS time. The results of these measurements for each satellite are then uploaded to that satellite so that they may be incorporated into the data contained in its transmissions. The receiver can use this data to relate the time-of-arrival of the received transmissions from that satellite to GPS time.

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

Where to Use It

Since signals from the GPS satellites are available at all locations on the globe, you may deploy the Meridian virtually anywhere. However, you must be able to install an antenna with good sky visibility, preferably on the rooftop.. Once synchronized, the Meridian can maintain acceptable network synchronization accuracy for about a day without GPS reception, by flywheeling on its standard temperature compensated crystal oscillator (TCXO). For improved holdover for those using the Meridian as a frequency standard several oscillator upgrades are available.

Chapter *Two*

Basic Installation

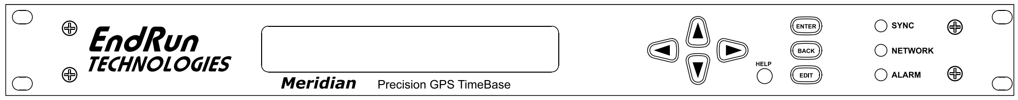
This chapter will guide you through the most basic checkout and physical installation of your Meridian Precision GPS TimeBase. Subsequent chapters and appendices will give you the information needed to configure your installation for the maximum performance in your operating environment. Though some familiarity with Linux or other Unix-like operating systems would be helpful, it is not essential. When operating your Meridian with its standard network interface, basic familiarity with TCP/IP protocols like **`ping`**, **`telnet`** *and* **`ftp`** *is required.*

Checking and Identifying the Hardware

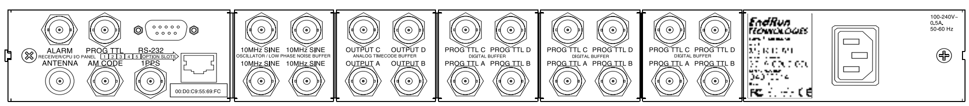
Unpack and check all the items using the shipment packing list. Contact the factory if anything is missing or damaged. The Meridian shipment typically contains:

- Meridian (part # 3019-0001-000 or #3019- variant)
- Meridian User Manual (part #USM3019-0000-000)
- IEC 320 AC Power Cord (part #0501-0003-000)
  (This part will not be present if using the DC power option.)
- DB9F-to-DB9F Null Modem Serial I/O Cable (part #0501-0002-000)
- RJ-45 to RJ-45 CAT-5 patch cable, 2 meters (part #0501-0000-000)
- Antenna/cable assembly (part #0610-0006-001 or #0610- variant)

Meridian Physical Description

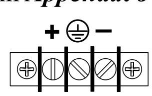


Sync LED	This green LED flashes to indicate synchronization status.
Network LED	This amber LED illuminates when the Meridian is connected to the network and flashes when receiving or transmitting packets..
Alarm LED	This red LED illuminates briefly at power-up, and thereafter whenever a serious fault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



Antenna Jack	This TNC connector mates with the downlead cable from the external antenna.
RS-232 Connector	This DB-9M connector provides the RS-232 serial I/O console interface to the Meridian. This console allows the user to initialize and maintain the Meridian. See ***Chapter 4 - RS-232 Serial I/O Port Signal Definitions*** for detailed information.
10/100Base-T Jack	This RJ-45 connector mates with the ethernet twisted pair cable from the network.
1PPS Jack	This BNC connector provides the 1PPS TTL output. The pulse width is normally 1 millisecond wide when shipped from the factory but can be changed via the front-panel keypad or via console command **`cpuoptsconfig`**. Other selections are 20 microseconds, 100 milliseconds and 500 milliseconds. See signal definition in ***Appendix J - Specifications*** for the 1PPS Output.
AM Code Jack	This BNC connector provides the amplitude-modulated timecode output. The timecode output is normally IRIG-B122 when shipped from the factory, but can be changed via the front-panel keypad or via console command **`cpuoptsconfig`**. Other selections are available. See signal definition in ***Appendix J - Specifications*** for the AM Code Output.
Alarm Jack *(Option)*	This BNC connector (or terminal strip) provides the optional alarm output, and is usually not installed. If installed, see description in ***Chapter 6 - Optional Rear-Panel Outputs*** and signal definition in ***Appendix J - Specifications.***

Prog TTL Jack *(Option)*	This BNC connector provides the optional Programmable TTL pulse rate output and is usually not installed. If installed, see description in ***Chapter 6 - Optional Rear-Panel Outputs*** and signal definition ***in Appendix J - Specifications.***
10 MPPS or 100 PPS, etc. *(Option)*	This BNC connector provides an optional customer-specified rate output and is usually not installed. If installed, it will be labeled for the appropriate rate such as “10 MPPS” or “100 PPS”, etc. This output is set at the factory and cannot be changed. See details in ***Chapter 6 - Optional Rear-Panel Outputs*** and signal definition ***in Appendix J - Specifications*** for the Fixed Rate Output.
1PPS (RS-422) *(Option)*	This optional DB-9M connector provides the 1PPS output at RS-422 levels and is usually not installed.. The pulse width is normally 1 millisecond wide when shipped from the factory but can be changed via the front-panel keypad or via command **`cpuoptsconfig`**. See pinout details in ***Appendix J - Specifications*** for the 1PPS RS-422 Output.
Sysplex or Serial Time *(Option)*	This optional DB-9M connector provides the serial I/O interface with a once-per-second ASCII time string output and is usually not installed. For further information refer see description in ***Chapter 6 - Optional Rear-Panel Outputs*** and ***Appendix J - Specifications.***
Plug-In Modules *(Options)*	Your Meridian has five option slots that can be configured with a variety of plug-in modules. See ***Chapter 6 - Optional Rear-Panel Outputs*** for detailed information on the various modules.
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. See details in ***Appendix J - Specifications.***



Performing an Initial Site Survey

Using the status LED indicators, it’s easy to find out if your Meridian will work in your desired location:

1. Mount the antenna on the roof using the supplied mounting hardware. Make sure that it is not blocked by large metallic objects closer than one meter.

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

3. Plug one end of the supplied AC power cord into an 85-270 VAC outlet.

4. Plug the other end into the AC input connector on the chassis rear panel of the Meridian.

Initially upon power up:

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

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

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

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

At this point, the GPS time and frequency engine has fully synchronized, and you may proceed to permanently mounting the chassis and antenna in their desired locations. If you are unable to achieve GPS lock after 24 hours call Customer Support (1-877-749-3878) for assistance.

NOTE

If your unit has a medium-stability OCXO (MS-OCXO) or rubidum (Rb) oscillator then it will require a 5-10 minute warm-up period before it begins searching for a GPS signal.

Installing the Meridian

FCC NOTICE

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

Mount the Meridian

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 Meridian.

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

Connecting the DC Power Option

Connect the safety ground terminal to earth ground. Connect the "+" terminal to the positive output of the DC power source. Connect the "-" terminal to the negative output of the DC power source. Note that the Meridian has a "floating" internal power supply, therefore either the positive or negative output of the DC power source can be referenced to earth ground. This unit will not operate if the +/- connections are reversed; however it will not be damaged by a reverse connection.

SHOCK/ENERGY HAZARD

Install in Restricted Access Location.

Use 10-14 AWG copper wire only.

Terminal block screw torque: 9 in-lbs (1 nM).

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

Install terminal block cover after wiring.

Connecting and Configuring Ethernet

Connect one end of the CAT-5 patch cable supplied with your Meridian 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 Meridian will attempt to configure the ethernet interface automatically via the Dynamic Host Configuration Protocol (DHCP). The Meridian 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 Meridian 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 Meridian 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 **`bash`** shell prompt. This shell script will prompt you for the needed information and perform some syntax checking on your inputs. Then it will create or modify the appropriate files needed to configure the ethernet interface. The following sections will guide you in setting up communications with the Meridian 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 Meridian 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 Meridian.

To test serial communications with the Meridian 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 Meridian.

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

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 4 - 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 Meridian 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 Meridian. After about 20 seconds, your terminal should display a sequence of boot messages similar to these:

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

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

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

6010-0041-000 Linux Kernel v2.4.26-1 #0 Wed Aug 18 17:28:45 UTC 2004
BIOS-provided physical RAM map:
BIOS-88: 0000000000000000 - 000000000009f000 (usable)
BIOS-88: 0000000000100000 - 0000000002000000 (usable)
32MB LOWMEM available.
On node 0 totalpages: 8192
zone(0): 4096 pages.
zone(1): 4096 pages.
zone(2): 0 pages.
DMI not present.
Kernel command line: config=11000001 initjffs=0 console=ttyS0,19200 root=/dev/
mtdblock4 load_ramdisk=1 rw
Initializing CPU#0
Calibrating delay loop... 66.96 BogoMIPS
Memory: 30784k/32768k available (812k kernel code, 1596k reserved, 162k data, 68k
init, 0k highmem)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
Dentry cache hash table entries: 4096 (order: 3, 32768 bytes)
Inode cache hash table entries: 2048 (order: 2, 16384 bytes)
Mount cache hash table entries: 512 (order: 0, 4096 bytes)
Buffer cache hash table entries: 1024 (order: 0, 4096 bytes)
Page-cache hash table entries: 8192 (order: 3, 32768 bytes)
CPU: AMD 486 DX/4-WB stepping 04
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
PCI: Using configuration type 1
PCI: Probing PCI hardware
PCI: Probing PCI hardware (bus 00)
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
Starting kswapd
JFFS2 version 2.1. (C) 2001 Red Hat, Inc., designed by Axis Communications AB.
Serial driver version 5.05c (2001-07-08) with MANY_PORTS SHARE_IRQ SERIAL_PCI enabled
ttyS00 at 0x03f8 (irq = 4) is a 16550A
ttyS01 at 0x02f8 (irq = 3) is a 16550A
ttyS02 at 0x03e8 (irq = 0) is a ST16654
ttyS03 at 0x02e8 (irq = 3) is a ST16654
sc520_wdt: CBAR: 0x800df000
sc520_wdt: MMCR Aliasing enabled.
sc520_wdt: WDT driver for SC520 initialised.
RAMDISK driver initialized: 16 RAM disks of 16384K size 1024 blocksize
pcnet32.c:v1.28 02.20.2004 tsbogend@alpha.franken.de
PCI: Enabling device 00:0d.0 (0000 -> 0003)
pcnet32: PCnet/FAST III 79C973 at 0x1000, 00 0e fe 00 00 33
    tx_start_pt(0x0c00):~220 bytes, BCR18(9a61):BurstWrEn BurstRdEn NoUFlow
    SRAMSIZE=0x1700, SRAM_BND=0x0800, assigned IRQ 12.
eth0: registered as PCnet/FAST III 79C973
pcnet32: 1 cards_found.
Tempus SC520 flash device: 1000000 at 2000000
 Amd/Fujitsu Extended Query Table v1.3 at 0x0040
number of CFI chips: 1
Creating 7 MTD partitions on "Tempus SC520 Flash Bank":
0x00000000-0x000e0000 : "Tempus kernel"
mtd: Giving out device 0 to Tempus kernel
```

```
0x000e0000-0x00100000 : "Tempus Lo BootLdr"
mtd: Giving out device 1 to Tempus Lo BootLdr
0x00100000-0x00200000 : "Tempus /boot"
mtd: Giving out device 2 to Tempus /boot
0x00200000-0x00300000 : "Tempus /logs"
mtd: Giving out device 3 to Tempus /logs
0x00300000-0x00900000 : "Tempus FACTORY rootfs"
mtd: Giving out device 4 to Tempus FACTORY rootfs
0x00900000-0x00fe0000 : "Tempus UPGRADE rootfs"
mtd: Giving out device 5 to Tempus UPGRADE rootfs
0x00fe0000-0x01000000 : "Tempus Hi BootLdr"
mtd: Giving out device 6 to Tempus Hi BootLdr
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP, IGMP
IP: routing cache hash table of 512 buckets, 4Kbytes
TCP: Hash tables configured (established 2048 bind 2048)
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
mtdblock_open
ok
RAMDISK: Compressed image found at block 0
mtdblock_release
ok
VFS: Mounted root (ext2 filesystem).
Freeing unused kernel memory: 68k freed
INIT: version 2.76 booting
/etc/rc.d/rc.S: /bin: is a directory
mtdblock_open
ok
mtdblock_open
ok
Loading GPS
Loading Keypad/VFD
Fri Aug 20 00:53:54 2004 -0.707128 seconds
2004
Setting system time using hwclock
INIT: Entering runlevel: 3
Entering multiuser...
Attempting to configure eth0 by contacting a DHCP server...
```

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

```
Meridian GPS 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:

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

During this process, the factory default MeridianGPS_0 root file system is loaded from FLASH disk to an 16MB ramdisk and the remainder of the boot process completes. At this point, the Meridian login prompt is displayed:

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

gsys login:
```

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

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

This last line is the standard Meridian shell prompt. The Meridian uses the **bash** shell, which is the Linux standard, full-featured shell. After configuring the unit, you should change the passwords using the **gsyspasswd** 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 4 - RS-232 Serial I/O Port Signal Definitions*** for the signal connections for the Meridian.

NOTE

You must use a null-modem cable or adapter if you are connecting the Meridian 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 Meridian, you may procede to configuring the network parameters. Then you can communicate with the Meridian 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:

```
Meridian GPS(root@gsys)-> netconfig
******************************************************************************
******************* Meridian GPS Network Configuration  *********************
******************************************************************************
*                                                                            *
```

```
*   This script will configure the TCP/IP network parameters for your        *
*   Meridian GPS. You will be able to reconfigure your system at any time    *
*   by typing:                                                               *
*                                                                            *
*   netconfig                                                                *
*                                                                            *
*   The settings you make now will not take effect until you restart your    *
*   Meridian GPS, 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 Meridian GPS. Only the base
hostname is needed, not the domain.
Enter hostname: gsys

---DOMAIN name setting

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

---STATIC IP ADDRESS setting

Set the IP address for the Meridian GPS. Example: 111.112.113.114
Enter IP address for gsys (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 Meridian GPS's current IP address, full hostname, and base hostname:
192.168.1.245       gsys.your.domain    gsys

---DOMAIN NAMESERVER(S) address setting

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

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

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

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

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

********************************************************************************
********************************************************************************
*                                                                              *
*          The Meridian GPS 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 Meridian and re-boot it. There are two ways to do this:

1. Cycle power to the Meridian.

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

```
Meridian GPS(root@gsys:~)-> shutdown -r now
```

If you are using the RS-232 serial I/O port to communicate with the Meridian, 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 Meridian 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 Meridian 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`**:

```
Meridian GPS(root@gsys:~)-> ifconfig

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

```
          Interrupt:5 Base address:0x300

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

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

```
Meridian GPS(root@gsys:~)-> 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 Meridian has been successfully configured to operate on your network and you are ready to check operation of the Meridian 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:

```
Meridian GPS(root@gsys:~)-> 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 Meridian 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 Meridian. Alternatively, you could **ping** one of your servers or workstations from the Meridian shell prompt to test the setup.

Once you have successfully established network communications with the Meridian, you may perform all maintenance and monitoring activities via **telnet** and **ftp**. The Meridian provides both client and server operation using **telnet**. For security reasons as well as to reduce the memory footprint in the Meridian, 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 Meridian. Both of these protocols are supported in the Meridian via the OpenSSH implementations for Linux. Refer to ***Appendix D - Security*** for more information about the secure shell protocol.

Using Telnet

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

```
********************************************************************************
*           Welcome to Meridian GPS telnet console on:  gsys.your.domain
********************************************************************************

gsys login:
```

Here you may log in as "gsysuser" with password "Praecis". When logged in as "gsysuser", 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 Meridian GPS and shows the software part number, version and build date:

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

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

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

```
Meridian GPS(root@gsys:~)-> 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 Meridian, logging in directly as *root* is permitted. When you log in as *root* via a **ssh** session with the Meridian, this banner will be displayed:

```
********************************************************************************
*             Welcome to Meridian GPS SSH console on:  gsys.your.domain
********************************************************************************

root@gsys.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 Meridian and shows the software part number, version and build date:

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

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

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

Connecting Instruments to the Meridian TimeBase

Rear-panel mounted BNC jacks provide the means of connecting your equipment to the Meridian. The standard Meridian provides two precision output signals capable of driving properly terminated coaxial cables: 1PPS and AM Code. These two signals are DC-coupled and sourced from Advanced CMOS (ACMOS) drivers which are able to maintain output TTL levels into a 50-ohm load. The optional low-phase noise, spectrally pure sinewave outputs are capable of driving 1 Vrms into a 50-ohm load. If your unit is equipped with other optional timing or frequency outputs, these will also be designed to drive a 50-ohm load. Care should be taken not to short circuit these outputs or to connect them to other voltage sources.

If your unit is equipped with the optional Alarm Output, it will be available on a rear-panel BNC jack labeled “ALARM”. Care should be taken not to directly connect this open-collector output to a voltage source. A series current-limiting resistor of at least 1K ohms in value should be used. The pull-up voltage must not exceed 40V.

If your primary application for the Meridian is as a frequency standard and you have not purchased one of the optional higher-stability oscillators, you should consider operating with the display set to view the Receiver State. (See ***Chapter 3 - Front-Panel Keypad and Display***.) With this display in view you will always know whether the Meridian is currently locked to a GPS signal while you are performing measurements based on its frequency outputs. The holdover frequency accuracy of the standard TCXO will degrade to the $5x10^{-8}$ level fairly quickly following GPS signal loss, depending upon the ambient temperature.

Refer to ***Chapter 6 - Rear-Panel Output Options*** and to ***Appendix J - Specifications*** for more information on the rear-panel output signals.

Chapter *Three*

Front-Panel Keypad and Display

This section describes the Meridian 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 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.

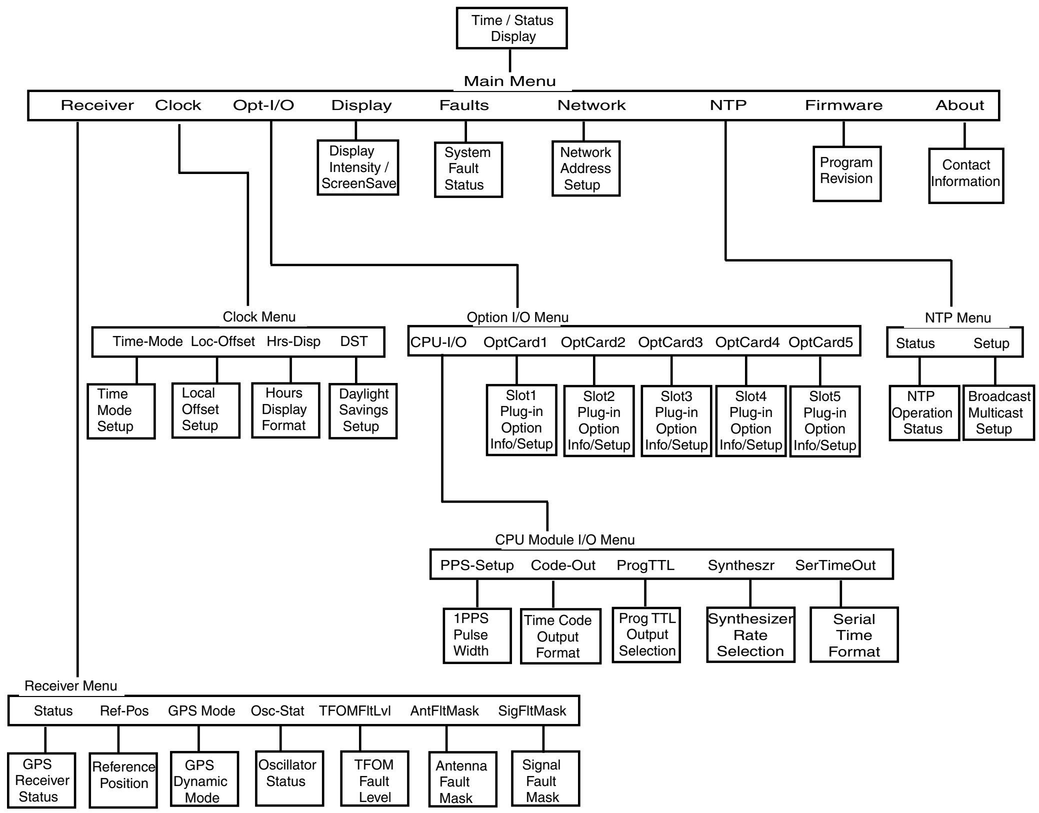
Keypad Description

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. When the EDIT key has been disabled, a warning message will appear whenever a user tries to edit a parameter. To enable the lockout feature use the `lockoutkp` command as described in ***Chapter 4 - Control and Status Commands***. The lockout feature will prevent editing only, the displays are always available for viewing.

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).

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. To select the Shortcut Menu, press ENTER for one second while viewing the Time/Status display.

Detailed Display Descriptions

Time/Status Display

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.
TFOM:	A detailed explanation of TFOM is in ***Appendix A - Time Figure-of-Merit***. 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 never locked to GPS.

Receiver Status: GPS receiver status as follows:

Acquire:	Searching for a signal.
Locking:	Locking to the GPS signal.
Locked:	Fully 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 Display*** in this chapter for more information.

An alternate Time/Status display can be viewed by pressing the right arrow key. You can go back to the original Time/Status display by pressing the left arrow key.

Main Menu Display

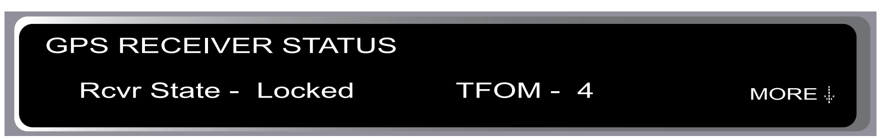
Press ENTER from the Time/Status display to select the Main Menu display. The Main Menu provides access to the following displays: ***Receiver***, ***Clock***, ***CPU-I/O***, ***Display***, ***Faults***, ***Network***, ***NTP***, ***Firmware***, and ***About***. To select one of these items use the RIGHT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

Receiver Menu Display

The Receiver Menu is selected from the Main Menu and provides access to the Receiver Status, Oscillator Status, Reference Position, and GPS Dynamic Mode displays described below.

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.

TFOM: A detailed explanation of TFOM is in ***Appendix A - Time Figure-of-Merit***. 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 never locked to GPS.

Carrier-to-Noise: The carrier-to-noise 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 desired. The GPS reference position is the position of the GPS receiver antenna. Accurate position is necessary to generate precise time and frequency outputs.

The source field (SRC) indicates the source of the position information. Possible values are "unknown", "average" and "user". When first installed, the position source will be "unknown". It changes to "average" after the receiver has computed the first 3-dimensional position fix. The position continues to be averaged for about 24 hours. 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 above the WGS-84 ellipsoid.

With a rooftop 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".

User: Selecting "user" will allow you to enter a position. It is very important that the new reference position be accurate.

GPS Dynamic Mode

The GPS dynamic mode setting affects the position value used by the system to derive accurate time synchronization. In dynamic mode, the average position is the current position, i.e. there is no postion averaging. 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.

Last-Fix Position

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

Oscillator Status

This display provides the oscillator type, electronic frequency control status and several oscillator disciplining parameters. 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)

Osc Cntrl DAC:	The oscillator control DAC value indicates the frequency control setting. The system automatically sets this value to remove frequency errors. Values may range from 0 to 1048575. Values close to the maximum/minimum settings will set the DAC fault flag that will appear in the fault status display. The Time/Status display will also indicate a fault condition.
Coast Time:	This indicates the number of seconds the unit has been in coast mode.
Estimated Time Error:	This is the estimated time error of the instrument while in coast mode.
Measured Time Error:	This is the last measured time offset while locked.
Time Deviation:	Time deviation of measurements.
Ageing Rate:	Regression computed oscillator ageing rate per day.
Control Loop TAU:	Control loop averaging time constant.
Temperature:	The internal temperature (OCXO and Rubidium oscillators only).

Clock Calibration

Use Clock Calibration to advance or retard the clock in order to correct for antenna cable length or to compensate for the inherent time offsets that may exist with external hardware such as distribution amplifiers, etc. Clock Calibration range is ±500.000 microseconds.

TFOM Fault Level

The TFOM Fault Level is the threshold at which a signal loss fault will be asserted. See ***Appendix A - Time Figure of Merit*** for more information. The factory default for the TFOM Fault Level is 9, which is also the maximum TFOM value. By changing the TFOM Fault Level you control the point at which the time error will produce a signal loss fault, which then creates an alarm condition.

Antenna Fault Mask

This setting allows you to prevent the antenna fault from creating an alarm conditon. Some installations may need to mask this fault due to special antenna situations like splitters or DC blocks that confuse the antenna detection circuit.

Signal Loss Fault Mask

This setting allows you to prevent a signal loss fault from creating an alarm condition. Some installations may need to mask this fault when operating the NTP server as a Stratum 2 server.

Clock Menu Display

The Clock Menu provides access to the parameters related to timekeeping. These are Time Mode, Local Offset, Hours Format, and Daylight Savings Time. These displays are 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. 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. Enter a negative offset for time zones west of the Greenwich meridian, 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

Daylight Savings Time (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.

Option I/O Menu Display

The Option I/O Menu provides access to the parameters related to the rear-panel I/O connectors. In addition to the standard CPU module, each Meridian has five option slots available. Each slot has an associated display for setup or status monitoring. Slot 1 is the first plug-in location next to the CPU module. If, at power-up, an option slot is found to be empty, the display will indicate No-Card(1-5). When a plug-in option card is found, the display will show OptCard(1-5). Select an option slot to view status and setup information for the option card located there. Select CPU-I/O to view status and setup information for the CPU module outputs.

CPU-I/O Menu Display

The CPU I/O Menu provides access to the setup displays for the 1PPS Pulse Width, the Timecode Output Format, and the optional Programmable TTL Output and Synthesizer. Displays for the standard Meridian outputs (1 PPS and Timecode) are described below. For information on the optional Meridian outputs plus the different option cards see ***Chapter 6 - Optional Rear-Panel Outputs.***

1PPS Output Setup

The 1PPS-Setup display allows you to select the pulse width for the 1PPS output. Factory default is normally 1 millisecond wide. See details in ***Appendix J - Specifications*** for 1PPS Output.

Timecode Output Setup

The Code-Out display allows you to select the timecode format. Factory default is normally IRIG-B122. See details in ***Appendix J - Specifications*** for the AM Code Output.

Programmable TTL Setup

The ProgTTL display allows you to select a pulse rate for the optional Programmable TTL output. Many pulse rates are available to choose from. See details in ***Chapter 6 - Optional Rear-Panel Outputs*** or ***Appendix J - Specifications*** for the Optional Programmable TTL Pulse Rate Output.

Synthesizer (DDS) Setup

The Syntheszr display allows you to select the rate for the optional Direct Digital Synthesizer (DDS) Output. See details in ***Chapter 6 - Optional Rear-Panel Outputs*** or ***Appendix J - Specifications*** for the Optional Programmable TTL Pulse Rate Output (Synthesized Rate).

Serial Time Output Setup

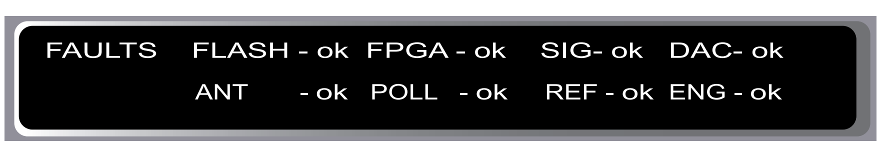
The SerTimeOut display allows you to set up the parameters for the optional, once-per-second, serial time output. See details in ***Chapter 6 - Optional Rear-Panel Outputs*** or ***Appendix J - Specifications*** for Optional Serial Time Output.

Display Setup Display

This display is selected from the Main Menu and 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, 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 Display

This display is selected from the Main Menu and 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 - 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 Configuration - This fault indicates that the microprocessor was unable to configure the FPGA. This would be a fatal fault and the unit should be returned to the factory for repair.

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

DAC DAC Control Over-Range - This fault indicates that the electronic frequency control
DAC

for the oscillator has reached either the high (880000) or low (160000) 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 requests 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.

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

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

Network Setup Display

This display is selected from the Main Menu and 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 Display

The NTP Menu is selected from the Main Menu and provides access to the NTP Status and NTP Setup displays described below:

NTP Status

This display provides information associated with the NTP subsystem.

Stratum: This stratum field has three possible values:
- Stratum 1: The server is fully synchronized and accurate.
- Stratum 2: The server is synchronized to a stratum 1 server with IP address shown in Source.
- Stratum 16: The server is unsynchronized. NTP clients will not use a Stratum 16 server.

Source: The synchronization source is named here. For the Meridian the source is GPS, IP address of upstream source, or none.

Offset: The NTP offset indicates the accuracy of the NTP system clock relative to the GPS subsystem clock. 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 +/- 1 microsecond.

LI Bits: Shows the status of the leap indicator bits as sent by the Meridian time server to the clients in the NTP reply packets. Descriptions of the leap indicator are:
00 - None: No fault and no pending leap second.
01 - Insert Pending: No fault and a leap second insertion is pending.
10 - Delete Pending: No fault and a leap second deletion is pending.
11 - Fault: Unsynchronized fault condition exists.

NTP Setup

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

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 Display

The Firmware display is selected from the Main Menu and provides version information for the application software running on the GPS subsystem and the NTP subsystem (Linux Root File System and Linux Kernel). Use UP and DOWN to toggle between the information windows.

About Display

The About display is selected from the Main Menu and provides contact information for EndRun Technologies. The website and toll-free phone number are listed.

Chapter*Four*

Control and Status Commands

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

General Linux Shell Operation

You do not need to know Linux in order to operate the Meridian. However, for those interested, the command shell used by the Meridian is the Linux standard: **`bash`**. All commands and file names are case sensitive, which is standard for Unix-like operating systems. If you are unfamiliar with Unix-like operating systems, and you would like to be able to more closely monitor or optimize the performance of your Meridian you should consult either the web

http://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 Meridian that is limited to specific hosts. The resulting */etc/hosts.allow* and */etc/hosts.deny* files are saved to the non-volatile FLASH disk. Factory default configuration allows access by all hosts.
antfltmask	Prints the current setting for the Antenna Fault Mask.
cpuopts	Returns the current settings for any installed, user-selectable outputs from the CPU Module. These are 1PPS, AM Code and the optional Programmable TTL and Synthesizer.
cpuoptsconfig	An interactive script that allows the user to modify the settings for the CPU Module outputs listed above.
cpusertime	Prints the current settings for the Serial Time Output Option.
cpusertimeconfig	An interactive script that allows the user to modify the settings for the Serial Time Output Option. These settings are format, baud rate, and parity.
eraserootfs_1	Command to erase the UPGRADE root file system FLASH partition. This must be executed prior to loading the new file system image during the Linux/NTP upgrade process.
gpscaldelay	Prints the calibration delay 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.
gsyshwaddr	Prints the ethernet hardware address, if the ethernet has been configured.
gsysosctype	Prints the installed oscillator type, which is one of: TCXO, MS-OCXO, HS-OCXO or Rubidium.
gsyspasswd	Allows the *root* user to change the password for the two configured users on the Meridian: *gsysuser* and *root*. This script calls the standard Linux **`passwd`** binary and then saves the resulting */etc/shadow* file to the non-volatile FLASH disk.
gsysrootfs	Prints the current root file system image, either MeridianGPS_0 (factory default) or MeridianGPS_1 (field upgrade) which is running in the Meridian to the console.
gsysstat	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.
gsystimemode	Prints the time mode settings in effect for the timecode output or front-panel display.

gsystimemodeconfig	Interactive shell script that guides the user in configuring the time mode settings for the timecode output or front-panel 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.
gsysversion	Prints the Meridian application software version information to the console.
help	Prints help for Meridian commands (not Linux).
inetdconfig	Interactive shell script that allows the user to configure the list of protocol servers which are started by the **`inetd`** server daemon running in the Meridian.
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 Meridian.
ntpconfig	Interactive shell script that guides the user in configuring the Meridian NTP subsystem. Allows configuration of MD5 authentication and broadcast/multicast mode. All parameters are retained in non-volatile FLASH disk storage.
oscctrlstat	Prints the oscillator disciplining parameters.
pluginopts	Returns the board type and settings for any installed plug-in option boards.
pluginoptsconfig	An interactive script that allows the user to change the settings on any configurable plug-in option board.
setantfltmask	Command to enable or mask the Antenna Fault. Parameters to this command are either MASKED or ENABLED.
setgpscaldelay	An interactive script that allows the user to change the clock calibration delay.
setgpsdynmode	Allows the user to set the dynamic mode of operation of the GPS subsystem. It may be ON or OFF.
setgpsrefpos	Interactive shell script that prompts the user for an accurate reference position, performs syntax and argument validity checking then passes the position to the GPS subsystem.
setsigfltmask	Command to mask or enable the signal loss fault.
settfomfltlvl	Command to change the TFOM fault level.
sigfltmask	Prints the current setting for the Signal Loss Fault.
tfomfltlvl	Prints the current setting for the TFOM Fault Level.
unlockkp	Unlocks access to the front-panel keypad EDIT key.
updaterootflag	Command to update the flag stored in FLASH that is read by the Linux bootloader at boot time to select operation with either the FACTORY or UPGRADE root file system.
upgradegps	Shell script that facilitates the GPS subsystem firmware upgrade process.
upgradekernel	Shell script that facilitates the Linux kernel firmware upgrade process. Limited applicability. Use with caution.

Detailed Command Descriptions

accessconfig

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

Set:	**`accessconfig`**
Meridian response:	Interactive shell script is started.

antfltmask

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

Query:	**`antfltmask`**
Meridian response:	**`Antenna Fault is ENABLED`**

cpuopts

This command displays the current settings for the installed RCVR/CPU outputs. The exception is the Serial Time Output Option which uses command **`cpusertime`**.

Query:	**`cpuopts`**
Meridian response:	**`CPU Option 1PPS is installed.`** **`Current setting = 20 microseconds.`** **`CPU Option TIME CODE is installed.`** **`Current Setting = IRIG-B122.`**

cpuoptsconfig

This command starts an interactive shell script that will allow the root user to change the settings of any installed RCVR/CPU output. The user-selectable outputs are 1PPS, AM Code, and the optional Prog TTL and Synthesizer. The optional Serial Time Output is configured using command **`cpuser-timeconfig`**.

Set:	**`cpuoptsconfig`**
Meridian response:	Interactive shell script is started.

cpusertime

This command displays the current settings for the optional Serial Time Output.

Query:	**`cpusertime`**
Meridian response:	**`Current Serial Time Output Baud Rate Setting = 9600`** **`Current Serial Time Output Format Setting = Sysplex`** **`Current Serial Time Output Parity Setting = Odd`**

cpusertimeconfig

This command starts an interactive shell script that will allow the root user to change the settings of the optional Serial Time Output. The user-selectable outputs are the format (Sysplex, Truetime, End-Run, EndRunX and NENA), the baud rate (4800, 9600, 19200, 57600) and the parity (ODD< EVEN, or NONE).

Set: **`cpusertimeconfig`**
Meridian response: Interactive shell script is started.

eraserootfs_1

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

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

gpscaldelay

This command displays the current calibration delay setting. The allowable calibration delay range is +500000 to -500000 nanoseconds.

Query: **`gpscaldelay`**
Meridian resposne: **`+0 nanoseconds`**

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

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

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

Query: **`gpsdynmode`**
Meridian 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.

Query: **`gpsrefpos`**
Meridian response:

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

gpsstat

This command allows the user to query the status of the GPS 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 = ? A detailed explanation of TFOM is in ***Appendix A - Time Figure-of-Merit***.
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 never locked to GPS.

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 1048575 with larger numbers implying higher oscillator frequency. Typical range is 320000 to 640000.

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:

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

DAC Control Over-Range: This bit indicates that the electronic frequency control DAC for the oscillator has reached either the high (55000) or low (10000) limit while locked to the GPS signal. Unless the unit is being subjected to out-of-specification environmental conditions, this would indicate that the oscillator frequency has drifted near to the end of life region. This should normally only occur after about ten years of operation. The unit will continue to function until the oscillator frequency finally reaches one of the actual DAC endpoints. The unit should be returned to the factory for oscillator replacement at the customer's convenience. Note: The value referred to here is the upper 16 bits of a 20-bit DAC value.

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.

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

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

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 Meridian. If the condition persists after checking the antenna/downlead for obvious faults, this is a fatal fault and the unit should be returned to the factory for repair.

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

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

gpstrkstat

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

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

gpsversion

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

Query: **`gpsversion`**
Meridian response: **`F/W 1.00 FPGA 0202`**

gsyshwaddr

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

Query: **`gsyshwaddr`**
Meridian response: **`00:D0:C9:25:78:59`**

gsysosctype

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

Query: **`gsysosctype`**
Meridian response: **`Installed Oscillator is TCXO.`**

gsyspasswd

This command allows the root user to change the passwords of the two configured users on the system: *root* and *gsysuser*. Arguments passed to **`gsyspasswd`** 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.

Query: **`gsyspasswd gsysuser`**
Meridian response: Passwd interactive utility is started.

gsysrootfs

This command displays the currently booted root file system image. It can be either MeridianGPS_0 (factory image) or MeridianGPS_1 (field upgrade image). Refer to ***Appendix B - Upgrading the Firmware*** for detailed instructions on performing the upgrade procedure.

Query: **gsysrootfs**
Meridian response: **BOOT_IMAGE=MeridianGPS_1**

gsysstat

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 = ? A detailed explanation of TFOM is in ***Appendix A - Time Figure-of-Merit***. 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 never locked to GPS.

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).

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

gsystimemode

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.

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

gsystimemodeconfig

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 Meridian. *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.

Set:	**`gsystimemodeconfig`**
Meridian response:	Interactive shell script is started.

gsysversion

This command displays the firmware version and build date of the Meridian.

Query:	**`gsysversion`**
Meridian response:	

`Meridian GPS 6010-0042-000 v 2.00 Wed Jan 16 22:38:21 UTC 2004`

help

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

Query:	**`help`**
Meridian response:	Meridian commands are displayed.
Query:	**`help gpsstat`**
Meridian response:	Information specific to the **`gpsstat`** command is displayed.

inetdconfig

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

This script modifies the */etc/inetd.conf* file, which is non-volatilely stored in the FLASH disk */boot/etc* directory. You must re-boot the Meridian after running this script for the changes to take effect.

Set:	**`inetdconfig`**
Meridian 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 Meridian. Refer to the **`lockoutkp`** and **`unlockkp`** commands.

Set:	**`kplockstat`**
Meridian response:	**`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 Meridian. Refer to the **`kplockstat`** and **`unlockkp`** commands.

Set:	**`lockoutkp`**
Meridian 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 Meridian. 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 Meridian after running this script for the changes to take effect.

Set:	**`netconfig`**
Meridian 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 Meridian. 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 Meridian after running this script for the changes to take effect.

Set:	**`ntpconfig`**
Meridian response:	Interactive shell script is started.

oscctrlstat

This command displays the current settings for the oscillator control parameters. These parameters are used to discipline the oscillator. The command formats the data and prints this fixed-length string having these fields:

```
Oscctrlstat = LKSTAT COAST ESTERR MEASERR TIMEDEV AGERATE TAU TEMP
```

Where:

LKSTAT	is the GPS subsystem control status, either acquiring, locking or locked.
COAST	is the number of seconds in coast mode (unlocked).
ESTERR	is the estimated time error when in coast mode in seconds.
MEASERR	is the last measured time offset while locked in seconds.
TIMEDEV	is the time deviation (TDEV) of measurements in seconds.
AGERATE	is the regression computed oscillator ageing rate per day (several-hour delay before the first measurements are displayed).
TAU	is the oscillator control loop averaging time constant in seconds.
TEMP	is the internal temperature in °C for OCXO and Rubidium oscillators only.

Query: **`oscctrlstat`**

Meridian response:

```
Oscctrlstat = LKD  0 2.72e-09 -2.72e-09 1.23e-09 -0.00e+00   235.2  524332 -999.999
```

pluginopts

This command displays the current settings for the installed plug-in option boards.

Query: **`pluginopts`**

Meridian response:

```
Digital Buffer, 2001-0004-012-NC is installed.
Port A Current Setting = 10M PPS.
Port B Current Setting = 5M PPS.
Port C Current Setting = 10 PPS.
Port D Current Setting = 10 PPS.
```

pluginoptsconfig

This command starts an interactive shell script that will allow the root user to change the settings of any installed, user-selectable, plug-in option board outputs. The user-selectable outputs are all board-specific. For more information see ***Chapter 6 - Optional Rear-Panel Outputs.***

Set:	**`pluginoptsconfig`**
Meridian response:	Interactive shell script is started.

setantfltmask

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

Set:	**`antfltmask MASKED`**
Meridian response:	**`Antenna Fault Mask set to MASKED`**

setgpscaldelay

This command starts an interactive shell script that allows the user to change the clock calibration delay. This setting is used to advance or retard the clock in order to compensate for antenna cable length or other external hardware. Allowable range is +500000 to -500000 nanoseconds.

Set:	**`setgpscaldelay`**
Meridian 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 GPS subsystem. By default, the unit is configured for static operation, so this setting is OFF. If the Meridian will be mounted on a moving platform, like a ship, then this setting must be changed to ON. The change takes place immediately and is stored non-volatilely.

Set:	**`setgpsdynmode ON`**
Meridian 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 Meridian. 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. *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 Meridian to re-establish a new reference position using the GPS satellite constellation.

Set:	**`setgpsrefpos`**
Meridian response:	Interactive shell script is started.

setsigfltmask

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

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

settfomfltmask

This command allows the change the TFOM Fault Level. This is the threshold at which a signal loss fault will be asserted. See ***Appendix A - Time Figure of Merit*** for more information. By changing the TFOM Fault Level you control the point at which the time error will produce a signal loss fault, which then creates an alarm condition. The factory default setting is 9, which is the maximum TFOM value.

Set:	**`settfomfltlvl 6`**
Meridian response:	**`TFOM Fault Level set to 6`**

sigfltmask

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

Query:	**`sigfltmask`**
Meridian response:	**`Signal Loss Fault is ENABLED`**

tfomfltlvl

This command displays the current setting for the TFOM Fault Level.

Query:	**`tfomfltlvl`**
Meridian response:	**`9`**

unlockkp

This command unlocks 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 Meridian. Refer to the **`kplockstat`** and **`lockoutkp`** commands.

Set:	**`unlockkp`**
Meridian response:	**`Front-panel keypad EDIT key enabled.`**

updaterootflag

This command allows the user to update the configuration of the Linux bootloader after a new root file system image has been uploaded to the UPGRADE root file system partition, */dev/rootfs_1* of the Meridian FLASH disk. It may also be used to reset the default back to the FACTORY root file system partition. Refer to ***Appendix B - Upgrading the Firmware*** for detailed instructions for performing the upgrade procedure. One argument is accepted, whose value is either 0 or 1, causing a flag to be set that will indicate to the bootloader which root file system image should be loaded by default. If an argument value of 2 is given, then the currently configured default root file system is shown.

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

upgradegps

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

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

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

Meridian response:

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

Waiting for download using XMODEM 128 or XMODEM 1K (both with CRC).
Control X will abort download.
CCC
---Starting file upload, should take about 60 seconds...

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

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

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

upgradekernel

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

Set	**upgradekernel /tmp/newkernelimage**
Tempus LX response:	Interactive shell script is started.

RS-232 Serial I/O Port Signal Definitions

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

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

Chapter*Five*

Setting Up the NTP Server

This chapter will guide you through the configuration of the Network Time Protocol (NTP) server. When operating your Meridian with its standard network interface, 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.

Instructions for setting up the NTP Clients are given in ***Appendix E - Setting Up NTP Clients on Unix-Like Platforms*** *and in* ***Appendix F - Setting Up NTP Clients on Windows NT 4.0/2000/XP****.*

Configuring the Network Time Protocol

This chapter assumes that the network port has been configured and tested as per the instructions in ***Chapter 2 - Basic Installation***. Once this has been done, you may configure the operation of the NTP server. By default, the Meridian 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 Meridian. If you need to modify the factory default Meridian MD5 keys (recommended) or set up broadcast/multicast operation, then you will need to re-configure the NTP subsystem. You may perform the configuration from either a **`telnet`** or **`ssh`** session, the front-panel keypad, or the local RS-232 console.

NOTE

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

Configuring NTP Using the 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:

```
Meridian GPS(root@gsys:~)-> ntpconfig
```

```
*******************************************************************************
*********************Network Time Protocol Configuration**********************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure the ntp.conf and ntp.keys files   *
*   that control Meridian 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       *
*   Meridian GPS.  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_GPS

Writing key number: 2 and Key: Tempus_GPS to ntp.keys
Enter a key number (1-65534) or 0 to quit: 0
---NTP Authentication Configuration
Do you want authentication enabled using some or all of the keys in
the ntp.keys file? ([y]es, [n]o) y

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

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

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

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

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

---NTP Broadcast/Multicast Configuration

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

Set the network broadcast/multicast address for the Meridian GPS to use.  For
broadcast mode, this address is the all 1's address on the sub-net.
Example: 111.112.113.255
For multicast operation, it is this specific address:  224.0.1.1

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

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

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

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

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

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

Configuring the Meridian as a Stratum 2 Server

Operating the Meridian as a Stratum 1 Server is the recommended mode. You may operate the unit as a Stratum 2 server but since there are innumerable ways to configure your network with Stratum 2 servers, specific insructions for how to do that are beyond the scope of this manual. General instructions are that you need to edit the *etc/ntp.conf* file and then copy it to the */boot/etc* directory to make it nonvolatile.

Unless you are a very knowledgeable NTP user and understand the ramifications we advise against using your Meridian as anything other than a Stratum 1 server. Since the Meridian is running standard NTP compiled from the distribution maintained at the University of Delaware all information in the following link is pertinent:

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

Chapter*Six*

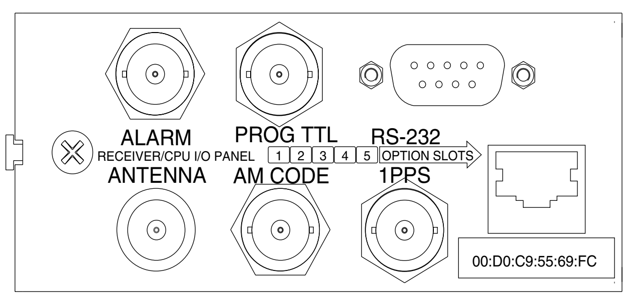
Optional Rear-Panel Outputs

Your Meridian Precision GPS TimeBase supports several output options via the CPU module and up to five plug-in option cards. Status and user settings for the various output signals can be easily viewed and modified via the front-panel keypad and display, the standard network port, or the RS-232 serial port.

CPU Module Options

Standard rear-panel configuration for the CPU module is the Antenna input, the AM Code output, the 1 PPS output, the RS-232 connector and the ethernet connector. Information for the standard outputs, including getting status and control capability via the user interface is described in the main text of this manual. Refer to ***Chapter 3 - Front-Panel Keypad and Display*** for details on the Option I/O Menu and refer to ***Chapter 4 - Control and Status Commands*** for details on the **`cpuopts`** and **`cpuoptsconfig`** commands.

In addition to the standard connectors, the CPU module can be configured with optional outputs. These optional outputs include a Programmable TTL Output, a Synthesizer Output, an Alarm Output, and a second RS-232 serial port with a Sysplex output.



Programmable TTL Output

The Programmable TTL Output Option provides user-selectable, on-time pulse rates from 1 PPS to 10 MPPS, or a digital timecode. The output signal can be programmed for any of the various selections via the front-panel display by navigating to Main Menu > Option I/O > CPU-I/O > ProgTTL. Alternatively, you can change the output signal via the network or serial port by using console command **`cpuoptsconfig`**. Refer to Chapter 3 for details on the Option I/O Menu and refer to Chapter 4 for details on the **`cpuopts`** and **`cpuoptsconfig`** commands. For signal definition see ***Appendix J - Specifications***.

Direct Digital Synthesizer (DDS)

The Programmable TTL Output Option may be upgraded with the addition of the Direct Digital Synthesizer selection. This option provides user-selectable pulse rates from 1 PPS to 10 MPPS, programmable in 1 PPS steps, including 1.544 MPPS or 2.048 MPPS. The selected pulse rate is phase locked to the system oscillator. However, the DDS output is not aligned with system time.

If your Meridian has this option available then it will show up as "SYNTH" in the list of available selections for the Programmable TTL Output. The actual synthesizer frequency is set via the front-panel keypad by navigating to Main Menu > Option I/O > CPU-I/O > Synthesizer. Alternatively, you can change the synthesizer rate via the network or serial port by using console command **`cpuoptsconfig`** (see Chapter 4). For signal definition see ***Appendix J - Specifications***.

Fixed Rate TTL Output (10 MPPS, etc.)

The Fixed Rate Output Option provides an optional customer-specified fixed rate output ranging from 1 PPS to 10 MPPS, or a digital timecode. The rear-panel BNC will be labeled for the appropriate rate such as "10 MPPS" or "100 PPS", etc. This signal is specified by the customer when the order is placed, preset at the factory, and cannot be changed. There is no user interface status or control. For signal definition see ***Appendix J - Specifications***.

1 PPS (RS-422) Output

This option is provided on a second RS-232 serial port which replaces the two upper BNCs on the CPU Module. The pulse width is normally 1 millisecond wide when shipped from the factory but can be changed via the front-panel keypad or via the console command **`cpuoptsconfig`**. See details in ***Appendix J - Specifications*** for the 1PPS RS-422 output.

Serial Time Output

This option is provided on a second RS-232 serial port labeled "Serial Time". It replaces the two upper BNCs on the CPU Module. It is an output that provides a once-per-second sequence of ASCII characters indicating the current time. The "on-time" character is transmitted during the first millisecond of each second. The output starts automatically on power-up.

To configure this output refer to Chapter 3 for details on the Serial Time Output and refer to Chapter 4 for details on the **`cpusertime`** and **`cpusertimeconfig`** commands.

There are several different formats for this string. The format, baud rate and parity can all be changed via the front-panel keypad or via the console command **`cpusertimeconfig`**. Baud rate selections are 57600, 19200, 9600, and 4800. Parity selections are odd, even, and none. Format selections are Sysplex, Truetime, EndRun, EndRunX and NENA.

Sysplex Format

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

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

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

Truetime Format

The format of the Truetime string is identical to the Sysplex format. The only difference between the two is that the Sysplex format always uses UTC time. The time contained in the Truetime format depends on the time mode of the Meridian. (See Time Mode in ***Chapter 3 - Front-Panel Keypad and Display*** and `gsystimemodeconfig` in ***Chapter 4 - Control and Status Commands***.) For example, if you want an output with this string format that uses Local Time, then select the Truetime format.

EndRun Format

The following string is sent once each second:

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

T	is the Time Figure of Merit (TFOM) character described in ***Appendix A - TFOM***. This is the on-time character, transmitted during the first millisecond of each second.
YYYY	is the year
DDD	is the day-of-year
:	is the colon character (0x3A)
HH	is the hour of the day
MM	is the minute of the hour
SS	is the second of the minute
z	is the sign of the offset to UTC, + implies time is ahead of UTC.
ZZ	is the magnitude of the offset to UTC in units of half-hours. Non-zero only when the Timemode is Local (see Chapter 5).
m	is the Timemode character and is one of: G = GPS L = Local U = UTC
<CR>	is the ASCII carriage return character (0x0D)
<LF>	is the ASCII line feed character (0x0A)

EndRunX (Extended) Format

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

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

T	is the Time Figure of Merit (TFOM) character described in ***Appendix A - TFOM***. This is the on-time character, transmitted during the first millisecond of each second.
YYYY	is the year
DDD	is the day-of-year
:	is the colon character (0x3A)
HH	is the hour of the day
MM	is the minute of the hour
SS	is the second of the minute
z	is the sign of the offset to UTC, + implies time is ahead of UTC.
ZZ	is the magnitude of the offset to UTC in units of half-hours. Non-zero only when the Timemode is Local (see Chapter 5).
m	is the Timemode character and is one of: G = GPS L = Local U = UTC
CC	is the current leap seconds value.
FF	is the future leap seconds value.
<CR>	is the ASCII carriage return character (0x0D)
<LF>	is the ASCII line feed character (0x0A)

NENA Format

NENA is the National Emergency Number Association. This organization has adopted a format for use in PSAPs (Public Safety Answering Points). This format follows:

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

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

Alarm Output

The Alarm Output Option provides an open-collector output that indicates when the GPS receiver has lost lock, or when serious hardware faults are detected. For a detailed description of the faults see the ***Faults Display*** section in ***Chapter 3 - Front-Panel Keypad and Display.*** There is no user interface control for this option.

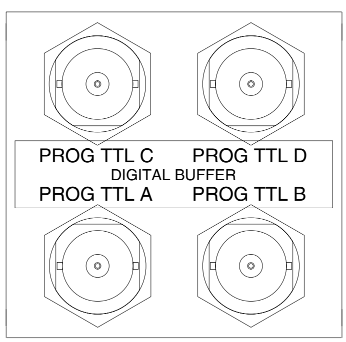
Care should be taken not to directly connect this open-collector output to a voltage source. A series current-limiting resistor of at least 1K ohms in value should be used. The pull-up voltage must not exceed 40V. For signal definition see ***Appendix J - Specifications***.

Plug-In Module Options

Your Meridian TimeBase is supplied with five option slots that can be configured with a variety of plug-in modules. Most of these modules can be added to the Meridian as "plug-and-play" options without hardware or software modification. At power-up, automatic recognition software detects the identity of any plug-in module installed and launches the corresponding software routines necessary to control and monitor the operation of each module. Standard plug-in modules are described below:

Programmable Digital Buffer Plug-in Module

The Programmable Digital Buffer Module is a "plug-and-play" option that adds four independently programmable TTL outputs to your Meridian TimeBase. These buffered outputs can provide on-time pulse rates from 1 PPS to 10 MPPS, or a digital timecode output. Each output can be individually programmed for any of the various selections via the front-panel display by navigating to Main Menu > Option I/O > OptCardx (see Chapter 3). To program the outputs via the network or serial port use console command **`pluginoptsconfig`** (see Chapter 4). For signal definition see ***Appendix J - Specifications***. The rear panel outputs are identified as PROG TTL A through D as shown below:



Digital Timecode Formats

If you have selected timecode as the output on the Digital Buffer Module then its format will be the same format as that on the standard CPU Module AM Code connector. This format can be changed via the front-panel display by navigating to Main Menu > Option I/O > CPU I/O > Code-Out (see Chapter 3). Alternatively, you can change the timecode format via the network or serial port by using console command **`cpuoptsconfig`** (see Chapter 4).

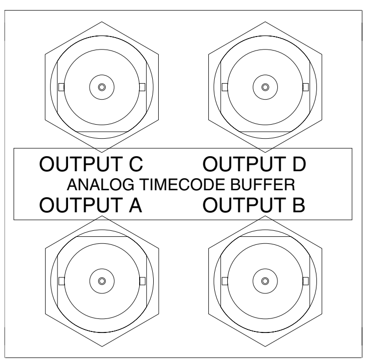
Direct Digital Synthesizer (DDS)

An additional upgrade to the Programmable Digital Buffer Module provides access to the DDS that is resident on the Meridian CPU module. Programmable synthesized pulse rates from 1 PPS to 10 MPPS in 1 PPS steps are available, including 1.544 MPPS or 2.048 MPPS. The pulse rate is phase locked to the system oscillator. However, the DDS output is not aligned with system time.

If your Meridian has this option available then it will show up as “SYNTH” in the list of available selections for the Programmable Digital Buffer outputs. The actual synthesizer frequency that is resident on the Meridian CPU module is set via the front-panel keypad by navigating to Main Menu > Option I/O > CPU I/O > Synthesizer. Alternatively, you can change the synthesizer rate via the network or serial port by using console command **`cpuoptsconfig`** (see Chapter 4).

Analog Timecode Buffer Plug-In Module

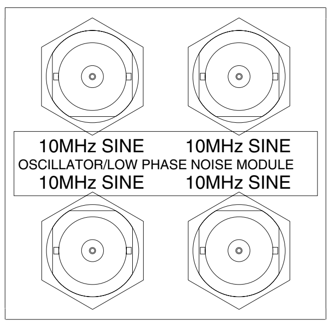
The Analog Timecode Buffer Module is a “plug-and-play” option that adds four additional timecode outputs to your Meridian TimeBase. These buffered outputs can provide synchronization of equipment such as synchronized generators, digital fault recorders, SCADA systems, and time displays, and are suitable for recording onto magnetic tape or for transmission over another medium such as coaxial cable. Available timecode formats are: IRIG-B120 (IEEE-1344), IRIG-B122, IRIG-B123, NASA-36, or 2137. All four output connectors use the same code format. The format is identical to that of the CPU Module AM Code output which is set via the front-panel display by navigating to Main Menu > Option I/O > CPU-I/O > Code-Out. Alternatively, you can change the timecode format via the network or serial port by using console command **`cpuoptsconfig`** (see Chapter 4). For signal definition see ***Appendix J - Specifications***. The rear panel outputs are identified as OUTPUT A through D as shown below:



Oscillator/Low Phase Noise Plug-In Module

The Meridian TimeBase can be configured with several high-performance, disciplined, 10-MHz oscillators. The Low Phase Noise Output Option works in conjunction with these oscillators to provide up to eight individually buffered, spectrally pure, sinewave outputs. The levels of the contributors to spectral impurity have been carefully controlled by the selection of the optional oscillators that are offered, and by the design of the option module and its integration into the Meridian chassis. In addition, very good channel-to-channel isolation has been achieved.

This plug-in module is not field-upgradeable and it always resides in Slot 1 (next to the CPU module). The rear-panel outputs are labeled with their configured frequency. These frequencies are not changeable but can be viewed via the front-panel display by navigating to Main Menu > Option I/O > OptCard1. You can also view the Low Phase Noise Output configuration via the network or serial ports by using console command **`pluginopts`** (see Chapter 4). For signal definition see ***Appendix J - Specifications***.



Appendix A

Time Figure-of-Merit (TFOM)

This appendix describes the Time Figure of Merit (TFOM) number. The Meridian displays this number on the front panel via the Receiver Status display (see Chapter 3). The TFOM is also printed out in the time-of-day fields printed by the Meridian **`gpsstat`** *and* **`gntpstat`** *commands (see Chapter 4). 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 locked to GPS

In all cases, the Meridian reports this value as accurately as possible, even during periods of GPS signal outage where the Meridian is unable to directly measure the relationship of its timing outputs to UTC. During these GPS outage periods, assuming that the Meridian had been synchronized prior to the outage, the Meridian extrapolates the expected drift of the Meridian 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 Meridian is unable to achieve re-synchronization within one hour after reaching this state, the red LED will illuminate. The fault status field returned in either of the **`gpsstat`** or **`gntpstat`** commands will have the appropriate bit set to indicate a loss-of-signal time-out condition.

If the GPS subsystem reaches the unsynchronized TFOM state, the NTP daemon will cease to use the timing information returned by the GPS subsystem in its polling event timestamps. At this point, the NTP daemon will report in its replies to network NTP clients that it is running at stratum 16 and the leap indicator bits will be set to the fault state. NTP clients will recognize that and cease to use the unsynchronized server.

Appendix 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 Meridian.

The firmware consists of two FLASH binary image files. One of these is the firmware for the Meridian itself. This firmware executes on the IBM-compatible CPU and contains the embedded Linux operating system and NTP specific application software. The other file is the firmware for the GPS time and frequency subsystem. Each of these files may be upgraded independently, although some upgrades require both images to be modified together.

What You Need To Perform the Upgrade

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

Performing the Linux/NTP Upgrade

There are two FLASH disk partitions which hold the compressed Linux root file system images. These partitions are raw FLASH blocks, have no file system and may not be mounted. They are accessed through low-level devices. To protect the factory root file system from accidental erasure or over-writing, the device node has been deleted. The upgrade FLASH disk partition is accessed via */dev/rootfs_1*. When performing an upgrade, you will be copying the new image to this device.

CAUTION

Some browsers will automatically unzip the gzip file when downloading from the website. Please make sure that the gzip file is less than 6M 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 re-programming.

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

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

```
eraserootfs_1
```

If you are using **ftp** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to */dev/rootfs_1* on your Meridian using FTP (substitute the name of the root file system image that you are installing for *rootfsupgrade.gz*): Issue these commands from the console of your Meridian:

```
ftp remote_host                        {perform ftp login on remote host}
bin                                    {set transfer mode to binary}
get rootfsupgrade.gz /dev/rootfs_1     {transfer the file}
quit                                   {close the ftp session after transfer }
```

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

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

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

```
updaterootflag 1
```

You should see this line displayed:

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

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

```
shutdown -r now
```

Wait about 30 seconds for the system to shutdown and re-boot. Then log in to the Meridian 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

```
gsysversion
```

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:

```
gsysrootfs
```

Which should cause this to be printed to the console:

```
BOOT_IMAGE=MeridianGPS_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 Meridian.

Recovering from a Failed Upgrade

To restore your Meridian to a bootable state using the factory root file system, you must use the serial I/O port and re-boot the Meridian by cycling the power. For setup details refer to sections ***Connect the Serial I/O Port*** and ***Test the Serial I/O Port*** in ***Chapter 2 - Basic Installation***. When you have connected your terminal to the serial I/O port, apply power to the Meridian.

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

```
To override and boot the FACTORY partition type 'FACTORY' within 5 seconds...
```

you must begin typing "factory" within five seconds to let the bootloader know that you are going to override the default root file system. After you hit <enter> the bootloader will boot the factory root file system. Watch the rest of the boot process to make sure that you have successfully recovered. If the system boots normally, then you should resolve the problems with the previous upgrade and re-perform it.

Performing the Linux Kernel Upgrade

If you want to upgrade your kernel to the IPv6-capable one then you must first be sure that your root file system is version 2.60 or later.

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

If you are using **ftp** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to a temporary location on your Meridian using FTP (substitute the name of the kernel image that you are installing for *newkernelimage*): Issue these commands from the console of your Meridian:

```
ftp remote_host                {perform ftp login on remote host}
bin                            {set transfer mode to binary}
get newkernelimage /tmp        {transfer the file}
quit                           {close the ftp session after transfer }
```

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

```
scp -p newkernelimage root@cntp.your.domain:/tmp
```

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

```
upgradekernel /tmp/newkernelimage
```

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

CAUTION

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

Performing the GPS Upgrade

To perform this upgrade, log in as the *root* user to the Meridian 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@gsys.your.domain:/tmp
```

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

```
upgradegps /tmp/gpsupgrade.bin
```

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

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

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

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

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

```
---Starting file upload, should take about 60 seconds...
```

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

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

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

The first message should be ignored. It is only reporting that one of the intermediate processes of the script execution has been terminated. The next message informs you that the GPS engine file transfer has completed, and that its start-up messages should appear. First the bootloader message will appear:

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

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

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

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

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

```
gpsversion
```

The upgraded version information should be displayed.

Problems with the GPS Upgrade

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

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

You should now see the ‘C’ character being received every three seconds. This is the character that the GPS engine bootloader sends to indicate to the XMODEM utility that it is wating for a download. You may now 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 re-transfer the binary file:

```
upgradegps /tmp/gpsupgrade.bin
```

Appendix C

Simple Network Management Protocol (SNMP)

Your Meridian includes the (NET)-SNMP version 5.3.1 implementation of an SNMP agent, **`snmpd`**, *and a SNMP notification/trap generation utility,* **`snmptrap`**. *It supports all versions of the protocol in use today: SNMPv1 (the original Internet standard), SNMPv2c (never reached standard status, often called "community SNMP") and SNMPv3 (the latest Internet standard).*

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

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

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

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

SNMPv3 Security

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

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

Enterprise Management Information Base (MIB)

In addition to providing the SNMP variables contained in MIB-II as described in RFC-1213, EndRun Technologies has implemented an enterprise MIB using the syntax of the SMI version 2 (SMIv2) as described in RFC-2578:

MERIDIAN-MIB

Which is located on your Meridian in this ASCII file:

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

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

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

Invocation of the SNMP daemon

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

```
snmpd –m “$MIBNAME” -Ls d -c /etc/snmpd.conf
```

By default, it will listen on port 161 for SNMP queries from the network management system. If you would like to have it listen on another port, you could edit the file by adding **`-p port`** to the end of this line, where **`port`** is the number of the port you would like for the agent to listen on. If you would like to disable starting of the **`snmpd`** daemon altogether, you can either remove this line or place a **#** character at the beginning of the line so that it will not be executed. (A very compact editor with WordStar command keystrokes is available on the system for this purpose: **`edit`**. If you start **`edit`** without giving it a file name to open, it will display its help screen, showing the supported keystrokes.)

IMPORTANT

After editing ***/etc/rc.d/rc.local***, you must copy it to the ***/boot/etc/rc.d*** directory and 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 overwritten.

Quick Start Configuration -- SNMPv1/v2c

You should be able to compile the MERIDIAN-MIB file on your SNMP management system and access the variables defined therein. The factory default community names are “MeridianGPS” 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  MeridianGPS
```

Configuring SNMPv1 Trap Generation

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

Configuring SNMPv2c Notifications and Informs

To have your Meridian 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 Meridian. 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 Meridian 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 (readable only by ***root***), so be sure to use **`cp -p`** when performing the copy. During the boot process, the files contained in the ***/boot/etc*** directory are copied to the working ***/etc*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Configuration of SNMPv3

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

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

The first file contains static configuration parameters that the agent uses to control access and to determine where to send notifications/traps. Other aspects of the agent's operation are also configurable in this file, but you should not need to modify those. To use the SNMPv3 capabilities of the Meridian, 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 meridianuser 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 *meridianuser* whose minimum security level will be authenticated but not encrypted, and who will have read-only access to the entire *iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).endRunTechnologiesMIB(13827)* branch of the SMI object tree. After adding the user lines to */etc/snmpd.conf*, copy it to the */boot/etc* directory using **cp -p**.

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

```
createUser root    MD5 endrun_1 DES endrun_1
createUser meridianuser SHA MeridianGPS
```

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 *meridianuser* to be created who may be authenticated using the Secure Hash Algorithm (SHA) with password *MeridianGPS*. Passwords and passphrases must have a *minimum* of 8 characters, or you will not be able to be authenticated.

IMPORTANT

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

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

IMPORTANT

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

Security

Your Meridian TimeBase 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 Meridian. Others are provided by the additional protocol servers selected for inclusion in your Meridian, 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 NET-SNMP implementation of the Simple Network Management Protocol (SNMP) daemon,* **`snmpd`**. *conforms to the latest Internet standard, known as SNMPv3, which also supports secure user authentication and session privacy. In addition, the Network Time Protocol daemon,* **`ntpd`** *supports client-server authentication security measures to deter spoofing of NTP clients by rogue NTP servers. This appendix describes these security measures and gives the advanced network administrator information that will allow custom configuration to fit specific security needs.*

Linux Operating System

The embedded Linux operating system running in the Meridian is based on kernel version 2.4.26 and version 10 of the Slackware Linux distribution. As such it supports a complete set of security provisions:

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

- Direct *root* logins are only permitted on the local RS-232 console or via SSH.

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

- 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 Meridian by a pair of shell scripts which ease configuration for the inexperienced user of Unix-like operating systems. These are **`accessconfig`** and **`inetd-config`**.

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

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

in.telnetd: ALL
sshd: ALL
snmpd: ALL

This tells **`tcpd`** to deny access to **`in.telnetd`** and **`sshd`** to all hosts not listed in the */etc/hosts.allow* file. The **`snmpd`** and **`sshd`** daemons also parse this file prior to granting access to a requesting host. Then the user is prompted to enter a list of hosts that will be granted access to **`in.telnetd, sshd`** and **`snmpd`**. These appear in the */etc/hosts.allow* as lines like this:

in.telnetd: 192.168.1.2, 192.168.1.3
sshd: 192.168.1.2, 192.168.1.3
snmpd: 192.168.1.2, 192.l68.1.3

This simple shell script handles the needs of most users, however the syntax of these two files supports elaborate configuration possibilities which are beyond the capabilites of this simple shell script. Advanced users who need these capabilities will need to edit these two files directly and then copy them to the */boot/etc* directory. (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, three servers are configurable via **`inetdconfig`**: TIME and DAYTIME, whose daemons are contained within the **`inetd`** daemon itself, and **`in.telnetd`**. Any one or all of these may be enabled or disabled for start-up.

OpenSSH

The secure shell protocol server running in the Meridian is based on the portable OpenSSH 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: http://www.openssh.com.

An excellent book which describes operation and configuration of the various SSH implementations, including OpenSSH is available from O'Reilley & Associates:

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

In the interest of conserving scarce system memory resources, only the secure shell server daemon, **sshd** and the secure copy utility, **scp**, are implemented in the Meridian. This means that users on remote hosts may log in to the Meridian via an **ssh** client, but users logged in on the Meridian 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 Meridian via **scp** over **ssh** but users logged in on the Meridian 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 Meridian 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 Meridian. 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 Meridian. 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 Meridian. At boot time, the Meridian 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 Meridian. 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 Meridian is built from the standard distribution from the http://www.ntp.org site. By factory default, remote control of the NTP daemon **ntpd** is disabled. Query-only operation is supported from the two NTP companion utilities **ntpq** and **ntpdc**.

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

restrict default nomodify

This line eliminates control access from ALL hosts. Query access is not affected by this restriction. Knowledgable NTP users who would like to customize the security aspects of the configuration of the NTP daemon in the Meridian 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 E

Setting Up NTP Clients on Unix-like Platforms

To configure your Unix-like computer to use your Meridian NTP interface, you must have successfully configured the Meridian NTP Server as per the instructions in ***Chapter 5 - Setting Up The NTP Server****. This manual is not a 'How-To' on installing and using NTP; basic approaches to NTP client configuration for operation with the Meridian 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

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

Three methods of using the Meridian 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 Meridian 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 Meridian 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 Meridian server. Use the NTP utility **`ntpq`** to check that **`ntpd`** is able to communicate with the Meridian. 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 Meridian 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 Meridian 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 Meridian on your network.
- Your Meridian has been configured to perform authentication either by factory default, or by running the **`ntpconfig`** shell script. The example Meridian authentication configuration shown in ***Chapter 5 - Setting Up The NTP Server*** 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 Meridian. You can **telnet** into your Meridian and start an **ftp** session with your client computer to send the Meridian'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 Meridian 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 Meridian server with MD5 authentication. Use the NTP utility **ntpq** to check that **ntpd** is able to communicate with the Meridian. 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 Meridian 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 Meridian 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 Meridian on your network.

- Your Meridian 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 Meridian 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 Meridian configuration shown in ***Chapter 5 - Setting Up the NTP Server*** 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 Meridian server has been configured to use key 2 for broadcast authentication as shown in the example in ***Chapter 5 - Setting Up the NTP Server***, 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 Meridian as a broadcast or multicast server. Use the NTP utility **`ntpq`** to check that **`ntpd`** is able to communicate with the Meridian. 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 Meridian 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 Meridian 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.

Appendix *F*

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

*To configure your Windows NT 4.0/2000/XP computer to use your Meridian NTP interface, you must have successfully configured the Meridian NTP Server as per the instructions in **Chapter 5 - Setting Up the NTP Server**. This manual is not a 'How-To' on installing and using NTP; basic approaches to NTP configuration for operation with the Meridian 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

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

Three methods of using the Meridian 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 Meridian 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 Meridian on your network.
- You have installed NTP on your client computer.

Configure NTP

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

```
server 192.168.1.245
```

This line tells **`ntpd.exe`** to use the NTP server at address 192.168.1.245 in addition to any other servers which might also be configured in the *ntp.conf* file.

Re-start **`ntpd.exe`** to have it begin using the Meridian 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 Meridian. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT/2000/XP partition. From a console window, after issuing the command

```
ntpq
```

you will see the **`ntpq.exe`** command prompt:

```
ntpq>
```

Use the command

```
peers
```

to display the NTP peers which your computer is using. One of them should be the Meridian 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 Meridian 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 Meridian on your network.

- Your Meridian has been configured to perform authentication either by factory default, or by running the **`ntpconfig`** shell script. The example Meridian authentication configuration shown in ***Chapter 5 - Setting Up the NTP Server*** will be assumed in the example configuration commands shown here.

- You have installed NTP on your client computer.

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

Create the ntp.keys File

You must create a file named *ntp.keys* in the *\winnt\system32\drivers\etc* directory or, for XP, the *\windows\system32\drivers\etc* directory. It must be a copy of the one residing in the */etc* directory of your Meridian. You can **`telnet`** into your Meridian and start an **`ftp`** session with your client computer to send the Meridian */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 Meridian server, you should create your own keys after you understand the process and have your clients operating correctly with the default file.

IMPORTANT

Handling of the ***\windows\system32\drivers\etc\ntp.keys*** file is the weak link in the MD5 authentication scheme. It is very important that it is owned by "administrator" and not readable by anyone other than "administrator".

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

Configure NTP

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

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

Modify the line added previously in ***Basic NTP Client Setup*** so that authentication will be used with the Meridian 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 Meridian 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 Meridian. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT/2000/XP partition. From a console window, after issuing the command

```
ntpq
```

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

```
ntpq>
```

Use the command

```
peers
```

to display the NTP peers which your computer is using. One of them should be the Meridian 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 Meridian 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 Meridian on your network.

- Your Meridian 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 Meridian 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 Meridian configuration shown in ***Chapter 5 - Setting Up the NTP Server*** 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 or, for XP, the *\windows\system32\drivers\etc* directory. Assuming that your Meridian server has been configured to use key 2 for broadcast authentication as shown in the example in ***Chapter 5 - Setting Up the NTP Server***, 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 Meridian 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 Meridian. By default it is installed in the *\Program Files\Network Time Protocol* sub-directory of your Windows NT/2000/XP partition. After issuing the command

```
ntpq
```

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

```
ntpq>
```

Use the command

```
peers
```

to display the NTP peers which your computer is using. One of them should be the Meridian 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 Meridian server. If you see “bad”, you should wait a few minutes to be sure that there is a problem since “bad” is the initial state of this setting. If the “bad” indication persists then you must check your configuration for errors. Typically this is due to a typing error in creating the *\windows\system32\drivers\etc\ntp.keys* file on the client that causes a mismatch between the keys being used by the server and client. (If you transfer the file by **`ftp`** or **`scp`**, this shouldn’t be a problem.) It is also possible to have a typing error in the *\windows\system32\drivers\etc\ntp.conf* file that causes the needed key to not be included in the “trustedkey” list.

Appendix G

Timecode Formats

A standard feature of your Meridian TimeBase is a single timecode output available at the rear panel BNC connector identified as AM CODE. A DC-shift timecode output is available via the optional Programmable TTL Output on the CPU Module (see ***CPU Module Options*** *in* ***Chapter 6 - Optional Rear-Panel Outputs****). Multiple timecode outputs (both AM and DC-shift) are also available via an option board module (see* ***Plug-In Module Options*** *in* ***Chapter 6****).*

The output code format is selectable via the front-panel user interface. See ***Timecode Output Setup*** *in* ***Chapter 3 - Front-Panel Keypad and Display****. You can also select the timecode format via a console command. See* ***CpuOpts*** *in* ***Chapter 4 - Control and Status Commands****. Each format is described below. Time codes are commonly used to provide time information to external devices such as displays, magnetic tape devices, strip chart recorders and several types of embedded computer peripheral cards.*

IRIG-B122/002

This is the most widely used format and is normally the factory default for the AM Code output. The IRIG-B122 format is a 100 pps code and is used to amplitude modulate a 1000 kHz sine wave carrier. The information contained in the timecode is seconds through day-of-year coded in Binary Coded Decimal (BCD). Reference IRIG Document 104-60.

IRIG-B123/003

In addition to the time information identified in B122 above, this format also contains Straight Binary Seconds (SBS) of day. SBS is provided at the end of the frame, in the 17 bits starting in position 80.

IRIG-B120/000 (IEEE-Standard 1344-1995)

In addition to the time data and the Straight Binary Seconds data this format provides for time/status data in the control bit positions of IRIG-B. The information provided there is defined by IEEE standard 1344-1005: Unit and Tens of Years, Leap Second, Daylight Savings, Local Time Offset, Time Quality and Parity. The IEEE-1344 table provided below shows each bit position with detailed information.

NASA-36

NASA-36 bit time code is a 100-bit, pulse width modulated format used to amplitude modulate a 1000 kHz sine wave carrier. The information contained in the timecode is seconds, minutes, hours and days. The format is used by several military ranges. Reference IRIG Document 104-59.

2137

The 2137 code is a 25-bit pulse width modulated format used to amplitude modulate a 1000 kHz sine wave carrier. The information contained in the timecode is seconds, minutes and hours. The format is used by certain security organizations.

IEEE-1344 Bit Definition

Bit Position	Bit Definition	Explanation
P50	Year, BCD1	Unit years
P51	Year, BCD2	
P52	Year, BCD4	
P53	Year, BCD8	
P54	Not used	
P55	Year, BCD10	Tens years
P56	Year, BCD20	
P57	Year, BCD40	
P58	Year, BCD80	
P59	P6	Position identifier
P60	Leap second pending	Set to one, 59 seconds prior to leap insertion
P61	Leap second	0 = add second, 1 = delete second
P62	Daylight Savings Time pending	Set to one, 1 second prior to DST change
P63	Daylight Savings Time	1 = DST active
P64	Local offset sign	0 = +, 1 = -
P65	Local offset binary 1	Local offset from UTC time
P66	Local offset binary 2	
P67	Local offset binary 4	
P68	Local offset binary 8	
P69	P7	Position identifier
P70	Local offset half hour bit	0 = none, 1 = half hour time offset added
P71	Time quality binary 1	Time quality indicates clock precision.*
P72	Time quality binary 2	
P73	Time quality binary 4	
P74	Time quality binary 8	
P75	Parity	Odd parity for all preceding data bits
P76-P78	Not used	
P79	P8	Position identifier

* Refer to Appendix A - Time Figure-of-Merit for detailed information. Briefly:

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

Appendix H

IPv6 Information

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

To determine which kernel resides in your Meridian check the firmware version using the front-panel keypad/display. Or you can use the console port command **`cat /proc/version`**.

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

6010-0041-000 ver 2.4.26-1

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

6010-0041-100 ver 2.4.31-IPv6

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

Enabling New IPv6 Capabilities

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

OpenSSH

By default, **`sshd`** is factory-configured to listen on both IPv4 and IPv6 addresses. It may be forced to listen on either IPv4 only, or IPv6 only by editing the */etc/rc.d/rc.inet2* startup script, where **`sshd`** is started, and then copying it to */boot/etc/rc.d*.

Net-SNMP

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

IPv6-Capable syslog-ng

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

IPv4-Only Protocols

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

Appendix*I*

Third-Party Software

The Meridian is running several different software products created and/or maintained by open source projects. Open source software comes with its own license. These are printed out for your information below.

The license for the GNU software project requires that we provide you with a copy of all source code covered under the GNU Public License (GPL) at your request. Please contact us with your request and we will mail it to you on a CD. We will charge you a fee for our incurred expenses as allowed for in the license.

GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989,1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

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

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

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

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

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

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

NO WARRANTY

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

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

END OF TERMS AND CONDITIONS

NTP Software License

Information about the NTP Project, led by Dr. David Mills, can be found at www.ntp.org. The distribution and usage of the NTP software is allowed, as long as the following copyright notice is included in our documentation:

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


```
*************************************************************
*                                                           *
* Copyright (c) David L. Mills 1992-2006                    *
*                                                           *
* Permission to use, copy, modify, and distribute this software and *
* its documentation for any purpose with or without fee is hereby *
* granted, provided that the above copyright notice appears in all *
* copies and that both the copyright notice and this permission *
* notice appear in supporting documentation, and that the name *
* University of Delaware not be used in advertising or publicity *
* pertaining to distribution of the software without specific, *
* written prior permission. The University of Delaware makes no *
* representations about the suitability this software for any *
* purpose. It is provided “as is” without express or implied *
* warranty.                                                 *
*                                                           *
*************************************************************
```

Appendix J

Specifications

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

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

Local Oscillator:
TCXO is standard ($2.5x10^{-6}$ over -20º to 70º C).
Options: Medium-Stability OCXO (MS-OCXO) ($4x10^{-9}$ over 0º to 70º C).
High-Stability OCXO (HS-OCXO) ($1x10^{-9}$ over 0º to 70º C).
Rubidium (Rb) ($1x10^{-9}$ over -20º to 70º C).
Rubidium (HS-Rb) ($1x10^{-10}$ over -20º to 70º C).

NTP Stratum 1 Holdover Performance:
24 Hours - TCXO
35 Days - MS-OCXO
35 Days - HS-OCXO
140 Days - Rb
400 Days - HS-Rb

Time to Lock:
< 5 minutes, typical (TCXO).
< 10 minutes, typical (OCXO/Rb).

Alphanumeric Display/Keypad:
Display: Brilliant 16x280 dot-matrix vacuum-fluorescent.
Keypad: Enter, Back, Edit, Right, Left, Up, Down, Help.

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

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

1 PPS Output:

Signal: Positive TTL pulse into 50Ω.
User-Selectable Width: 20 us, 1 ms, 100 ms, 500 ms.
User Calibration: +/- 500 us, 1 ns resolution.
Accuracy: <10 nanoseconds RMS to GPS Time when locked.*
Alignment: Within 10 ns of the other TTL outputs in this unit (except the optional DDS).
Stability: TDEV < 10 ns, $\tau < 10^5$ seconds, $\sigma_y(\tau) < 1x10^{-13}$ @ $\tau=10^5$ secs.
Connector: Rear-panel BNC jack labeled "1PPS".

***** <100 nanoseconds to UTC. Constraints in the official GPS specification prohibit anyone from claiming an accuracy to UTC better than 100 nanoseconds.

Timecode Output:

Signal: Amplitude-modulated (AM), 3:1 ratio, 1 kHz carrier.
Drive: 1 Vrms into 50Ω.
User-Selectable Formats: IRIG-B120 (IEEE-1344), IRIG-B122, IRIG-B123, NASA-36, or 2137.
Connector: Rear-panel BNC jack labeled "AM CODE".

NTP Synchronization Accuracy:

NTP Timestamp Accuracy: <10 microseconds @ 200 packets/second (200,000 clients).
NTP Client Synchronization Accuracy: Network factors can limit LAN synchronization accuracy to 1/2 to 2 milliseconds, typical.

Maintenance Console:

RS-232 serial I/O on rear panel DB9M plug for secure, local terminal access.
Parameters fixed on 19200 baud, 8 data bits, no parity, 1 stop bit.
See ***RS-232 Serial I/O Port Signal Definitions*** in ***Chapter 4*** for more information.

Supported IPv4 Network Protocols:

SNTP, NTP v2, v3, v4 and broadcast/multicast mode; MD5 authentication and autokey
SSH server with "secure copy" utility, SCP
SNMP v1, v2c, v3 with Enterprise MIB
TIME and DAYTIME server
TELNET client/server
FTP client
DHCP client
SYSLOG

Supported IPv6 Network Protocols:

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

Power:

90-132 VAC/180-264 VAC, 47-63 Hz, 0.5 A Max. @ 120 VAC, 0.25 A Max. @ 240 VAC
3-Pin IEC 320 on rear panel, 2 meter line cord is included.

DC Power (option):

12 VDC (10-20 VDC), 5A maximum.
24 VDC (19-36 VDC), 2.5A maximum.
48 VDC (37-76 VDC), 1.5A maximum.
125 VDC (70-160 VDC), 0.75A maximum.
3-position terminal block on rear panel: +DC IN, SAFETY GROUND, -DC IN
(Floating power input: Either "+" or "-" can be connected to earth ground.)

Size:

Chassis:	1.75"H x 17.0"W x 10.75"D
Antenna:	3.5" Dia. x 2.5" H
Weight:	< 10 lb. (4.50 kg.)

Environmental:

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

Optional Programmable TTL Pulse Rate Outputs (on CPU Module):

See ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Signal: Positive TTL pulse @ 50Ω on BNC jack.
Rate: User selectable to 1, 10, 100, 1K, 10K, 100K, 1M, 5M, 10M PPS and Timecode.
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Alignment: Within 10 ns of the other TTL outputs in this unit (except the optional DDS).
Synthesized Rate: 1 PPS to 10 MPPS in 1PPS steps with optional DDS Upgrade.
Stability: See Stability (Allan Deviation) Table below.
Connector: Rear-panel BNC jack labeled "PROG TTL".

Optional TTL Fixed Pulse Rate Output (on CPU Module):

See ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Signal: Positive TTL pulse @ 50Ω on BNC jack.
Rate: Preset at factory and cannot be changed.
Accuracy: $< 10^{-13}$ to UTC for 24-hour averaging times when locked.
Alignment: Within 10 ns of the other TTL outputs in this unit (except the optional DDS).
Stability: See Stability (Allan Deviation) Table below.
Connector: Rear-panel BNC jack labeled with appropriate rate such as: "10 MPPS".

Optional Alarm Output (on CPU Module):

See ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Alarm: MMBT2222A open collector, grounded emitter. High impedance in alarm state.
Voltage: 40 VDC, maximum.
Saturation Current: 100 mA, maximum.
Connector: Rear-panel BNC jack or terminal strip labeled "ALARM".

Optional Sysplex/Serial Time Output (on CPU Module):

See ***Serial Time Output*** in ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Signal: Output only port at RS-232 levels.
Pinout: Pin 3 is Transmit Data. Pin 5 is GND.
Baud Rate: User-selectable to 4800, 9600, 19200 or 57600.
Parity: User-Selectable to Odd, Even or None.
ASCII Formats: User-Selectable to Sysplex, Truetime, EndRun, EndRunX or NENA.
Connector: Rear-panel DB-9M connector labeled: “SYSPLEX” or “SERIAL TIME”.

Optional 1 PPS (RS-422) Output (on CPU Module):

Signal: RS-422 levels.
User-Selectable Width: 20 us, 1 ms, 100 ms, 500 ms.
User Calibration: +/- 500 us, 1 ns resolution.
Accuracy: <10 nanoseconds RMS to GPS Time when locked.*
Alignment: Within 10 ns of the TTL outputs in this unit (except the optional DDS).
Stability: TDEV < 10 ns, $\tau < 10^5$ seconds, $\sigma_y(\tau) < 1x10^{-13}$ @ $\tau=10^5$ secs.
Connector: Rear-panel BNC jack labeled “1PPS RS-422”.
Pinout: Pin 3 is +signal. Pin 6 is -signal. Pin 5 is GND.

Optional Programmable Digital Buffer Module Outputs:

See ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Quantity: Four outputs.
On-Time Pulse Rates:
- Drive: TTL into 50Ω.
- Duty Cycle: 50%.
- Rate: User selectable to 1, 10, 100, 1K, 10K, 100K, 1M, 5M, 10M PPS.
- Alignment: Within 10 ns of the other TTL outputs in this unit (except the optional DDS).
- Stability: See Stability (Allan Deviation) Table below.

Digital Timecode:
- Drive: TTL into 50Ω (DC level shift).
- Format: User-selectable to IRIG-B (002, 003, IEEE-1344 compliant), NASA-36, or 2137.
- Alignment: Within 10 ns of the other TTL outputs in this unit (except the optional DDS).

Synthesized Rate: 1 PPS to 10 MPPS in 1 PPS steps with optional DDS Upgrade.
Connector: Rear-panel BNC jack.

Optional Analog Timecode Buffer Module Outputs:

See ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Quantity: Four outputs.
Analog Timecode:
- Drive: 1 Vrms into 50Ω.
- Frequency: 1 kHz.
- User-Selectable Formats: IRIG-B (122, 123, IEEE-1344 compliant), NASA-36, and 2137.

Connector: Rear-panel BNC jack.

Optional Oscillator/Low Phase Noise Module Outputs:

See ***Chapter 6 - Optional Rear-Panel Outputs*** for more information.
Quantity: 4 (uses one slot) or 8, 12, 16 or 20 (requires additional slots).
Output Frequency: 5 MHz or 10 MHz.
Output Level: +13 dBm, +/- 2 dBm at 50Ω.
Harmonics: < -45 dBc at 50Ω.
Channel-to-Channel Isolation: > +75 dB
Stability: See Stability (Allan Deviation) Table below.
Connector: Rear-panel BNC jack.
Phase Noise dBc/Hz @ 10 MHz:

Hz	*TCXO*	*Spurs*
1	-70	-100
10	-100	-100
100	-125	-100
1 k	-135	-100
10 k	-140	-100
100 k	-145	-120

Hz	*MS-OCXO*	*HS-OCXO*	*Rb/HS-Rb*	*Spurs*
1	-95	-105	-80	
10	-120	-130	-100	-120
100	-135	-140	-135	-115
1 k	-145	-150	-145	-125
10 k	-145	-150	-145	-125
100 k	-145	-150	-145	-110

Stability (Allan Deviation) Table:

(Does NOT pertain to the Synthesized Rates (Optional DDS Outputs).)

Tau in Seconds	**TCXO**	**MS-OCXO**	**HS-OCXO**	**Rb**	**HS-Rb**
1	$1x10^{-9}$	$7x10^{-12}$	$4x10^{-12}$	$2x10^{-11}$	$2x10^{-11}$
10	$5x10^{-10}$	$9x10^{-12}$	$4.5x10^{-12}$	$6.7x10^{-12}$	$6.7x10^{-12}$
100	$1x10^{-10}$	$1.8x10^{-11}$	$8.5x10^{-12}$	$2.5x10^{-12}$	$2x10^{-12}$
1000	$1x10^{-11}$	$1x10^{-11}$	$7x10^{-12}$	$1.4x10^{-12}$	$9x10^{-13}$
10000	$1x10^{-12}$	$1x10^{-12}$	$1x10^{-12}$	$8x10^{-13}$	$5x10^{-13}$
100000	$1x10^{-13}$	$1x10^{-13}$	$1x10^{-13}$	$1x10^{-13}$	$1x10^{-13}$

CE/FCC Compliance:

R&TTE Directive 99/5/EEC
Low Voltage Directive 73/23/EEC
EMC Directive 89/336/EEC
With Amendment 93/68/EEC

Supplementary Compliance Data:

- **Safety:** EN 60950:2000 (3rd Edition)
- **EMC:** EN55022:1998 Class A, VCCI (April 2004) Class A, FCC Part 15 Subpart B Class A, ICES-003 Class A, EN 50024:1998 w/ A1:2001 and A2:2003, EN61000-3-2:2000, EN61000-3-3:1995 w/ A1:2001

EndRun
TECHNOLOGIES

DECLARATION OF CONFORMITY

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

Manufacturer's Name: ***EndRun Technologies***

Manufacturer's Address: ***1360 North Dutton Avenue #200,***
Santa Rosa, CA 95401

DECLARES, THAT THE PRODUCT

Product Name: ***Precision GPS Time Base***

Model Number: ***Meridian***

CONFORMS TO THE FOLLOWING EUROPEAN DIRECTIVES

R&TTE Directive 99 / 5 / EEC
Low Voltage Directive 73 / 23 / EEC
EMC Directive 89 / 336 / EEC
With Amendment 93 / 68 / EEC

Supplementary Information:

Safety : ***EN 60950:2000 (3rd Edition)***
EMC: ***EN 55022:1998, Class A; VCCI (April 2004) Class A***
FCC Part 15 Subpart B Class A; ICES-003 Class A
EN 55024:1998,(w/A1:2001 & A2:2003
EN 61000-3-2:2000; EN 61000-3-3:1995 w/A1:2001

Year Mark First Applied: ***2005***

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

Place: Santa Rosa, CA USA
Signature:
Date: March 31, 2005
Full Name: David J. Lobsinger
Position: V.P. Hardware Engineering

Appendix K

Software Release Notes for Previous Meridian Users

Version 2.60 of the Linux root file system (RFS) and the new IPv6-capable Linux 2.4.31-IPV6 kernel are now shipping in new products. Both files are also available for download so that you can upgrade your installed units in the field. This is a major upgrade, and features updated versions of all applications, utilities and shared libraries typically installed in an embedded Linux-based system. In addition, the critical open source protocol implementations, NTP, OpenSSH, Net-SNMP and Syslog-ng are now IPv6-capable, along with other various support daemons and configuration utilities that need to understand IPv6 addresses. The NTP implementation is now capable of "autokey" cryptographic operation. Previously, only symmetric MD5 cryptography was available.

Easy Field-Installable Upgrade

The new system detects the presence of an IPv6-capable kernel and enables the IPv6 configuration menus and command line utilities automatically. As with all of our firmware upgrades, we have designed the upgrade to be as seamless as possible for existing customers, which means that after applying the update, your existing configuration settings and passwords will continue to function properly. However, due to the magnitude of the changes included in this upgrade, there are a couple of cases where configuration files must be re-configured:

If You Are Using DHCP

The new version DHCP client daemon included in the 2.60 RFS will by default overwrite the /etc/ntp.conf. This will cause serious problems. If you have a pre-existing */boot/etc/rc.d/rc.inet1* that is set up to invoke **dhcpcd** to configure the ethernet interface, you will need to re-run **netconfig** immediately after performing the upgrade and re-boot. This will replace the old */boot/etc/rc.d/rc.inet1* with a new one that will invoke **dhcpcd** with the appropriate arguments to inhibit this behavior.

If You Are Operating NTP Without MD5 Authentication

The new version NTP server daemon included in the 2.60 RFS interprets certain keywords in the "restrict" directive differently than the previous version. In particular, it will now interpret the "notrust" keyword to mean that it will not reply to client requests that do not use authentication (MD5 or autokey). Previous versions of the NTP server did not operate this way. If you have a pre-existing */boot/etc/ntp.conf*, and any of your NTP clients are configured to not use MD5 authentication, you should re-run **ntpconfig** immediately after performing the upgrade and re-boot. This will replace the old */boot/etc/ntp.conf* with a new one that will have the "notrust" keyword removed from the "restrict" directive. The new file will also contain the "keysdir" directive to support operation with autokey.

Freedom of Choice

EndRun Technologies understands that IPv6 is still in the experimental stage with essentially no mainstream deployment. Customers who are not interested in IPv6 need not perform the Linux

2.4.31-IPV6 kernel upgrade procedure, and your systems will continue to behave as before. Customers buying new products may choose to have the IPv6-capable kernel installed at the factory. The default will be the previous Linux 2.4.26 IPv4-only kernel.

Performing the Upgrade

Performing the 2.60 RFS upgrade is identical to the current procedure (see your User Manual, Appendix B, Performing the Linux/NTP Upgrade), and must be performed first if you are also planning to upgrade your kernel. The IPv6 Linux 2.4.31 kernel upgrade procedure is new, and a new utility, **upgradekernel** has been added to the 2.60 RFS to facilitate and failsafe this procedure. First you need to upload the new compressed kernel image file to a temporary location on the file system, using scp. (Alternatively, you could **ftp** from your timeserver to an ftp server on your network and download the file). Then the kernel upgrade utility is executed with a single argument passed on the command line: the path to the previously uploaded kernel image file. Like this, for example:

```
upgradekernel /tmp/newkernelimage
```

The kernel upgrade utility verifies the integrity of the file, reads the kernel version information, presents it to you and asks you to verify before replacing the old kernel image. If you verify, it will then erase the old image and write the new one in its place. The erase and write operation takes about 10 seconds. ***A power failure during this time would render the unit unbootable, so it is highly advisable to plug the unit into a UPS while performing the upgrade.***

Enabling New IPv6 Capabilities

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

OpenSSH

Starting with the 2.60 RFS, **sshd** is no longer started by the superserver daemon, **inetd**. If you have a previously reconfigured */boot/etc/inetd.conf*, the */etc/rc.d/rc.inet2* startup script will detect it and remove the line that allows **sshd** to be started by **inetd**. By default, **sshd** is factory configured to listen on both IPv4 and IPv6 addresses. It may be forced to listen on either IPv4 only, or IPv6 only by editing the */etc/rc.d/rc.inet2* startup script, where **sshd** is started, and then copying it to */boot/etc/rc.d*.

Net-SNMP

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

The 2.60 RFS now contains the Net-SNMP open source implementation, which replaces the older UCD-SNMP implementation, which did not support IPv6. There are several new directives in the */etc/snmpd.conf* related to IPv6. If you are upgrading and you need IPv6 capability with SNMP, you should merge any changes that you may have made to the previous *snmpd.conf* file (which would be stored in */boot/etc/snmpd.conf*) into the new *snmpd.conf* file, like trapsink addresses and community strings. Using the new *snmpd.conf*, you can set up any IPv6 trapsink addresses. If you are using snmpv3 secure access, you will need to perform the **`createUser`** operations to the new /boot/net-snmp/snmpd.conf persistent configuration file. The older */boot/ucd-snmp* directory is no longer used for this.

New IPv6-Capable syslog-ng

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

Remaining IPv4-Only Protocols

There remain several protocols in the 2.60 RFS which are not IPv6 capable: **`telnet`** (client and server), **`ftp`** and **`dhcpcd`**. Due to their intrinsic insecurity, **`telnet`** and **`ftp`** are rapidly being deprecated, and probably have little business running over an IPv6 network. The address autoconfiguration capabilities of IPv6 make the DHCP protocol less important, however it is likely that the new **`dhcpv6`** capability will appear in a future upgrade.

Special Modifications

Changes for Customer Requirements

From time to time EndRun Technologies will customize the standard Meridian Precision GPS Time-Base for special customer requirements. If your unit has been modified then this section will describe what those changes are.

This section is blank.

EndRun
TECHNOLOGIES
"Smarter Timing Solutions"

1360 N. Dutton Ave. Suite 200
Santa Rosa, CA 95401
TEL 1-877-749-3878
FAX 707-573-8619
www.endruntechnologies.com