SPECTRACOM

PUBLIC SAFETY) SECURITY) GOVERNMENT

MODEL TTS 200

GPS Time Server

INSTRUCTION MANUAL

95 Methodist Hill Drive
Suite 500
Rochester, NY 14623

Phone: 585.321.5800
Fax: 585.321.5219

www.spectracomcorp.com

Revisions, if any, are located at the end of the manual.

Part number 1125-5000-0050
Manual Revision C
December 2004

Current to software version 2.2.0

SPECTRACOM 5-YEAR WARRANTY

LIMITED WARRANTY

Spectracom warrants each new product manufactured and sold by it to be free from defects in software, material, workmanship, and construction, except for batteries, fuses, or other material normally consumed in operation that may be contained therein AND AS NOTED BELOW, for five years after shipment to the original purchaser (which period is referred to as the "warranty period"). This warranty shall not apply if the product is used contrary to the instructions in its manual or is otherwise subjected to misuse, abnormal operations, accident, lightning or transient surge, repairs or modifications not performed by Spectracom.

The GPS receiver is warranted for one year from date of shipment and subject to the exceptions listed above. The power adaptor, if supplied, is warranted for one year from date of shipment and subject to the exceptions listed above.

THE ANALOG CLOCKS ARE WARRANTED FOR ONE YEAR FROM DATE OF SHIPMENT AND SUBJECT TO THE EXCEPTIONS LISTED ABOVE.

THE TIMECODE READER/GENERATORS ARE WARRANTED FOR ONE YEAR FROM DATE OF SHIPMENT AND SUBJECT TO THE EXCEPTIONS LISTED ABOVE.

The Rubidium oscillator, if supplied, is warranted for two years from date of shipment and subject to the exceptions listed above.

All other items and pieces of equipment not specified above, including the antenna unit, antenna surge suppressor and antenna pre-amplifier are warranted for 5 years, subject to the exceptions listed above.

WARRANTY CLAIMS

Spectracom's obligation under this warranty is limited to in-factory service and repair, at Spectracom's option, of the product or the component thereof, which is found to be defective. If in Spectracom's judgment the defective condition in a Spectracom product is for a cause listed above for which Spectracom is not responsible, Spectracom will make the repairs or replacement of components and charge its then current price, which buyer agrees to pay.

Spectracom shall not have any warranty obligations if the procedure for warranty claims is not followed. Users must notify Spectracom of the claim with full information as to the claimed defect. Spectracom products shall not be returned unless a return authorization number is issued by Spectracom.

Spectracom products must be returned with the description of the claimed defect and identification of the individual to be contacted if additional information is needed. Spectracom products must be returned properly packed with transportation charges prepaid.

Shipping expense: Expenses incurred for shipping Spectracom products to and from Spectracom (including international customs fees) shall be paid for by the customer, with the following exception. For customers located within the United States, any product repaired by Spectracom under a "warranty repair" will be shipped back to the customer at Spectracom's expense unless special/faster delivery is requested by customer.

Spectracom highly recommends that prior to returning equipment for service work, our technical support department be contacted to provide trouble shooting assistance while the equipment is still installed. If equipment is returned without first contacting the support department and "no problems are found" during the repair work, an evaluation fee may be charged.

EXCEPT FOR THE LIMITED WARRANTY STATED ABOVE, SPECTRACOM DISCLAIMS ALL WARRANTIES OF ANY KIND WITH REGARD TO SPECTRACOM PRODUCTS OR OTHER MATERIALS PROVIDED BY SPECTRACOM, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Spectracom shall have no liability or responsibility to the original customer or any other party with respect to any liability, loss, or damage caused directly or indirectly by an Spectracom product, material, or software sold or provided by Spectracom, replacement parts or units, or services provided, including but not limited to any interruption of service, excess charges resulting from malfunctions of hardware or software, loss of business or anticipatory profits resulting from the use or operation of the Spectracom product or software, whatsoever or howsoever caused. In no event shall Spectracom be liable for any direct, indirect, special or consequential damages whether the claims are grounded in contract, tort (including negligence), or strict liability.

EXTENDED WARRANTY COVERAGE

Extended warranties can be purchased for additional periods beyond the standard five-year warranty. Contact Spectracom no later than the last year of the standard five-year warranty for extended coverage.

Table of Contents

List of Figures

List of Tables

1 General Information

1.1 Introduction

Spectracom Corporation is a leading manufacturer of synchronized, precise time-keeping devices meeting the demands for accuracy, reliability and trace ability in mission-critical systems across networks. Our NetClock is a direct response to customer needs for cutting-edge synchronization technology at an affordable price.

Spectracom NetClock Master Clocks are based on GPS (Global Positioning System) technology – tracking up to twelve satellites simultaneously and synchronized to their atomic clocks. This enables computer networks to synchronize all elements of network hardware and software (including system logs) down to the millisecond over LANs or WANs – anywhere on the planet.

Technology advancements, including an embedded processor, make it possible to obtain Legally Traceable Time™ tags on log files and simplify digital forensics. The NetClock allows users to accurately time stamp video surveillance systems, access points, card readers, time clocks and alarm systems to provide necessary evidence and validation of events.

Set-up and reporting are web-enabled – a NetClock can be accessed, under appropriate security policies, anywhere within a network. The product features browser-based remote diagnostics, configuration and control as well as Flash memory for remote software upgrades. A 10/100 Mbps Ethernet LAN port provides support for Network Time Protocol (NTP) over a variety of platforms including Win2K and XP, Win 95/98/ME, NT, Cisco, UNIX, Linux and more. Remote control and monitoring can also be done through SNMP and Telnet.

Time code outputs are available to meet the requirements of diverse systems – RS-232 serial ports, RS-485 data bus ports.   Alarm outputs and programmable timer outputs are also provided.

The NetClock Master Clock system includes a CE/UL-approved power supply for international use, GPS antenna and associated mounting hardware.

1.2 Warranty Information and Product Support

Warranty information is found on the leading pages of this manual.

Spectracom continuously strives to improve its products and therefore greatly appreciates any and all customer feedback given. Please participate in Spectracom's Customer Satisfaction Survey found on our web site at:

http://www.spectracomcorp.com/

The online survey is also used for warranty registration of your new Spectracom products. All completed entries are automatically entered into a monthly prize give away drawing.

Technical support is available by telephone. Please direct any comments or questions regarding application, operation, or service to Spectracom Customer Service Department. Customer Service is available Monday through Friday from 8:00 A. M. to 5:00 P.M. Eastern time.

Telephone Customer Service at: **585-321-5800**.

In addition, please contact customer service to obtain a Return Material Authorization Number (RMA#) before returning any instrument to Spectracom Corporation. Please provide the serial number and failure symptoms. Transportation to the factory is to be prepaid by the customer. After obtaining an RMA# ship the unit back using the following address:

> **Spectracom Corporation**
> **Repair Department, RMA# xxxxx**
> **95 Methodist Hill Drive, Suite 500**
> **Rochester, NY 14623**

Product support is also available by e-mail. Questions on equipment operation and applications may be e-mailed to Spectracom Sales Support at:

mailto:sales@spectracomcorp.com

Repair or technical questions may be e-mailed to Spectracom Technicians at:

mailto:techsupport@spectracomcorp.com

Visit our web page for product information, application notes and upgrade notices as they become available at:

http://www.spectracomcorp.com/

1.3 Unpacking

Upon receipt, carefully examine the carton and its contents. If there is damage to the carton that results in damage to the unit, contact the carrier immediately. Retain the carton and packing materials in the event the carrier wishes to witness the shipping damage. Failing to report shipping damaging immediately may forfeit any claim against the carrier. In addition, notify Spectracom Corporation of shipping damage or shortages, to obtain a replacement or repair services.

Remove the packing list from the envelope on the outside of the carton. Check the packing list against the contents to be sure all items have been received, including an instruction manual and ancillary kit.

1.3.1   Package Contents

1.   Unit

2.   User manual

3.   CE/UL-approved power supply for international use

4.   AC power cord

5.   Rack mount kit (2 ears, 4 side screws)

6.   Rubber footpads for desktop installation

7.   Two 3-pin terminal block connector for RS-485 connections

8.   10-pin terminal block connector

9.   Terminating Resistor, 120Ω

Spectracom models that have the modem dial out feature will also receive the following:

10.   Serial Modem kit

11.   Null modem adapter

1.4 Model TTS 200 Specifications

1.4.1 Receiver

Received standard: L1 C/A Code transmitted at 1575.42 MHz.

Satellites tracked: Up to twelve simultaneously.

Acquisition time: Typically <4 minutes from a cold start.

Antenna requirements: Active antenna module, +5V, powered by the NetClock, with 18 to 36 dB gain

Antenna connector: Type N, female.

1.4.2 RS-232 Setup Port

Function: Accepts commands to locally configure the IP network parameters for initial connectivity

Connector: DB9 female, pin assignments conform to EIA/TIA-574 standard, data communication equipment

Character structure: ASCII, 9600 baud, 1 start, 8 data, 1 stop, no parity.

1.4.3 10/100 Ethernet Port

Function: 10/100 Base T auto sensing LAN connection for NTP and remote monitoring, diagnostics, configuration and upgrade.

1.4.4 Protocols supported

NTP: Networked NTP Stratum 1 Time Server (RFC 1305), SNTP (RFC 1361)

Security: MD5 Security

Loading: 675 requests per second without encryption.
                              345 requests per second with encryption.

Accuracy: Output jitter within +/-50 microseconds of UTC typical.

Clients supported: Up to 128 users may be supported in a single sub-network.

                              A gateway greatly increases the number of users.

HTTP Server: For browser-based configuration and monitoring using Internet Explorer 5 or Netscape 6 per RFC 1945 and 2068.

FTP: For remote upload of event logs and download of upgrades per RFC 959.

SNMP: As of release 1.2.0 (future) will support v1, v2, v2c, and v3. Compliant with RFCs 1155, 1157, 1212, 1213, 12 15, 1901-8.

Telnet: For limited remote configuration per RFC 854.

Security Features: Up to 16-character Telnet password, Telnet Disable, TFTP Disable, SNMP Disable and MD5 Authentication.

Connector: RJ-45, Network IEEE 802.3.

1.4.5   RS-232 Communication Port

Signal: Selected time Data Format in RS-232 levels when interrogated by the connected device. This port may also be configured to provide a continuous once-per-second output.

Connector: DB9 female, pin assignments conform to EIA/TIA-574 standard, data communication equipment (DCE). No flow control.

Character structure: ASCII, 1 start, 8 data, 1 stop, and no parity.

Accuracy: Data stream on time marker within ± 100 microseconds of UTC on Sync in Formats 0, 1, and 3. Formats 2 and 4 within ±1 millisecond of UTC.

Configuration: Baud rate and output Data Formats are selected using the web interface. Bit rate selections are 1200, 2400, 4800 and 9600 baud. There are six Data Format selections available.

1.4.6   RS-485 Output

Signal: Selected time Data Format in RS-485 levels, output once-per-second.

Connector: Removable 3-position terminal block (supplied).

Character structure: ASCII, 1 start, 8 data, 1 stop, and no parity.

Accuracy: Data stream on time marker within ± 100 microseconds of UTC on Sync.

Configuration: Baud rate and output Data Formats are selected using the web interface. Bit rate selections are 1200, 2400, 4800, and 9600 baud. There are six Data Format selections available.

1.4.7   Front Panel LED Indicators

Power: Green, always on

Sync: Tri-color LED indicates the time data accuracy and equipment fault

LAN: Green: Good Link indicator

                                 Yellow: activity

1.4.8   Relay Outputs

Three separate outputs provided for either Programmable Event Timer Output or Major/Minor Alarm indication.

Relay contacts: NO, NC, and Common.

Contact rating: 30 VDC, 2 amps.

Connector: 10-position 3.81 mm terminal block (mate supplied).

Programmable Timer Output:

                                 128 On/Off events standard, 1024 events optional. Timer events that are hourly, daily or weekly only count as a single event so many events can be programmed in even the standard product.

Major/Minor Alarms: Relay contacts allow remote monitoring of operational status. A power failure, CPU failure loss of time sync, etc cause the alarm relay to de-

energize. The alarm relay returns to normal operation (energized) when the fault condition is corrected.

1.4.9   Input Power

Power source: 90 to 240 VAC, 47 to 63 Hz through an IEC 320 universal connector. North American AC power cord supplied. AC cables for other countries available locally.

DC input: 9.5 to 30 VDC, 10 watts, through a CE/UL/CSA-approved power adapter (supplied).

Connector: Barrel, 5.5mm O.D., 2.5 mm I. D.

Polarity: Negative shell, positive center.

1.4.10   Mechanical and Environmental

Dimensions: EIA 19" rack mount W x 1.75" H [1U] x 11.00" D
(483 mm W x 44 mm H x 305 mm D).

Weight: 4.8 lbs. (2.2 kg).

Temperature: 32° to 122°F (0° to 50°C) operating range.

-40° to 185°F (-40° to 85°C) storage range

Humidity: 10% - 95% relative humidity, non-condensing

2 Installation

2.1 Power and Ground Connection

An external AC to DC power adapter powers the NetClock.

The adapter is available in two forms:

1. US Only Wall Mount adapter, which plugs into any standard North American outlet.

2. The International and US Desk Top adapter, which has a detachable AC power cord to an IEC 320 connector.

This power adapter is shipped with a line cord compatible with AC receptacles (NEMA 5-15R) commonly found in the United States and Canada. Alternate type line cords or adapters may be obtained locally.

The chassis ground stud allows the NetClock chassis to be connected to an earth ground or single point ground. Connecting the chassis to a single point ground system may be required in some installations to ensure optimum lightning protection. An earth ground is also recommended in installations where excessive noise on the power line degrades receiver performance.

Note: Auto Negotiate, which determines the network settings to use, only occurs at power-on. Always connect the Ethernet cable before powering-on the unit for the first time. If the Ethernet cable is connected after power-on, the unit will default to 10 Mbps and half duplex.

2.2 GPS Antenna Installation

2.2.1   Antenna Cable for Outdoor Antenna

When using the Model 8225 GPS outdoor antenna, Spectracom recommends using LMR-400 low loss type cable, Spectracom CAL7xxx for the GPS antenna cable. RG-213 type coax, such as Belden 8267,may also be used but low loss cable offers the best performance. To simplify the installation process, Spectracom offers GPS cable assemblies terminated with Type N Male connectors. Specify part number CAL7xxx, where xxx equals the length in feet. Standard lengths are 10, 25, 50, 100, 150 and 200 feet.

If the antenna cable is purchased locally, select coax suitable for outdoor use. Consider the cable's weather ability, temperature range, UV resistance, and attenuation characteristics.

Do not allow the antenna cable to be placed in standing water, as water may permeate through the coax jacket over time. On flat roof installations, the coax can be suspended by cable hangers or placed in sealed PVC conduit. Apply a weather proofing sealant or tape over all outdoor connections.

Installation of a surge protection device in the antenna line is recommended to protect the NetClock receiver and connected devices from lightning damage. Spectracom offers the Model 8226 Impulse Suppressor to shunt potentially damaging voltages on the antenna coax to ground. Refer to the Model 8226 Impulse Suppressor Section for a complete description of the Model 8226.

2.2.2   Cable Lengths

Using Spectracom CAL7xxx or Times Microwave LMR-400 coax, the maximum antenna cable length permitted is 200 feet because the 91XX series allows 12 dB loss. An amplifier is needed whenever antenna cable lengths exceed 200 feet. Installations requiring longer antenna cables may use the Model 8227 Inline Amplifier, or lower loss cable. Refer to the Model 8227 Section for additional information on the Model 8227.

When selecting alternate antenna cable sources, the attenuation characteristics at the GPS frequency of 1575.42 MHz must be known. To ensure optimum receiver performance, the total antenna cable attenuation must not exceed 12 dB. Cable attenuation of greater than 12 dB requires the use of a Model 8227 Inline Amplifier.

2.2.3   Model 8226 Impulse Suppressor

Spectracom recommends the use of an inline coaxial protector for all products with an outside antenna. Spectracom offers the Model 8226, Impulse Suppressor, to protect the receiver from damaging voltages occurring on the antenna coax. Voltages exceeding the impulse suppresser trip point are shunted to the system ground. The Model 8226 is designed to withstand multiple surges. Mount the suppressor indoors, preferably where the coax enters the building. Install the suppressor on a grounding panel or bulkhead as shown in Figure 2.2-1.
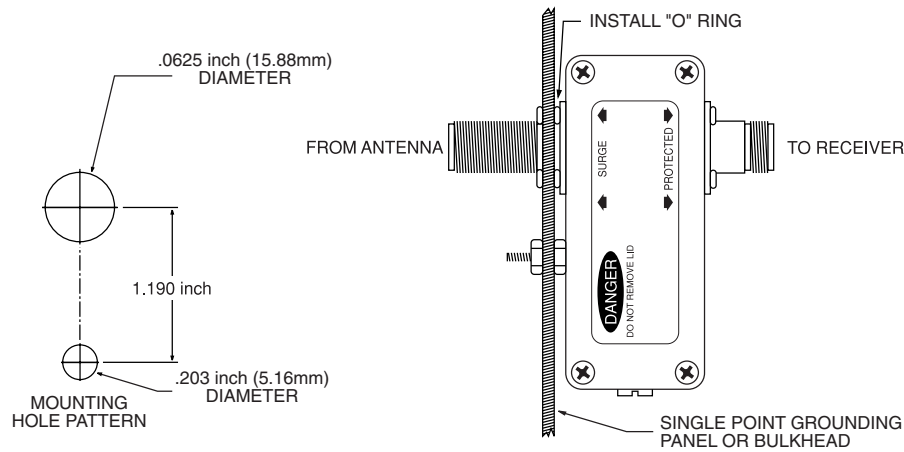
.0625 inch (15.88mm)
DIAMETER

1.190 inch

.203 inch (5.16mm)
DIAMETER

MOUNTING
HOLE PATTERN

INSTALL "O" RING

FROM ANTENNA

SURGE   PROTECTED

DANGER
DO NOT REMOVE LID

TO RECEIVER

SINGLE POINT GROUNDING
PANEL OR BULKHEAD

Figure 2.2-1: Model 8226 Impulse Suppressor

Refer to the Model 8226 Manual for proper installation.

2.2.4   Model 8227 GPS Inline Amplifier

An inline amplifier is required whenever GPS antenna cable lengths cause greater than 12 dB attenuation. Using Spectracom CAL7xxx coax, an amplifier is needed whenever antenna cable lengths exceed 200 feet.

The Model 8227 GPS Inline Amplifier, shown in Figure 2.2-2, extends the maximum cable length to 600 feet. The Model 8227 provides 20 dB of gain and is powered by the NetClock/ receiver.

Model 8227
ANT   Inline Amplifier   GPS
IN   OUT
         SIGNAL

Figure 2.2-2: Model 8227 Inline Amplifier

Refer to the Model 8227 Manual for proper installation.

2.3   Ethernet Network Cabling

Spectracom's 91xx products provide a 10/100 Ethernet port for full NTP functionality as well as full web enabled configuration, monitoring and diagnostic support.

The Ethernet port is provided on the front panel for easy connection to routers and hubs.

- Use standard CAT 5 cable with RJ45 connectors.

- When connecting to a hub or router use a straight-through wired cable.

- When connecting directly to a PC, use a crossover wired cable.

2.4 RS-485 Wiring and Set up

2.4.1   Remote Connections

The NetClock has two Remote Connections labeled RS-485 1 and RS-485 2. On NetClocks without a GPS reference, port 1 is used as a time output port and port 2 is a time input port. On NetClocks with a GPS reference, both ports are output ports. These outputs provide a continuous once-per-second time data stream in the selected Data Format. There are two input time Data Formats and five-output time Data Format selections and one position data stream in NMEA 0183 format available. Refer to Section 6.2 for a complete description of the data format structures.

In addition to Data Formats, baud rate and UTC time difference of each output is selectable. Refer to the Interface Set-up Section 3.4 for configuring these outputs.

A 3-position terminal block is supplied in the ancillary kit for each Remote Connections. Connector pin assignments are shown in Figure 2.4-1.
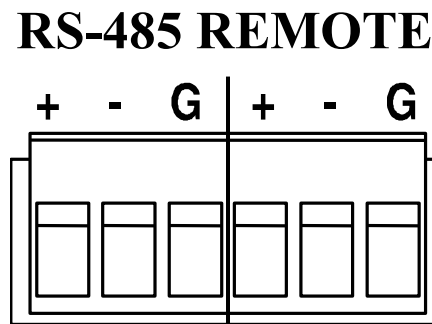

Figure 2.4-1: Remote Outputs

RS-485 is a balanced differential transmission requiring twisted pair cabling.

RS-485 characteristics make it ideal to distribute time data throughout a facility. Each Remote Output can provide time to 32 devices at cable lengths up to 4,000 feet. Refer to Figure 2.4-2 for a schematic representation of each RS-485 output driver. Relative to RS-485 specifications, the A terminal (Pin 2) is negative with respect to the B terminal (Pin 1) for a mark or binary 1. The A terminal is positive to the B terminal for a space or binary 0.
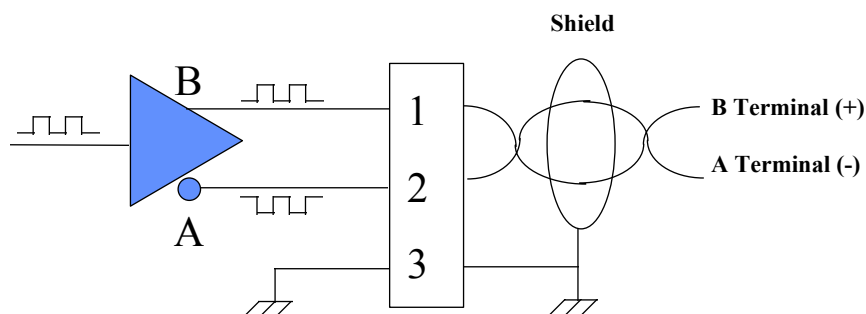

Figure 2.4-2: RS-485 Output

Spectracom offers many devices that accept the RS-485 data stream as an input reference. These products include display clocks, RS-485 to RS-232 converters, NTP time provider, and radio link products to meet various time applications and requirements. For information on Remote Output usage refer to Section 2.4.2 of this chapter.

2.4.2   Remote Output Usage

The Remote Outputs provide a continuous once-per-second time data stream in RS-485 levels. RS-485 is a balanced differential transmission, which offers exceptional noise immunity, long cable runs and multiple loading. These characteristics make RS-485 ideal for distributing time data throughout a facility. Each Remote Output can drive 32 devices over cable lengths up to 4000 feet. Spectracom manufactures wall clocks, NTP time providers, RS-485 to RS-232 converters and radio link products that utilize the RS-485 data stream as an input. Figure 2-5 and Figure 2.6 illustrate typical RS-485 time data bus interconnections. Follow the guidelines listed below when constructing the RS-485 data bus.

2.4.3   RS-485 Guidelines

Cable selection: Low capacitance, shielded twisted pair cable is recommended for installations where the RS-485 cable length is expected to exceed 1500 feet. Table 2-1 suggests some manufacturers and part numbers for extended distance cables. These cables are specifically designed for RS-422 or RS-485 applications; they have a braided copper shield, nominal impedance of 120 ohms, and a capacitance of 12 to 16 picofarads per foot.

RS-485 cable may be purchased from Spectracom. Specify part number CW04xxx, where xxx equals the length in feet.

MANUFACTURER	PART NUMBER
Belden Wire and Cable Company 1-800-BELDEN-1	9841
Carol Cable Company 606-572-8000	C0841
National Wire and Cable Corp. 232-225-5611	D-210-1

Table 2-1: Cable Sources for RS-485 Lines Over 1500 Feet

For cable runs less than 1500 feet, a lower-cost twisted pair cable may be used. Refer to Table 2-2 for possible sources. In addition, Category 5 cables may be used for cable runs less than 1500 feet.

MANUFACTURER	PART NUMBER
Alpha Wire Corporation 1-800-52ALPHA	5471
Belden Wire and Cable Company 1-800-BELDEN-1	9501
Carol Cable Company 606-572-8000	C0600

Table 2-2: Cable Sources for RS-485 Lines Under 1500 Feet

2.4.4   Connection Method

The RS-485 transmission line must be connected in a daisy chain configuration as shown in Figure 2.4-3: One-Way Bus Installation. In a daisy chain configuration, the transmission line connects from one RS-485 receiver to the next. The transmission line appears as one continuous line to the RS-485 driver.

A branched or star configuration is not recommended. This method of connection appears as stubs to the RS-485 transmission line. Stub lengths affect the bus impedance and capacitive loading which could result in reflections and signal distortion.
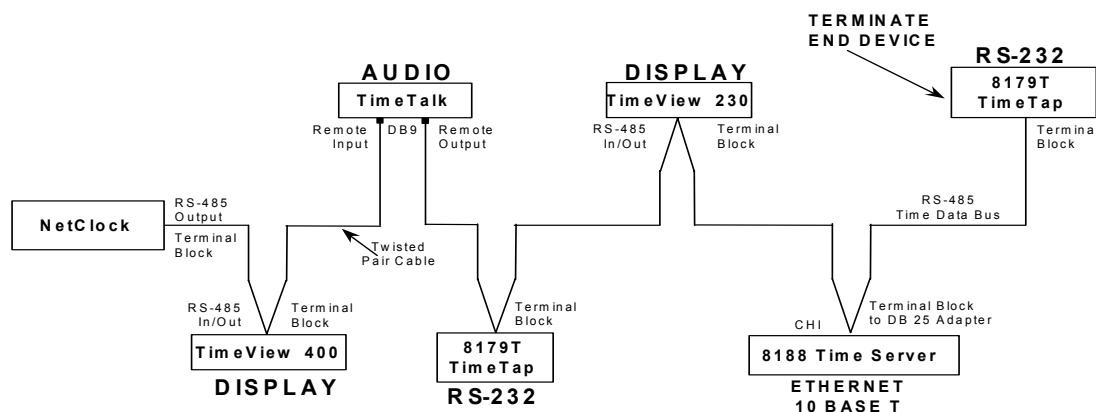
Figure 2.4-3: One-Way Bus Installation

The RS-485 Output could be split in two directions as shown in Figure 2.4-4. This allows the NetClock/GPS to be centrally located. Connecting in this method can simplify installation and possibly reduce the amount of cable required.
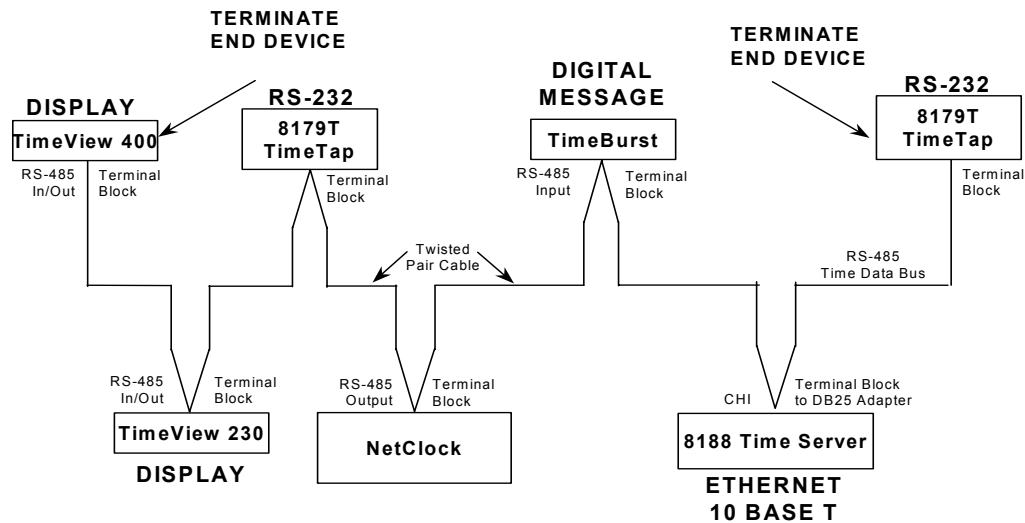
Figure 2.4-4: Split Bus Configuration

Most RS-485 connections found on Spectracom equipment are made using a removable terminal strip. A jaw that compresses the wires when tightened secures the wires. When using small diameter wire, 22-26 gauge, a strain relief can be fashioned by wrapping the stripped wire over the insulating jacket as shown in Figure 2.4-5. Wrapping the wires in this manner prevents smaller gauge wires from breaking off when exposed to handling or movement.

STRIP
WIRE

WRAP WIRE OVER
INSULATING JACKET
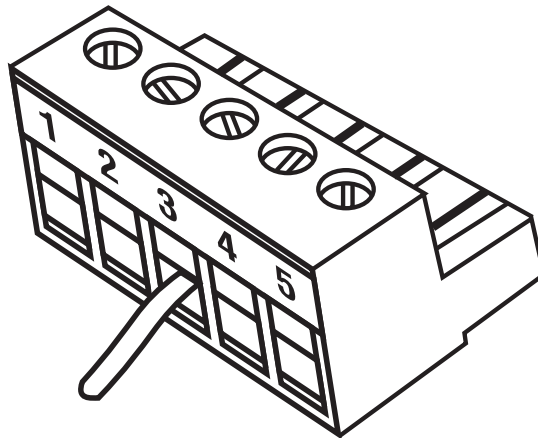
INSERT AND
TIGHTEN

Figure 2.4-5: Wire Strain Relief

TimeView display clocks use a 6-position terminal block to connect to the RS-485 data bus. Connect the TimeView to the NetClock/GPS RS-485 Output as shown in Figure 2.4-6. The TimeView display clocks accept only Data Formats 0 or 1.
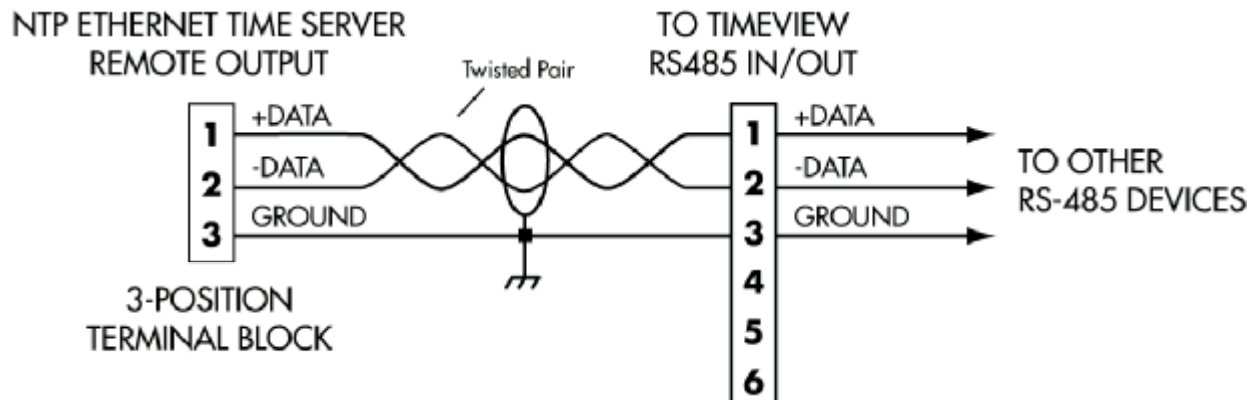
Figure 2.4-6: TimeView RS-485 Interface

The Model 8179T TimeTap is an RS-485 to RS-232 converter. The Model 8179T has a DB9 RS-232 interface that receives operational power from the RS-232 flow control pins RTS or DTR. Connect the TimeTap to the RS-485 data bus as shown in Figure 2.4-7.
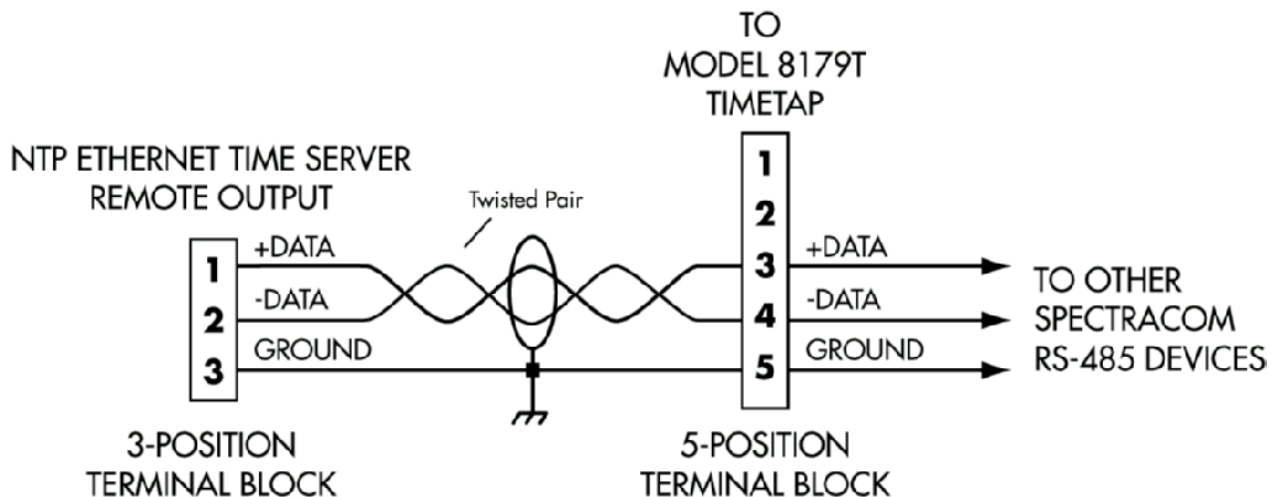
Figure 2.4-7: Model 8179T TimeTap RS-485 Interface

Spectracom Model 9188/8188, NetClock/ is an Ethernet Time Server that supports NTP and SNTP time protocols. The Model 9188/8188 accepts either Format 0 or Format 2 and connects to the RS-485 data bus through a three-position terminal block. Connect the Model 9188/8188 to the Netclock/GPS as shown in Figure 2.4-8.
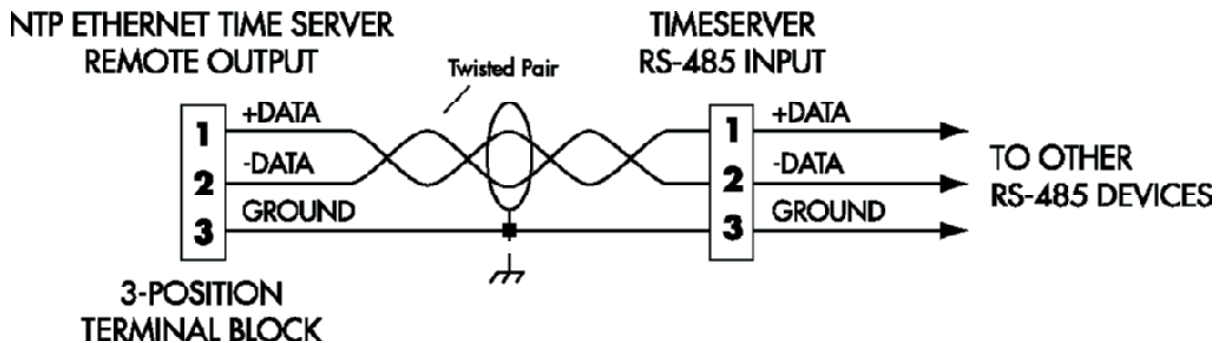

Figure 2.4-8: Model 9188/8188 RS-485 Interface

The Model 8185, TimeBurst™, provides a digital time-of-day data burst to a radio transmitter. The TimeBurst accepts only Format 0. Connect the TimeBurst to the RS-485 data bus using a 3-position terminal block as shown in Figure 2.4-9.
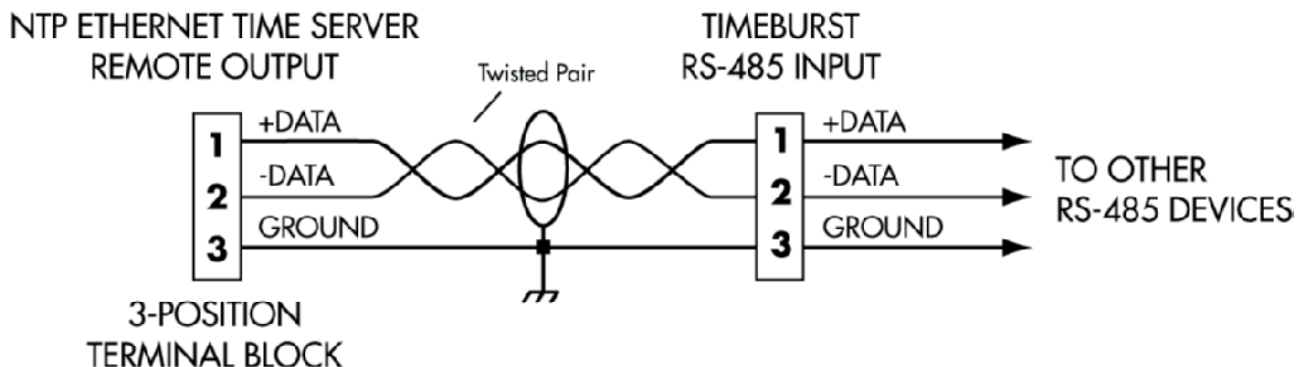
Figure 2.4-9: TimeBurst RS-485 Interface

2.4.5   Termination

A termination resistor is required on devices located at the ends of the RS-485 transmission line. Terminating the cable end preserves data integrity by preventing signal reflections.

For a one-way bus installation (Figure 2-5), terminate the last device on the bus. The RS-485 data bus can be split in two directions as shown in Figure 2-6. In a split bus configuration, terminate the devices installed on each end of the bus. Most Spectracom products include a built in termination switch to terminate the RS-485 bus when required.
If your unit comes with the modem dial out feature, you will need to connect a serial modem to the unit to allow it to connect to the modem time references.

- The cable needed to connect the unit to the modem is a DB9 male to DB25 male null modem serial cable. This should come with the modem package.

- Connect the null modem converter that comes with the serial cable to the DB9 end of the cable to modify the standard cable to work with the Spectracom unit.

- Connect the DB25 side to the modem and the modified DB9 side to the serial setup port on the unit.

- Connect the CAT2 telephone cable from the phone line to the modem.

- Connect the modem power adapter to a power outlet.

- Refer to the Modem Dial Out Setup in section three of this manual for instructions on how to configure and use the modem dial out feature.

3 Product Configuration

3.1 Network Configuration

3.1.1   Using the Web Interface to Configure the Network

The product has a 10/100 Mbps Ethernet port, which can be used to connect the unit to a network. The unit will need to be initially configured via the setup port, and can thereafter be modified through either the serial port or web interface. The values to enter into the fields described below will be specific to your setup, and can be obtained from your network administrator.

IP Address: This is the unique 32-bit address assigned to the product. The default address is 10.10.200.1

Subnet Mask: This is a 32-bit mask that specifies the range of IP addresses of the Ethernet segment the unit is connected to. The default value is 255.255.255.0.

Gateway: When the gateway IP is disabled on the product, the unit cannot be accessed from subnets outside the local subnet. When enabled, the IP address of the subnet's gateway will need to be specified. The default is disabled

Telnet: This is a toggle option to enable or disable the unit's telnet interface.

FTP: This is a toggle option to enable or disable the unit's FTP interface.

HTTP[*]:   This is a toggle option to enable or disable the unit's HTTP interface on secure Spectracom products only.

SSH[*]:   This is a toggle option to enable or disable the unit's SSH interface on secure Spectracom products only.

Note: Auto Negotiate, which determines the network settings to use, only occurs at power-on. Always connect the Ethernet cable before powering-on the unit for the first time. If the Ethernet cable is connected after power-on, the unit will default to 10 Mbps and half duplex.

---

[*] This feature is only available for secure Spectracom products

TO CONFIGURE THE PRODUCT TO WORK ON A NETWORK VIA SETUP PORT:

Serial Setup Interface

1. Connect the serial port of your PC to the 9-pin Serial Set-up Interface connector.
2. Use a Terminal Emulator program such as HyperTerminal or equivalent to connect to the NetClock®. Port settings should be 9600 Baud, No parity, 8 data bits, 1 stop bit, No flow control.
3. Power on the NetClock.

Initial network setup

If the unit has not yet been configured for a network, it will boot with the default settings and the '**Spectracom login:**' prompt will appear; Login as administrator to change the default settings.

═══

Note: To make changes to the settings, you must be logged in with configuration or administrator privileges. To Login with configuration- or administrator-level permissions with the 'login' command:

- For admin mode, type: login admin<enter>

- The unit will response with `Password:`

- Type admin123<enter> (the unit will not show what you type)

- For config mode, type: login config<enter>

- The unit will response with `Password:`

- Type config12<enter> (the unit will not show what you type)

If you hit enter during any part of the above commands, it will prompt you for the next value.

═══

'net ip' will display or change the current IP address of the unit.

'net mask' will display or change the current subnet mask.

'net gateway' will display or change the current default gateway settings.

Example: To put the product on the network as 10.10.200.5 with a subnet mask of 255.255.255.128 and no gateway:
Connect to the serial port of the unit.

1. Connect to the serial port of the unit.

2. Login with configuration- or administrator-level permissions with the 'login' command.

3. Type 'net ip 10.10.200.5 to set the IP address.

4. Type 'net mask 255.255.255.128' to set the subnet mask.

5. Type 'net gateway no' to disable the gateway feature.

TO CONFIGURE THE PRODUCT TO WORK ON A NETWORK VIA WEB INTERFACE:
Connect to the web interface after booting the unit. Use a PC with a web browser (Such as Internet Explorer version 5.0 or greater or Netscape) and connect to the product by typing in the IP address into the address window of the browser as follows: http://10.10.200.50 (or your IP address).   Then, click on "Enter Main Page".
Login to configuration or administrator level mode if changes are desired. Refer to 3.1.2 for instructions on Web Interface login.

Choose "System Setup" from the bottom frame, and "Network" from the left frame.

All fields will display the current system settings. At the bottom of the frame, clicking Reset will revert any changes made at this window since last pressing Submit.

The IP Address and Gateway Address fields must be entered in 'dotted-quad' format.

The Subnet Mask is displayed as pull down menu showing a list of possible subnet masks.

Setting the gateway to Disabled will cause the values in the Gateway Address field to be ignored.

The Telnet and FTP settings are displayed as radio buttons.

Example: To put a unit on the network as 10.10.200.5 with a subnet mask of 255.255.254.0, a gateway of 10.10.200.10, with Telnet disabled and FTP enabled:

1. Connect to the web interface of the product.

2. Login to configuration- or administrator-level mode and browse to the Network configuration page.

3. Enter '10', '10', '200', and '5' in the corresponding IP Address fields.

4. Select '255.255.254.0' from the Subnet Mask pull down menu.

5. Choose the Gateway Enabled radio button.

6. Enter '10', '10', '200', and '10' in the corresponding Gateway Address fields.

7. Choose the Telnet Disabled radio button.

8. Choose the FTP Enabled radio button.

9. Review the changes made and click Submit. The browser will display the status of the change.

3.1.2   Login
There are two login modes:

1. *Configuration Mode* allows basic control over configuration parameters.
2. *Administrator Mode* allows full control over all parameters

Both modes require a password.

Refer to Figure 3.1-1 for a list of the permission requirements.

Figure 3.1-1: Log-in Permissions

CAUTION: The Administrator login provides the most power to change settings but an erroneous entry could cause the NetClock® to malfunction or not perform within specifications. Only technicians trained in NetClock® operations should be given access to the Administrator mode.

No Password?
That's OK; you can still view the unit's configuration settings in the read-only mode.

Default Password
The default access settings for the *Configuration* and *Administrator Modes* are:

    Username: config   Username: admin
    Password: config12   Password: admin123

For security reasons, we recommend you change the password (and the user name) and don't lose them! [You can write them down here.]

Username [config]: _____   Username [admin]: _____

Password: _____   Password: _____

Once you have access to the settings web pages, you can set up each page.

3.1.3   To Change the Default Login Password Values

For security reasons, the account passwords cannot be changed using either the Web Browser or telnet command. Password changes must be made using the RS-232 Serial Setup Interface connection on the rear panel. To change the account passwords, connect to the Serial Setup Interface with a straight-thru serial cable. Using HyperTerminal, Procomm or any other terminal emulator, login as admin using the current password. At the command prompt, type the following:

    sec password [admin or config]<enter>
    Where [admin or config] is the account name desired to be changed.
    The unit will then ask you to type in the old password and then to type the new password (twice).

    Example:
Type:	sec password <ent>
Response:	`Account:`
Type:	[current account name] <ent>
Response:	`Old Password:`
Type:	[current password for this account] <ent>
Response:	`New Password:`
Type:	[New password for this account] <ent>
Response:	`New Password (again):`
Type:	[New password for this account] <ent>
Response:	New Password set

For additional information on the sec command, refer to the software command appendix (sec command).

NOTE: Always **LOGOUT** and **EXIT CONNECTION TO THE PRODUCT** prior to closing the Web Browser when you are finished viewing the Ethernet Time Server settings. For security reasons, only one connection session is supported at any one time, so this ensures that a new session can be activated immediately. If you don't log out or exit the connection, you will have to wait a time-out period or reset the unit to begin a new session.

3.2 NTP/SNTP

NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) are client-server protocols for synchronizing the time on IP networks. NTP provides greater accuracy and error checking than SNTP. NTP and SNTP can be used to synchronize the time on any computer equipment that is compatible with the Network Time Protocol. This includes CISCO routers and switches, UNIX machines and Windows machines with a suitable client. To synchronize just one workstation, several freeware or shareware NTP clients are available on the Internet. The software running on the PC determines if NTP or SNTP is used.

3.2.1   Configure NTP

The NTP setup page provides full control of the operation of your NTP server. Follow the simple steps below to quickly set up your unit as an NTP server on your network.

Connect to your unit through its web-based interface.

Click on the System Setup link on the bottom of the screen to open the menu for system configuration.
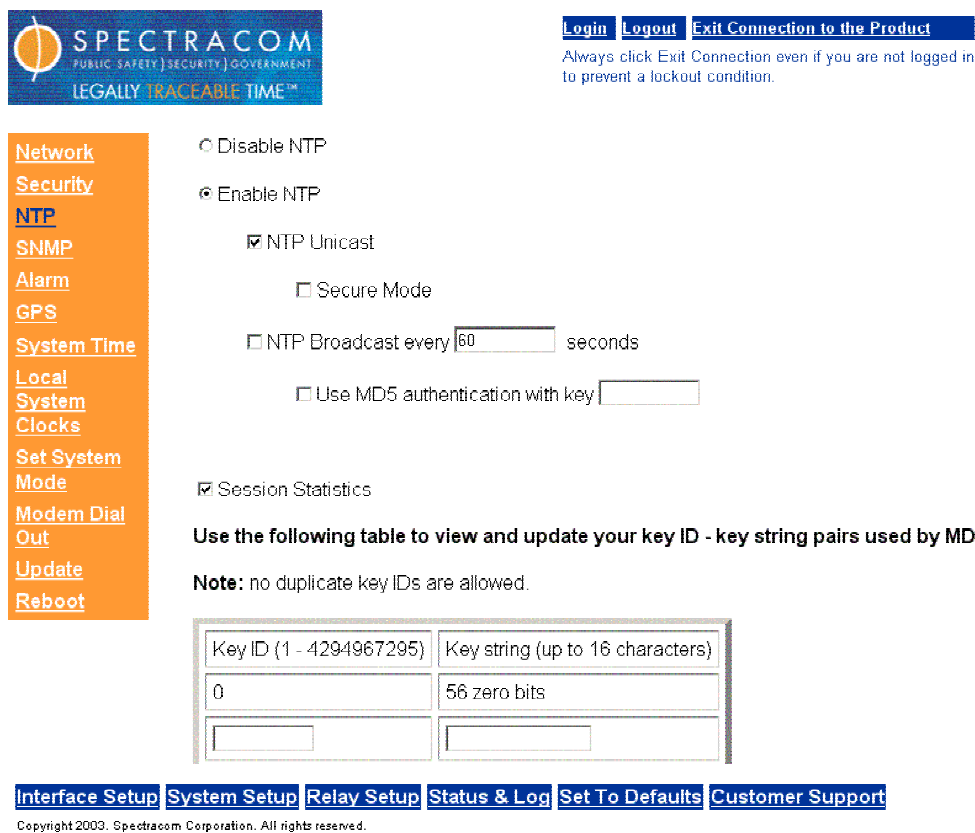
Figure 3.2-1: NTP Screen

Click on the NTP link on the left side of the screen to enter the NTP setup page. **Note**: you must be logged in as an administrator to modify the NTP settings.

The NTP server can operate in Unicast mode, multicast mode, or both concurrently. Simply place a checkmark in the boxes labeled "NTP Unicast" or "NTP Multicast …" or in both.

In the Unicast mode the unit will send a time packet response to an NTP "request" sent by a client. The Spectracom NTP server can handle up to 570 NTP requests per second typical without MD5 encryption (read below).

The Multicast mode sets the unit to send out NTP time packets at a user-specified rate. Enter the desired frequency in seconds into the Multicast field on the setup page.

Secure data transfer can be enabled using MD5 Security Protocol. The Encryption feature does not mean that the time packet will be encrypted. This feature is used to authenticate that the received time packet came from the desired time-server.

To use the authentication in Unicast mode both the NTP client and the Spectracom NTP server must contain the same "Key ID – Key String" pairs and the client must be set to use one of these MD5 pairs. The key ID must be a number between 1 and 4,294,967,295; the key string can contain any alphanumeric characters and can be from 1 to 16 characters long. No duplicate key IDs are permitted.

To enable MD5 authentication in Unicast mode, check the "Secure Mode" box under the NTP Unicast setting. The unit will respond to any request which contains an authentication checksum, and will in turn append an authentication checksum based on the MD5 (Message Digest 5) hashing algorithm.

To use MD5 authentication in multicast mode, check the "Use MD5 authentication with key …" box under the NTP Multicast setting, and enter the key ID to be used for authentication when sending out NTP packets.

The *Session statistics* checkbox will enable or disable logging of NTP usage statistics. This is displayed as part of the *status and log*. Refer to the status and log section for details.

At any time during the setup, press "Submit" to save the settings or "Reset" to restore the settings to their previous state.

3.2.2   NTP Support

Spectracom cannot provide technical assistance for configuring and installing NTP on Unix-based applications. Please refer to http://www.ntp.org/ for NTP information and FAQs. Another good source for support is the Internet newsgroup at news://comp.protocols.time.ntp/.

Spectracom can provide support for the Windows NT and Windows 2000 time synchronization. Refer to the Spectracom Web page for application notes at:
http://www.spectracomcorp.com/computernetworks.html.

3.2.3   Application Note: MD5 Authentication using a Cisco Router

According to the Cisco Manual located on their website to configure NTP Authentication the user would use the following commands:

set ntp key public_keynum {trusted | untrusted} [md5 secret_keystring]

where:
public_keynum is a number from 1 to 4,292,945,295 and is a key ID number
"trusted" is used to activate the key, "untrusted" to disable the key
md5 means the keyword (the type of key, Cisco only uses md5)
"secret_keystring" is the key value, it is from 1 to 32 printable characters.

To interoperate with the Ethernet Time Server, the "secret_keystring" must be eight printable characters and the public_keynum must be a number from 1 to 6.

For example: to define key id number 3 with the secret_keystring TICKTOCK" would require the following commands into the Cisco Router:

set ntp key 3 trusted md5 TICKTOCK

This will define the key and enable it in one step. The command "show ntp" can be used to display the key definitions.

On the NetClock side you would enable MD5 authentication with key **3** and then enter **TICKTOCK** into the Key Table with ID **3.**

3.3 Local System Clocks Setup

You can define up to 5 Local Clocks or Time Zones to be used with any of the remote serial interfaces, event timers, or front panel displays. Once defined, these Local Clocks can be used by any interface and will cause that interface to be automatically updated for its time zone and DST conditions. To configure a local clock:

Connect to the web interface after booting the unit. Login to administrator-level mode if changes are desired. Choose "System Setup" from the bottom frame, and the "Local System Clocks" from the left frame and you will see this screen:

Figure 3.3-1 Local System Clocks Setup Screen

Choose "Create/New" and click on the "Submit" button. This screen will appear ():

Login | Logout | Exit Connection to the Product

Always click Exit Connection even if you are not logged in
to prevent a lockout condition.

SPECTRACOM
PUBLIC SAFETY) SECURITY) GOVERNMENT
LEGALLY TRACEABLE TIME™

Network
Security
NTP
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Dial Out
Update
Reboot

New Local Clock Name: My City Name

TIME ZONE SETUP:

○ Automatically configure to unit's physical locality

⦿ Manually defined UTC offset UTC-00:00 [▼]

DST SETUP:

⦿ No DST rule, always standard time

○ Automatically configure to unit's physical locality

○ Manually defined by region [   ] [▼]

○ Manually defined by week and day

DST In Date:

Week: [   ] [▼] Day: [   ] [▼] Month: [   ] [▼]

Hours: [   ] Minutes: [   ]

DST Out Date:

Week: [   ] [▼] Day: [   ] [▼] Month: [   ] [▼]

Interface Setup | System Setup | Relay Setup | Status & Log | Set To Defaults | Customer Support

Figure 3.3-2 Time Zone and DST Setup Screen

Enter any name you wish for the Local Clock Name, up to 20 characters long. It can be any meaningful name that helps you know your point of reference (example: New York, Wall Clock in Bldg27, Eastern HQ, etc.)

Time Zone Setup:
This field allows the user to manually select which time zone to use when sending data. The default is UTC.

DST Setup:
Four options for Daylight Savings Time are available here. There is no DST observed. This is the default.

Manually specify a pre-defined DST rule.
- Europe
- North America
- Australia-1
- Australia-2

Define a DST rule by the [n]th [day of week] in [month] method.

Define a DST rule by the [day of month] in [month] method.

Example 1: To create a Local System Clock to UTC+1 with no DST rule:

1. Connect to the web interface of the unit.

2. Login to administrator-level mode and browse to the System Setup, Local System Clocks page.

3. Select Create/New and assign the clock a meaningful name.

4. Click on the "Manually Defined UTC Offset" button.

5. Select 'UTC+1:00' from the Time Zone pull down menu.

6. Select the 'No DST rule' radio button.

7. Review the changes made and click Submit. The browser will display the status of the change.

Example 2: To configure an RS-485 port to go in DST at 2:00am on the 3rd Friday in April and out of DST at 1:00am on the 1st Sunday in October, with a DST change of 1 hour:

1. Connect to the web interface of the unit.

2. Login to administrator-level mode and browse to the System Setup, Local System Clocks page.

3. Select Create/New and assign the clock a meaningful name.

4. Under "DST Setup", select the 'Manually defined by week and day' radio button.

5. Enter/select '3rd', 'Friday', 'Apr', '2', and '0' in the DST In Date section.

6. Enter/select '1st', 'Sunday', 'Oct', '1', and '0' in the DST Out Date section.

7. Enter '1' and '0' in the corresponding fields of the Change Amount section.

8. Review the changes made and click Submit. The browser will display the status of the change.

9. Browse to the "Interface Setup, Remote Port" page and Select the proper System Clock.

Example 3: To change a Local System Clock to be in DST at 1:01am on October 2nd and out of DST at 2:00am on April 17th, with a DST change of 30 minutes:

1. Connect to the web interface of the unit.

2. Login to administrator-level mode and browse to the System Setup, Local System Clocks page.

3. Select the desired Clock Name.

4. Select the 'Manually defined by month and day' radio button.

5. Enter/select '2', 'Oct', '1', and '1' in the DST In Date section.

6. Enter/select '17', 'Apr', '2', and '0' in the DST Out Date section.

7. Enter '0' and '30' in the corresponding fields of the Change Amount section.

8. Review the changes made and click Submit. The browser will display the status of the change.

3.3.1   Time Zone and DST

How to set up Time Zone and DST Rule:
The unit will allow you to define different Time Zone and DST rules for different Interfaces and a front panel display (if so equipped). In order to use this feature properly, users have to know the correct Time Zone offset and DST rule for your area.

The general Time Zone and DST rule information can be found from the following web sites: http://www.worldtimeserver.com/, http://webexhibits.org/daylightsaving/b.html.

Since the Time Zone and DST rules are set up for each Interface and front panel display separately, you should click the "Interface setup" hyperlink, and then select the Interface you want to modify. Then you will see the Time Zone setup and DST setup option on the web page.

Time Zone
Under the "TIME ZONE SETUP", you will see two choices:
- Automatically configure to unit's physical locality
- Manually defined UTC offset

Auto Time Zone
By selecting this option, the unit will compute the Time Zone Offset automatically based on the location of the unit provided by GPS receiver.

If you select this feature before the GPS receiver completes the position calculation, a message will be displayed to explain that this feature is not valid until the position is available.

If you select this feature after the GPS receiver determines its position, the computed Time Zone Offset information will be shown.

Note: that Automatic Time Zone calculations are imprecise because the time zones are determined by local political boundaries and may change often. This feature is made available as an aid only.

To apply the computed Time Zone, select the check box for the desired Interface.

Manual Time Zone
A drop down box is provided for the choice. Left click the drop down box and select the time zone offset you want to use.

Note: All of the Time Zone Offset drop-downs in the web browser are configured as UTC plus or minus a set number of hours. For **Eastern**, chose UTC–5, for **Central**, chose UTC-6, for **Mountain**, chose UTC-7 and for **Pacific**, chose UTC-8.

DST rule
Under the "DST SETUP", you will see four radio buttons. , The four options are "No DST rule, always standard time"; "Manually defined by region"; "Manually defined by week and day"; "Manually defined by month and day".

No DST Rule, always standard time
This option should only be used when you do not want to apply any DST rule to this Interface output.

Auto DST
This feature is designed to compute the DST rule automatically based on the location of the unit provided by GPS receiver.

If you select this feature before the GPS receiver completes the position calculation, a message will be displayed to explain that this feature is not valid until the position is available.

If you select this feature after the GPS receiver determines its position, the computed DST rule information will be shown.

 Note: that Automatic DST calculations are imprecise because the rules for DST are determined by local political boundaries and may change often. This feature is made available as an aid only.

To apply the computed DST rule, select the check box for the desired Interface.
Manually defined by region

This option is recommended if you do not need to define a special rule. Under this option, there is one drop down box. Left click the drop down box and you will see four regional choices: "Europe", "North America", "Australia-1" and Australia-2".

The official DST rules for these four regions are as follows:

Europe
Start: Last Sunday in March at 1am UTC
End : Last Sunday in October at 1am UTC

North America
Start: First Sunday in April at 2am local time
End : Last Sunday in October at 2am local time

Australia-1
Start: Last Sunday in October at 2am local time
End : Last Sunday in March at 3am local time

Australia-2
Start: First Sunday in October at 2am local time
End : Last Sunday in March at 3am local time

Manually defined by week and day
This option is provided for advanced users. You can input start time, end time and the hour to change for the daylight saving. By selecting this option, the DST rule can be defined based on the weekday, week, and month of the local time you defined for this Interface.

Manually defined by month and day
This option is provided for advanced users. You can input start time, end time and the hour to change for the daylight saving. By selecting this option, the DST rule could be defined based on the day and month of the local time defined for this Interface. If you select the February 29th as the start time or end time, the unit will treat it as March 1st during non-leap year.

3.4 Interface Setup

Using the web interface to configure any Interface:

The product can have RS-232 ports (also called Serial Ports) and RS-485 ports (also called Remote Output Ports) that support independent output of date/time stamps. Optionally the product can support Front Panel Displays providing human readable visual output. The web interface is the method by which these can be configured, and the available options are described below:

Baud Rate:
This is the speed at which this Interface will output data. Supported values are 1200, 2400, 4800, and 9600. 9600 baud is the default.

Data Format:
This is the format in which data/time stamps are output. Available formats are 00, 01, 02, 03, 04, and 90; and are described in detail in the "Data Format" section above. Format 00 is the default.

Request Char (feature not available on RS-485 port):
If Multicast is selected, the unit will automatically broadcast once per second. If User Defined is selected, the unit will only send data upon reception of the character in the textbox. The default is the user-defined character 'T'.

System Clock:
This field allows the user to select which Local System Clock (time zone) to use when sending data. The default is UTC.   See Section 3.3 Local Systems Clocks for more information on how to set these.

To configure a product's Interface via web interface:

Connect to the web interface after booting the unit. Login to configuration- or administrator-level mode if changes are desired. Choose "Interface Setup" from the bottom frame, and the desired port from the left frame. Serial Ports correspond to RS-232 outputs and Remote Output Ports correspond to RS-485 outputs. All fields will display the current system settings. At the bottom of the frame, clicking Reset will revert any changes made at this window since last pressing Submit.

Login Logout Exit Connection to the Product
Always click Exit Connection even if you are not logged in
to prevent a lockout condition.

SPECTRACOM
PUBLIC SAFETY) SECURITY) GOVERNMENT
LEGALLY TRACEABLE TIME™

Serial Port 1
Serial Port 2
Remote Output 1
Remote Output 2
Front Panel Display

BAUD RATE: 9600 ▾

DATA FORMAT: 00 ▾

REQUEST CHAR: ○ Multicast   ⊙ User defined T

SYSTEM CLOCK: UTC ▾ Click here to edit or create local system clocks.

Submit   Reset

Interface Setup System Setup Relay Setup Status & Log Set To Defaults Customer Support

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 3.4-1: Interface Screen

Example 1: To configure an RS-232 port to run at 2400 baud, and output Format 90 to run in Eastern Standard Time:

1. Connect to the web interface of the unit.

2. Login to configuration- or administrator-level mode and browse to the Serial Port page.

3. Select '2400' from the Baud Rate pull down menu.

4. Select '90' from the Data Format pull down menu.

5. Select a Local System Clock defined for the proper time zone.

6. Review the changes made and click Submit. The browser will display the status of the change.

3.5 Alarms

3.5.1   Alarm Outputs

The operational status of the NetClock can be monitored via the condition of its alarms. The alarm states may be obtained using any of the following mechanisms:

Timer/Alarm Relays output connector

For detailed information about the rear panel connectors, see the "Rear Panel Functions" section. For detailed information about configuring the relays to signal alarms, see Section 5.3.1.

System Status displayed on a web browser

Dynamic system information including the current state of the alarms can be obtained by clicking "Status & Log" along the bottom of the main browser screen, followed by clicking "System Status" on the left side of the screen. The alarm status is displayed in a table labeled "Dynamic System Information"

3.5.2   Alarm log

Alarm transition information is recorded in the alarm log.

An alarm is asserted whenever any of the following conditions exist:

Time Sync Alarm:	The period of time allotted for operation without tracking a satellite has expired. Factory default period is 2 hours. This is a **Major** alarm.
GPS Receiver Fault:	The CPU is unable to communicate with the GPS receiver. This is a **Major** alarm.
Frequency Error*:	Measured oscillator frequency error exceeds 1×10^{-7}. This is a **Major** alarm.
Power Failure:	The NetClock/NTP has lost power. This is both a **Major** and **Minor** alarm.
Antenna Problem:	The antenna sense circuitry warns when the antenna is not connected or a cable short or open is detected. This is a **Minor** alarm.
Oscillator Adjust*:	Warns that the TCXO time base oscillator requires an adjustment to maintain operation within specifications. This is a **Minor** alarm.

* These alarm conditions only exist on products that feature a corrected oscillator (TTS220, TTS240, TTS260, 9183).

An alarm is asserted whenever any of the following conditions exist AND the alarm has been enabled on the alarm setup screen via a web browser:

User-defined Alarm: The user-specified period of time allotted for operation while tracking less than a user-specified number of satellites has expired. This can be a **Major** and/or **Minor** alarm.

Software Fault: One or more software sub-systems has experienced a major run-time error. This is a **Major** alarm.

Figure 3.5-1: Alarm Setup Screen

User-defined alarms are configured using the Alarm Setup screen (Figure 3.5-1) from a web browser. The Alarm Setup screen may be viewed by clicking "System Setup" along the bottom of the main browser screen, followed by clicking "Alarm" on the left side of the screen. The default is a major alarm for tracking less than 1 satellite for 5 seconds.

NOTE: The Alarm Setup screen will not allow modification of any of the fields unless you have logged into the system in either configuration mode or administration mode.

Clicking the check box to the left of a particular user-defined alarm will enable that alarm condition. Each alarm condition may be set to exist for a specified duration before activating the alarm. This is done by filling in the Timeout fields directly beneath the alarm condition.

3.6 Relays

3.6.1   Configuring the relays

The operational status can be monitored remotely using the TIMER/ALARM RELAYS connector on the rear panel. This connector provides the common, NO and NC contacts for three relays. These relays can be connected to an alarm lamp, horn, or other indicator to warn when the clock accuracy or operation has been affected, or to signal the triggering of a programmed event. The relay contacts are rated at 2.0 amps, 30VDC.

The web interface allows the assignment to each relay of one of three functions: Major Alarm, Minor Alarm, and Event Timer.   For more details on these functions, see the "Alarm Outputs" section and the "Configuring the Event Timer" section.

To configure or view the relay assignments:
connect to the web interface. If configuring, login to configuration mode (or administration mode).   If just viewing, no login is needed. Along the bottom of the interface select Relay Setup. Along the left hand side select Relay Output. A page showing the relays along the left side and the functions along the top will appear. To assign a function to a relay, click the dot that lines up with both the function and the relay. If just viewing, no assignments can be changed. See the below example.

Figure 3.6-1 Relay Output Screen

Example: To assign "Major Alarm" to relay 1, "Minor Alarm" to relay 2, and "Event Timer" to relay 3, click on the following dots.

       Major alarm to relay 1: the dot in row 1, column 1.
       Minor alarm to relay 2: the dot in row 2, column 2.
       Event Timer to relay 3: the dot in row 3, column 3.

A single relay can only be assigned one function but a function can be assigned to multiple relays.

By default, all three relays are assigned "Major Alarm."

3.7 Event Timer

3.7.1 Configuring the Event Timer

The web interface allows for the configuration of 128 events that can turn any one of the event timer relays on or off. Make sure the rear panel relay that is going to be associated with an event is configured to be the event timer relay in order to use this feature (see Section 3.5.1 for details on relay configuration).

To configure the events:
Connect to the web interface. Login to configuration mode (or administration mode).

Along the bottom of the interface select Relay Setup.

Along the left hand side select Event Timer Relay.

Login Logout **Exit Connection to the Product**
Always click Exit Connection even if you are not logged in to prevent a lockout condition.

Relay Output
Event Timer Relay
Current Event Schedule
Reset ALL Event Timers
Set Event Clock
Test Relays

Note: There are a total of 128 event timers. Please enter the ID of the event scheduler you would like to edit or view.

Event Scheduler ID [   ] (1 - 128)

[Edit/View]

Currently Scheduled Events

* Relay not configured as 'Event Timer'

Event #	Enabled/ Disabled	Relay #	Action	Frequency
1	Enabled	3	On	Daily @ 02 hr : 00 min : 00 sec : 000 ms
2	Disabled	*1	On	Weekly @ MON : 01 hr : 02 min : 03 sec : 000 ms
3	Disabled	*1	Off	Monthly @ 03 day : 03 hr : 04 min : 05 sec : 000 ms

Interface Setup System Setup Relay Setup Status & Log Set To Defaults Customer Support
Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 3.7-1: Event Timer Relay Screen

A new page will load. This is where the user specifies which event to edit/view. If any events are already configured, they will be displayed by event number on this page. There are no requirements on the order of the events; each one is completely independent of the others. Enter the number of the event that you wish to edit/view and click the Edit/View button.

Now a page that displays the settings of the selected event appears and if logged in to configuration mode (or administration mode) the settings can be changed.

Choose a Time Zone
On the left side pane, select "Set Event Clock". Choose an already defined Clock (Time Zone) or define a new one. See Section 3.3 for more details on Local System Clock settings.

Note: All times entered for the Event Timers will use the same Local System Clock reference for Time Zone and DST rules. It is best to choose this reference first before entering your schedule.

Figure 3.7-2 Event Timer Relay Screen

Relay#:   Select the relay number that the event is to be associated with.

Enabled/Disabled/Delete: If the event is enabled, the event will occur when scheduled. If the event is disabled, it will not occur at the scheduled time, but will still appear in the list of scheduled events on the previous page. If the event is deleted, all fields of event are cleared and it is removed from all event lists.

ON/OFF: Each event can turn the specified event timer relay on or off.

The next section of the page describes when the event will occur and how often it will occur. The relay can be set to occur hourly, daily, weekly, monthly, and yearly.

Hourly: The event will happen every hour at the minute, second, and millisecond that is specified (within 100 milliseconds).

Daily: The event will happen every day at the hour, minute, second, and millisecond specified (within 100 milliseconds).

Weekly: The event will happen every week at the weekday, hour, minute, second, and millisecond specified (within 100 milliseconds).

Monthly: The event will happen every month at the day of month, hour, minute, second, and millisecond specified (within 100 milliseconds). If the day is set to be a day that isn't in short months, the event will happen on the last day of the short months.

Yearly: The event will happen every year at the month, day of month, hour, minute, second, and millisecond specified (within 100 milliseconds). If the month and day of month are programmed for February 29th (this can only be done while currently in a leap year), the event will happen on March first on non-leap years and February 29th on leap years.

If configuring, clicking the submit button will save the settings. The reset button undoes any changes that were made before the submit button is clicked.

Example: Program event relay #3 to turn on at 5:00PM (Eastern Standard Time) for five seconds every day.

Get to the Event Timer Relay page and "Edit/View" event 1.

Configure the event as relay #3, enabled, and to turn the event relay on daily at 22:00:00.000. Click the submit button.

If all the information was correctly entered, the "Event Scheduler update successful." message will appear.

Click Event Timer Relay and the newly configured event will appear in the list of configured events. **"Edit/View" event 2.**

Configure the event as relay #3, enabled, and to turn the event relay off daily at 22:00:05.000. Click the submit button.

If all the information was correctly entered, the "Event Scheduler update successful." message will appear.

Click Event Timer Relay and the newly configured events will appear in the event list.

To view the events:

Connect to the web interface. No login is needed to just view the events.

Along the bottom of the interface select Relay Setup.

Along the left hand side you have two options to view the events:

Event Timer Relay: Selecting this option will display all events that are either, enabled or disabled. The events are ordered by event number (1-128).

Current Event Schedule: Selecting this option will display a list of only enabled events. The events are ordered by next occurrence.

3.8 Logs

Note: The times indicated in all log entries are UTC (No correction for Local time / Daylight Saving Time).

3.8.1   Display Alarm Log

To Display the Alarm log do the following:
Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http://10.10.200.1 (or your IP address).

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item. On the left side menu, select the "Alarm Log" item. The Alarm History Log is then displayed in the center of the screen. Each time a change in alarm status occurs an alarm log is created. An alarm log includes the UTC time and date of the log, the alarm relay status and lists the conditions causing the alarms. The alarm log is displayed one page at a time, and can be navigated by using the scroll bar control on the right hand side.

Example response:
TIME= 10:17:19 DATE= 2000-03-21 STATUS CHANGE
ALARM RELAY= OFF
ACTIVE ALARMS: NONE
TIME= 13:51:29 DATE= 2000-05-05 STATUS CHANGE
ALARM RELAY= ON
ACTIVE ALARMS: MINOR
Antenna Problem
TIME= 15:51:30 DATE= 2000-05-05 STATUS CHANGE
ALARM RELAY= ON
ACTIVE ALARMS: MAJOR AND MINOR
TIME SYNC ALARM
Antenna Problem
TIME= 18:23:39 DATE= 2000-05-05 STATUS CHANGE
ALARM RELAY= ON
ACTIVE ALARMS: MAJOR
Time Sync Alarm
TIME= 18:24:44 DATE= 2000-05-05 STATUS CHANGE
ALARM RELAY= OFF
ACTIVE ALARMS: NONE

In the example above, the antenna cable was damaged at 13:51:29 on May 5, 2000. Note that a Minor Alarm was asserted at that time due to an "Antenna Problem". Since no GPS signal could be received, the Sync Time-out counters expired, causing a Major Alarm due to loss of time sync. The cable was repaired at 18:23:39, clearing the Minor and Antenna Problem messages. The receiver then reacquired and qualified at least one satellite for one minute, which cleared all alarms at 18:24:44.

3.8.2   Display Dial Out Log

If you have the optional Dial Out Modem Interface, display the log by doing the following:

Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http://10.10.200.1 (or your IP address).

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item. On the left side menu, select the "Dial out Log" item. The Dial out History Log is then displayed in the center of the screen. Each time an operation in the dial out process occurs, a dial out log entry is created. A dial out log includes the UTC time and date of the log, the operation that was just completed or the status from the previous operation. The log can be navigated by using the scroll bar control on the right hand side.

Example response:
TIME= 15:48:21 DATE= 2004-03-22
Modem dial out to 9 1-303-494-4774.

TIME= 15:48:03 DATE= 2004-03-22
Synced clock to modem time.

TIME= 15:48:55 DATE= 2004-03-22
Dial out successful. Sync'ing system 1PPS.

TIME= 15:48:58 DATE= 2004-03-22
Synced 1PPS to modem time.

In the example above, the unit initiated a dial out at 15:48:21 to the number (9)1-303-494-4774. It receives an in-sync time message at 15:48:03 and adjusted the unit's clock to the modem time. At 15:48:55 it finished the call and disconnected the modem from the phone line. It then process the collected time messages and finally synced the unit's 1PPS to the modem time's 1PPS at 15:48:58.

During the dial out operation, errors and timeouts can occur. These are also logged in the Dial out log. The exception log entries are as follows:

Failed to sync during call:
This log entry records a dial out attempt that was successful in communicating with the modem time reference, but was unable to sync the time messages during the call.

Dial out failed or aborted:
This log entry records a dial out attempt that was aborted due to system state change or an error response from the modem. For example, if the unit regain time sync with GPS during a dial out attempt he operation will be aborted. Changing the setup serial port mode to console mode or receiving a BUSY message from the modem can also trigger this log entry. This log entry is usually following with a disconnect command to the modem.

Timeout occurs, operation is aborted:
During time message acquisition and 1PPS sync process, if the process takes too long, it will be automatically aborted and retried if possible. For example, if a time message acquisition receive no response from the modem for two minutes, the operation is aborted and the dial out process is restarted again.

3.8.3   Display Operational Log

To Display the Operational log do the following:

Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http:// 10.10.200.1 (or your IP address).

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item.
On the left side menu, select the "Operational Log" item.

The Operational History Log is then displayed in the center of the screen. The operational log response begins with a header containing all firmware version levels and the time and date since power up. Entries are made to this log when the following events occur:

Unit Started:
The unit started log contains a UTC time and date stamp.
This log is created when power is restored to the clock.

For example:
Unit Started 19:13:06 2003-07-29

First Satellite Acquired:
This log time stamps when the receiver acquires a satellite for the first time.

For example:
First Satellite Acquired 19:21:34 2003-07-29

GPS Signal Qualified:
This log entry records when the receiver acquires or re-acquires and qualifies at least one satellite for one minute. A satellite is considered qualified if the received vehicle ID number is greater than 1 and if the satellite can be used for Position Fix. The time and date contained in the log reflect UTC time.

For example:
GPS Signal Qualified 19:32:00 2003-07-29

System is synced to modem time: (For units with modem dial out feature)
This log entry records when the modem dial out software has just completed a dial out operation and was able to collect time message that was used to sync the unit's time to the modem time. The date and time in the log reflect UTC time.

For example:
TIME= 18:36:15 DATE= 2004-03-13
Synced 1PPS to modem time.

Example response:
Spectracom Corporation Model 9189
Software Version 1.0.0 Date: 7/29/2003
Unit Started 19:13:06 2003-07-29
Serial Port 1 Version 2.03
Remote Port 1 Version 2.03

GPS Receiver = 12 Channel M12+ Version 2.0

TIME= 19:26:21 DATE= 2003-07-29
First Satellite Acquired

Spectracom Corporation Model 9189
Software Version 1.0.0 Date: 7/29/2003
Unit Started 19:13:06 2003-07-29
Serial Port 1 Version 2.03
Remote Port 1 Version 2.03
GPS Receiver = 12 Channel M12+ Version 2.0

TIME= 18:36:15 DATE= 2004-03-13
Synced 1PPS to modem time.

The Operational log is output in a continuous format, and can be navigated by using the scroll bar control on the right hand side.

3.8.4   Display Oscillator Log

Note: The oscillator log is not available for rubidium-based units.

To Display the Oscillator log do the following:
Use a PC with a web browser and connect to the product by typing the IP address into the address window of the browser as follows: http:// 10.10.200.1 (or your IP address)

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item.
On the left side menu, select the "Oscillator Log" item. The Oscillator Log is then displayed in the center of the screen. The oscillator log will list a history of oscillator disciplining events. Entries are made to this log when the following events occur:

Power on reset:
Time stamps the event of the unit recovering from a power cycle.

Coarse Adjust Mode:
Marks the beginning of the Coarse Adjustment of the oscillator. The coarse adjust samples and adjust the D/A setting to stabilize the oscillator to the desired frequency. Once the setting is close enough, the unit switches to Fine Adjust Mode.

Fine Adjust Mode:
Marks the beginning of the Fine Adjustment of the oscillator. This process begins once the Coarse adjust places the oscillator close to the desired frequency. The Fine Adjust mode will further tune the oscillator. The difference between coarse and fine adjust mode is that fine adjustment is done over a larger amount of samples and adjust the D/A slower than the Coarse adjust.

Reference 1PPS Unstable:
Time stamps the event when the 1PPS becomes unstable. When this happens, no disciplining will be performed until this situation is corrected.

Periodic Frequency measurement:
This is the most common entry in the oscillator log. This entry displays the timestamp followed by the current D/A settings. It also displays the current frequency error and the measured frequency count. The Frequency error is calculated as:

Freq Error = (Measured Freq Count – Ideal Freq Count) / (Ideal Freq Count)

Automatic D/A adjustment:

Usually, small D/A adjustments are made to keep the oscillator disciplined to GPS. These small adjustments are only sampled periodically and shown as part of the periodic frequency measurement described above. If a large adjustment is made to the D/A it is logged immediately to inform the user.

Example response:

TIME= 13:19:57 DATE= 2004-09-03 POWER ON RESET

TIME= 13:20:42 DATE= 2004-09-03 COARSE ADJUST MODE

TIME= 13:22:22 DATE= 2004-09-03 D/A= 7E46 FREQ ERROR= 1.22E-07 FREQ CNT= 1000000122

TIME= 13:22:48 DATE= 2004-09-03 FINE ADJUST MODE

TIME= 13:23:02 DATE= 2004-09-03 AUTOMATIC D/A ADJUSTMENT
 D/A= 7E39 MATCH CNT= 47

TIME= 13:24:02 DATE= 2004-09-03 D/A= 7E38 FREQ ERROR= 4.00E-09 FREQ CNT= 1000000004

TIME= 13:25:42 DATE= 2004-09-03 D/A= 7E36 FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000

TIME= 13:27:22 DATE= 2004-09-03 D/A= 7E37 FREQ ERROR= 1.00E-09 FREQ CNT= 1000000001

TIME= 13:29:02 DATE= 2004-09-03 D/A= 7E35 FREQ ERROR= 2.00E-09 FREQ CNT= 1000000002

TIME= 13:30:42 DATE= 2004-09-03 D/A= 7E35 FREQ ERROR= 2.00E-09 FREQ CNT= 1000000002

TIME= 13:30:51 DATE= 2004-09-03 AUTOMATIC D/A ADJUSTMENT
 D/A= 7E33 MATCH CNT= 69

TIME= 13:32:22 DATE= 2004-09-03 D/A= 7E35 FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000

TIME= 13:34:02 DATE= 2004-09-03 D/A= 7E32 FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000

TIME= 13:35:42 DATE= 2004-09-03 D/A= 7E34 FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000

TIME= 13:37:22 DATE= 2004-09-03 D/A= 7E35 FREQ ERROR= -1.00E-09 FREQ CNT= 999999999

TIME= 13:39:02 DATE= 2004-09-03 D/A= 7E35 FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000

TIME= 13:40:42 DATE= 2004-09-03 D/A= 7E36 FREQ ERROR= -1.00E-09 FREQ CNT= 999999999

TIME= 13:42:22 DATE= 2004-09-03 D/A= 7E38 FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000

TIME= 13:44:02 DATE= 2004-09-03 D/A= 7E34 FREQ ERROR= 3.00E-09 FREQ CNT= 1000000003

TIME= 13:45:42 DATE= 2004-09-03 D/A= 7E33 FREQ ERROR= 2.00E-09 FREQ CNT= 1000000002

TIME= 13:46:15 DATE= 2004-09-03 REFERENCE 1PPS UNSTABLE

TIME= 13:52:00 DATE= 2004-09-03 COARSE ADJUST MODE

TIME= 13:52:12 DATE= 2004-09-03 FINE ADJUST MODE

TIME= 13:52:15 DATE= 2004-09-03 AUTOMATIC D/A ADJUSTMENT
 D/A= 7E3B MATCH CNT= 107

The example shows a unit that recovered from a power cycle. It immediately began coarse mode adjustment, followed by Fine adjustment. Periodic frequency measurements and Large D/A adjustments are then logged. After sometime, this unit loses a stable 1PPS reference. When the 1PPS reference is recovered, the unit began disciplining the oscillator again from coarse mode.

3.8.5 NTP Statistics

The NTP statistics is controlled from the NTP configuration described in the NTP section of this manual. To display the NTP Statistics do the following:
Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http:// 10.10.200.1 (or your IP address)

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item.
On the left side menu, select the "NTP Statistics" item. The NTP Statistics is then displayed in the center of the screen as shown:
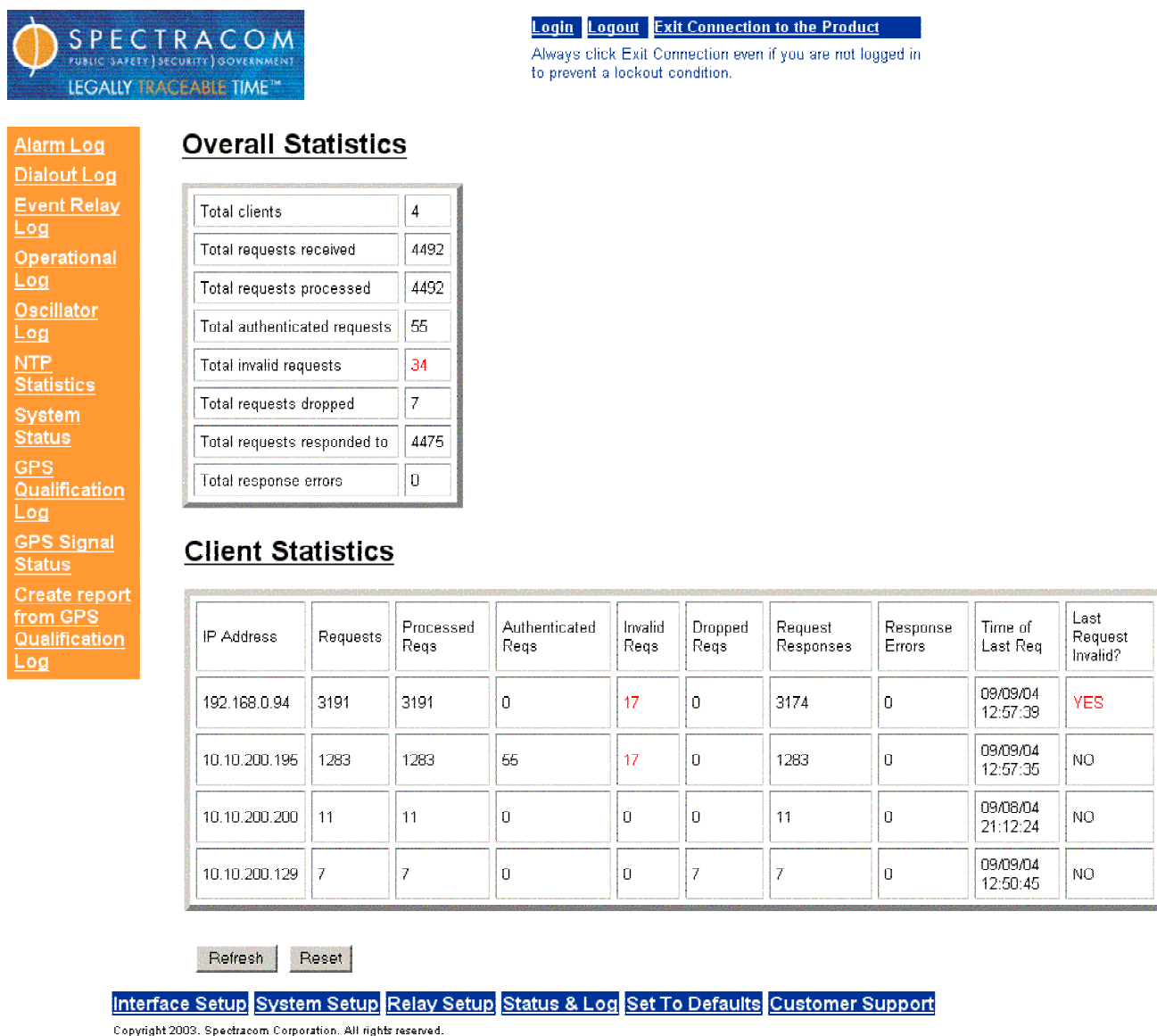
Figure 3.8-1 NTP Statistics

The overall statistics provides a quick overview of all the NTP activities from the unit while the client statistics displays the details of each client's interaction with the unit. Invalid requests are colored in red to improve the readability of the statistic list. If you need to find a specific client, you can use the find (Ctrl + F) function of the browser and search for the client's I.P. address.

3.8.6   Display Event Relay Log

To Display the Event Relay log do the following:
Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http:// 10.10.200.1 (or your IP address)

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item.
On the left side menu, select the "Event Relay Log" item. The Event Relay Log is then displayed in the center of the screen. The event relay log will list a history of event relay actions. Entries are made to this log when the following events occur:

An Event Timer Relay is triggered to OPEN the relays.
An Event Timer Relay is triggered to CLOSE the relays.

Sample Response:
TIME= 13:09:09 DATE= 2003-07-30
EVENT RELAYS: OPEN
EVENT #: 3
TIME= 13:12:25 DATE= 2003-07-30
EVENT RELAYS: CLOSE
EVENT #: 7

The Event Relay log is output in a continuous format, and can be navigated by using the scroll bar control on the right hand side.

3.8.7   GPS Qualification Log

The GPS Qualification Log records the number of qualified satellites tracked each second. At the end of every hour a log entry is created and the counters start again. The GSP qualification log is useful in verifying receiver and antenna performance.

The GPS qualification log is output in the following format:
TIME= HH:MM:SS DATE= YYYY-MM-DD
N = XXXX
N = XXXX …
Q = QQQQ
Where:
HH:MM:SS= UTC time log was created
YYYY-MM-DD= Date log was created
N= The quantity of satellites
XXXX= Number of seconds the receiver tracked the listed quantity of satellites since the beginning of the hour, 1…3600.
QQQQ= Number of seconds since the beginning of the hour the GPS signal was qualified, 0…3600

Typically, the receiver tracks two to three satellites when using a Model 8228 Window Mount GPS antenna. When using the Model 8225 Outdoor antenna, the receiver will typically track five or more satellites.

They may occasionally be short periods when the receiver is unable to track any satellites. When this occurs, the Time Sync alarm count down timer is started. The Sync Alarm Timer resets whenever the receiver reacquires and qualifies at least one satellite for one minute. If a receiver is unable to receive and qualify any satellites within the sync alarm period (two hours), a Time Sync Alarm is asserted.

Satellites are qualified as valid when the received vehicle ID number is greater than 1 and the satellite is available for Position Fix usage. The qualification count "Q" is incremented for each second these conditions are met. Typically, the Q value for each hour should exceed 3000.

To view the GPS Qualification Log, do the following:

1. Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http:// 10.10.200.1 (or your IP address).

2. Press the "Enter Main Page" button.

3. On the lower menu line, select the "Status & Log" item.

4. On the left side menu, select the "GPS Qualification Log" item. The GPS Qualification Log is then displayed in the center of the screen.

Create a Report from the GPS Qualification Log
Since the GPS qualification log includes lots of information, we also provide a comma-separated value (.CSV) file to use with Microsoft Excel™ or a similar program to convert the text data to a graph.

To get a "column" graph in Microsoft Excel, do the following:
Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: http:// 10.10.200.1 (or your IP address).

Press the "Enter Main Page" button. On the lower menu line, select the "Status & Log" item.
On the left side menu, select the "Create report from GPS Qualification Log" item. A status message will inform you, whether or not the qualification report is created successfully. If the file is created successfully, FTP to the unit.   Go the sys/logs directory and get the file named "GPSLog.csv". Please remember to get the file using ASCII data transfer option.   Open Microsoft Excel, select File/Open and then open the file saved on you local drive.   A spreadsheet should open with all the GPS log information.

To create a chart, Select "Insert/chart…" on the top menu in Excel.
A "Chart Wizard" window will pop-up, select "column" and then click "next". Click the data range box and then select all the data you want to chart, select "columns", then click "Next" button.   Define a chart title and category for the X and Y axes. If you do not want to define them, click the "Finish" button. A chart is then created based on the GPS qualification log data you selected.

3.9 SNMP

SNMP (Simple Network Management Protocol) is a set of standards for managing network devices, which includes a protocol, a database structure specification, and a set of data objects. The communication protocol involves one or more network management stations monitoring one or more network devices. SNMP enabled devices must have a SNMP agent application that is capable of handling network management functions requested by a network manager. The agent is also responsible for controlling the database of control variables defined in the product's MIB (Management Information Base).

3.9.1   SNMP Configuration

The SNMP setup page is used to configure the device's SNMP agent. The following steps can be used to quickly configure the device's SNMP agent while explaining the configuration options.

Login to the unit through its web-based interface as administrator.

Click on the System Setup link on the bottom of the screen to open the menu for system configurations.

Click on the SNMP link on the left side of the screen to enter the SNMP setup page.

Figure 3.9-1: SNMP Setup Screen

The SNMP agent has a number of access schemes that can be enabled/disabled, depending on your specific needs. The four schemes are described below.

SNMPv1/SNMPv2c – By enabling this access scheme, SNMP network managers may use SNMP version 1 or SNMP version 2 protocols to manage the device. Along with enabling/disabling this access scheme, you may change the read, read-write, and trap community names. The Trap Destination should be the network IP address of the management station handling any traps from the SNMP agent.

SNMPv3 (noAuth) – By enabling this access scheme, SNMP network managers may use SNMP version 3 protocol to manage the device. No form of PDU (Protocol Data Units) authentication or DES encryption is used. You may specify your own user name for this level of access.

SNMPv3 (auth) – By enabling this access scheme, SNMP network managers may use SNMP version 3 protocol to manage the device. This level of SNMPv3 has you select a form of PDU authentication (MD5 or SHA) but does not use DES encryption. You may specify your own user name and pass phrase for this level of access. The pass phrase is the secret key shared between the SNMP agent and manager, used in the MD5 or SHA authentication algorithm. The Pass phrase must be a minimum of 8 characters long.

SNMPv3 (authPriv) – By enabling this access scheme, SNMP network managers may use SNMP version 3 protocol to manage the device. This level of SNMPv3 also has you select a form of PDU authentication (MD5 or SHA) and performs DES encryption on all PDU's. You may specify your own user name and pass phrase for this level of access. The pass phrase is the secret key shared between the SNMP agent and manager, used in the MD5 or SHA authentication and DES encryption algorithms. The pass phrase must be a minimum of 8 characters long. NOTE: This access method is only available on secure products.

3.9.2   Spectracom MIB

Spectracom has been assigned the enterprise identifier 18837 by the IANA (Internet Assigned Numbers Authority). Spectracom's MIB for its time and frequency products resides under this enterprise identifier @ 18837.3.1 which is illustrated below.

```
                            iso
                             1
                             |
                            org
                             3
                             |
                            dod
                             6
                             |
                         internet
                             1
          _____|_____
         |                   |                   |
       mgmt            experimental            private
         2                   3                   4
         |                                       |
       mib-2                                 enterprises
         1                                       1
                                                 |
                                             spectracom
                                               18837
                                                 |
                                             specProducts
                                                 3
                                                 |
                                            specTimeFreqMIB
                                                 1
```
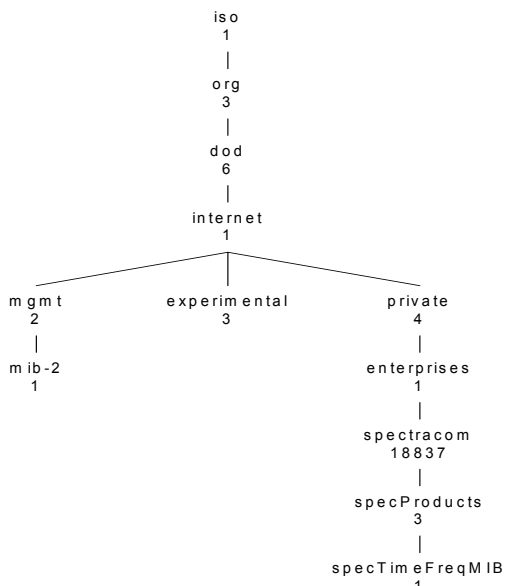
3.9.3   SNMP Support

Spectracom's private enterprise MIB can be obtained from customer service.

4 Operation

4.1 Status Indicator

At power up a quick LED test is run. The unit displays a **Red** – **Green** – **Orange** sequence to ensure the operation of the LEDs.

The table on the following page describes the operation of the LEDs. In this table, the terms "*Blink*" and *"Flash"* are used.

- **Blink** is defined as ½ second on, ½ second off
- **Flash** is defined as $^1/_{20}$ second on, $^{19}/_{20}$ second off

LABEL	COLOR	ACTIVITY	DESCRIPTION
POWER	Green	On Off	Power is supplied to the NetClock. Power is disconnected.
SYNC	Multi	Off	No fault but not synchronized to GPS. Holdover spec has not been met.
		Green On	Synced to GPS. Time is valid and within the Locked to GPS accuracy specs.
		Blinking Green	Holdover mode. Not synced to GPS but time is still within Holdover accuracy specs.
		Yellow On	No longer synced to GPS but no unit fault. Time accuracy may not be meeting holdover specs.
		Blinking Yellow	Unit is in power-up initialization mode. The unit is in this mode for the brief period between power on and when it is operationally ready to receive satellite data.
		Flashing Red	GPS antenna fault. This flash may occur over any of the other color conditions at runtime.
		Red On	Unit fault. Time may not be valid. Overrides all other indicators.
		Blinking Red	If the unit fails Power On Self Test (POST) then the indicator will blink in a sequence indicating the failure code (consult factory)
Ethernet (left)	Yellow	On Off	LAN Activity. No LAN traffic detected.
Ethernet (right)	Green	On Off	LAN Link established 10 or 100 Mb/s. No link established.

Table 4-1: Status Indicator

4.2 GPS

4.2.1 GPS Operation

HOW TO SET UP GPS RECEIVER:
Using the web browser, you will find the GPS configuration web page under the System Set up category. The GPS configuration web page is designed to allow a user to configure the GPS receiver to provide more accurate results and faster start up, but you do not have to configure them for the unit to run properly.

Figure 4.2-1: GPS Set-up Screen

ANTENNA CABLE DELAY:
To set this value, you must be logged into the unit with the Configuration or Administrator Mode. By setting the correct antenna cable delay, the on-time point is offset by the delay value to compensate for the antenna and in-line amplifier delays. Under typical condition, the expected cable and amplifier delays are negligible. You can calculate the delay based upon the manufacture's specification.

The range of the cable delay is from 0 to 999999 nanoseconds, the default value is 0 nanosecond, and the resolution is 1 nanosecond.

The following formula is used to calculate the cable delay:

D = (L * C) / V

Where:

      D =   Cable delay in nanoseconds
      L =   Cable length in feet
      C =   Constant derived from velocity of light: 1.016
      V =   Nominal velocity of propagation expressed as decimal, i.e. %66 = 0.66 Value is provided by cable manufacturer.

LOCATION OF THE UNIT:
You can read the current location of the unit calculated by the GPS receiver without logging in. The GPS receiver will automatically update this field when it has a Position Fix. Check the GPS Signal Status web page, and if the status is "Position Fix", then the location showed on this page is the right location.

You can only write the new location value to the unit when logged in under the Configuration or Administrator mode. The location input by the user may only help to speed up the time to first fix during the initial installation. The unit will automatically check the status of the GPS receiver after receiving the location input from the user, then based on the status of the GPS receiver, the unit will either tell the user that the GPS receiver already has finished the first fix and the input was abandoned, or send the location to the GPS receiver. To find the location for your city, please refer to the position table.

4.2.2   Set System Mode

The system supports two modes known as single satellite mode and standard mode.

Use single satellite mode if you are using a window mount antenna and cannot get more than four satellites. This will switch the qualification algorithm used, and allow the system to operate normally with fewer number of satellites, but the accuracy will be decreased because of the poor GPS antenna visibility.

Note: Always use standard mode if you are using a roof mount antenna and can get at least four satellites.   This is the default.

To set the System Mode using the webUI:
1. Using a PC with a web browser connect to the product by typing in the product's IP address into the address window of the browser as follows: http://10.10.200.1 (or your product's IP address).
2. Press the "Enter Main Page" button.
3. Select the login link on the top right corner to login as administrator.
4. On the lower menu line select the "System Setup" item.
5. On the left side menu select the "Set System Mode" item.
      The setup window for system mode is then displayed in the center of the screen.

4.2.3   GPS Signal Status

HOW TO READ THE GPS SIGNAL STATUS:
The GPS Signal Status pages provide insight into the GPS receiver's operation and the signal quality from the satellites. This information is useful to verify proper antenna placement and receiver performance during installation and later troubleshooting.

The overall tracking status, position solution and a table containing individual satellite data is on this page.

Figure 4.2-2: GPS Signal Status Setup Screen

Tracking X satellites:
Where: X = Number of satellites currently tracking (0 – 12)
GPS Status = SSSS
Where: SSSS = Receiver Status

Acquiring satellites is possible if the GPS Receiver is still looking for qualified satellites.

Bad Geometry is possible if the GPS Receiver is tracking qualified satellites, but the number of satellites or their relative position is not sufficient for calculating position.

2D Fix is possible if the receiver is tracking at least three qualified satellites.

3D Fix is possible if the receiver is tracking at least four qualified satellites.

Position Hold is possible if the GPS receiver has collected enough information to determine the location of the GPS receiver.

DOP = ##.#
Where: DOP means dilution of precision. The range is from 00.0 to 99.9
This value indicates the degree of uncertainty of a Position Fix due to the geometry of the Satellites used in the solution. The lower the DOP value, except 0, the lower the degree of uncertainty.

Antenna Sense = SSSSS
Where: SSSSS reports the status of the antenna sense circuit. There are three main flags (OK, Over Current, and Under Current). The three flags are described below:

OK Flag
The OK flag is displayed if both antenna sense bits are cleared. This indicates that the antenna is drawing current within the normal range.

Over Current Flag
This flag is displayed if the over current bit is set. This indicates that too much current is being drawn through the circuit and the overload protection circuit is limiting the feed current. The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.

Under Current Flag
This flag is displayed if the undercurrent bit is set. This indicates that little or no current is being drawn through the circuit, which may be due to a disconnected antenna, a severed antenna cable, or a damaged antenna. The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.
Undercurrent indication < 8 mA
Overcurrent indication > 80 mA

Latitude = [N:S][DD MM SS.SSSS]
Longitude = [E:W][DDD MM SS.SSSS]
Where: N = North latitude
S = South Latitude
E = East Longitude
W = West Longitude
D = Degree
M = Minute
S = Second

Quality = QQQQQ

Where: QQQQQ = Result of GPS qualification, either PASSED or FAILED. The GPS signal is considered qualified when at least one satellite is received having a vehicle ID greater than 1 and is available for Position Fix Usage.

Information on each satellite the receiver is currently tracking is presented in table form. The table columns are described below:

CHANNEL = Channel Number of the GPS receiver, 1…12

VID = Vehicle (satellite) Identification Number, 1…37

MODE = Channel Tracking Mode,

Where:
      0 =   Code Search
      1 =   Code Acquire
      2 =   AGC set
      3 =   Freq Acquire
      4 =   Bit Sync Detect
      5 =   Message Sync Detect
      6 =   Satellite Time Available
      7 =   Ephemeris Acquire
      8 =   Avail for position

Note: Mode 8 is the normal state for a valid satellite in use

---

STRENGTH = Signal strength value relative to the Signal to Noise Ratio [SNR].   Range: 0…255, the higher the number, the greater the receiver signal.

STATUS = Channel status flag. Convert the hexadecimal code word to binary to find the status flag set.
    Bit 11: Used for time

    Bit 10: Differential Correction Available

    Bit 9: Invalid Data

    Bit 8: Parity Error

    Bit 7: Used for Position Fix

    Bit 6: Satellite Momentum Alert Flag

    Bit 5: Satellite Anti-Spoof Flag Set

    Bit 4: Satellite Reported Unhealthy

    Bit 3-0: Satellite Accuracy as follows:

(Per para 20.3.3.3.13 ICD-GPS-200)
0000 (0) 0.00 <URA<=2.40
0001 (1) 2.40 <URA<=3.40
0010 (2) 3.40 <URA<=4.85
0011 (3) 4.85 <URA<=6.85
0100 (4) 6.85 <URA<=9.65
0101 (5) 9.65 <URA<=13.65
0110 (6) 13.65 <URA<=24.00
0111 (7) 24.00 <URA<=48.00
1000 (8) 48.00 <URA<=96.00
1001 (9) 96.00 <URA<=192.00
1010 (10) 192.00 <URA<=384.00
1011 (11) 384.00 <URA<=768.00
1100 (12) 768.00 <URA<=1536.00
1101 (13) 1536.00 <URA<=3072.00
1110 (14) 3072.00 <URA<=6144.00
1111 (15) 6144.00 <URA*

(* means No accuracy prediction is available – unauthorized users are advised to use the Space Vehicle at their own risk.)

Normal values for Status Field are

      8A0   or   8A1

Which is **1000 1010 000x** binary

Bit 11 = 1:	Used for time
Bit 10 = 0:	Differential Correction Not Available
Bit 9 = 0:	Not Invalid Data
Bit 8 = 0:	No Parity Error
Bit 7 = 1:	Used for Position Fix
Bit 6 = 0:	No Satellite Momentum Alert Flag
Bit 5 = 1:	Satellite Anti-Spoof Flag Set
Bit 4 = 0:	Satellite Reported as Healthy
Bit 3-0=low number:	Satellite is Accurate

4.2.4   Reception Troubleshooting

Please review this section prior to calling the Spectracom Customer Service Department. If the reception problem cannot be solved following the guidelines outlined in this section, please call for Customer Service at 585.321.5800.

No Reception
Cable or connector problem: Measure the antenna cable resistance to verify the integrity of the cable and connectors. Remove the antenna cable from the rear panel of the receiver and measure the resistance from the coax center to shield. Refer to Table 4-2 for typical resistance values of the antenna and inline amplifier alone and when combined.

DEVICE	DESCRIPTION	RESISTANCE (SP)
8228	Indoor Antenna	140 ohms
8225	Outdoor Antenna	180 ohms
8227	In-line Amplifier	165 ohms
8225 and 8227	Antenna/Amplifier	85 ohms

Table 4-2: Typical Antenna Cable Resistance Values

Failed Impulse Suppressor: The Model 8226 provides lightning protection when the outdoor GPS antenna is used. The Model 8226 has high impedance when measuring from the center conductor to ground and a low throughput resistance. A failing impulse suppressor may be tripping prematurely. The easiest way to test the Model 8226 is to temporarily replace it with a Type N barrel connector. If the receiver begins tracking satellites within 20 minutes, the impulse suppressor has failed and must be replaced.

Cable Length: The Model 8228 Indoor Antenna is supplied with 50 feet of antenna cable. Do not add cable. Excessively long or improper cable type may prevent the receiver from tracking satellites. Refer to Section 2.2 for cable recommendations when using the Model 8225 Outdoor Antenna.

Antenna Location: The antenna must have a good view of the sky. Refer to Section 2.1 for indoor antenna guidelines and Section 2.2 for outdoor antenna guidelines.

Window Type: Windows with metal film coatings, metal screens or blinds may impede GPS reception.

Low GPS Quality

Cable Length: Excessively long or improper cable type may cause low GPS quality due to cable attenuation. Long GPS antenna lengths may require an inline amplifier or lower loss cable. Refer to Section 2.2.2 for GPS cable recommendations and Section 2.2.4 for inline amplifier information when using the Model 8225 Outdoor Antenna.

The Model 8228 Indoor Antenna is provided with a 50-foot antenna cable. Do not substitute or add coax to the provided cable.

Antenna Location: The antenna must have a view of the sky with views to the horizon. Nearby obstructions can reduce the receiver's ability to track the maximum number of satellites available.

Window Type: Windows with metal film coatings, metal screens or blinds may reduce GPS reception.

5 Troubleshooting

5.1 Front Panel Power and Sync Lamps

Symptom	CAUSE	Corrective Action
Power LED is off	No power to the unit	• Ensure the AC power is live to the power adapter • Ensure the adapter is plugged in properly into the unit • Ensure no other connecting cables to the unit are pinched or shorted • Replace the power adapter
Sync LED		
New install and Sync LED is not lit	Not enough time has elapsed or can't track satellites	If less than 20 minutes since power-on, continue monitoring. If longer than about 20 minutes, refer to section 4.2.4 reception troubleshooting
Flashing Green	Recently stopped Tracking satellites (The unit has not timed-out of hold-over mode).	(Time is still valid. Other devices will still be synced). Refer to section 4.2.4 reception troubleshooting. Review the Alarm and Qualification logs.
Yellow	Not tracking Satellites (No longer in hold-over mode).	(Time is no longer valid). Other devices will not be synced. Refer to section 4.2.4 reception troubleshooting. Review the Alarm and Qualification logs.
Flashing Red	GPS antenna fault.	There is a short or open in the GPS antenna cable. Verify the antenna is connected. Using a multimeter, measure continuity of the cable to verify no open or shorts in the GPS cable. Refer to section 4.2.4 reception troubleshooting.
Red stays On	Unit fault. Time may not be valid. Overrides all other indicators.	Contact Customer Service
Blinking Red	If the unit fails Power On Self Test (POST) then the indicator will blink in a sequence indicating the failure code (consult factory)	Contact Customer Service

5.2 Front Panel LAN Connector

Symptom	Cause	Corrective Action
LAN Green LED is off (This LED also known as Good Link indicator).	Unit is not connected to the network	• Check LAN cable connections (Straight-thru network cable if connected to Hub/Switch, cross-over if connected direct to a PC). • Be sure to use a straight-through cable when connecting to a hub, a cross-over cable when connecting directly to a PC. • Check that the hub/switch/router device port is active and set to the correct port speed.
LAN Green on the Time Server but the Gold Link indicator on the HUB/Switch is not lit.	The Time Server and the HUB/Switch are not communicating at the correct port speed.	• If the Hub/switch is set to auto, power cycle the Time Server with the network cable connected. This will cause Auto-Negotiate to determine the settings of the HUB/Switch (Auto-Negotiate only occurs at power-on). • Try setting the HUB/Switch to 100mbps and 10mpps
Can "Ping" the unit but can't point web browser to the unit	• Gateway not configured correctly • Web Browser proxy settings not correct	• If the network has a Gateway, verify the Gateway has been set correctly and is enabled. • Verify the proxy settings in the web browser program are correct.
Can use web browser to configure the unit but can't synchronize any PC's with the Time Server	PC software not installed or configured correctly.	• Install YATS32 shareware program from www.dillobits.com. This program will allow you to view the raw NTP data to verify that the Time Server is outputting time data. Refer to the Spectracom website Support page for additional information on YATS32. • Refer to Spectracom website Support page for additional information on syncing PC's. • Verify the Sync lamp is solid green.
Unable to communicate with the unit on the network	Improper IP addressing	• Make sure your IP address and subnet mask are set correctly. • Make sure the unit is within the same Class and/or subnet range as the computers with which you are trying to communicate • Check that the hub/switch/router device port is active and set to the correct port speed. • Be sure to use a straight-through cable when connecting to a hub, a cross-over cable when connecting directly to a PC. • Consult your Network System Administrator.

5.3 Customer Service

Refer to Section 1.2, Warranty Information and Product Support for information on contacting Spectracom Customer Service for assistance.

6 Appendices

6.1 *Software Commands*

From the rear panel RS-232 Serial Setup Port, the user can manage files and configure network settings for the product. Table 6-1 provides a listing of the command set in alphabetical order and the page where you can find the description of the command. These commands may contain a set of subcommands that that are used to configure individual attributes for that subsystem.

Command	Description Page
help	Help
login	Log in at a specified security level
logout	Log out of the current security level
net	**Network configuration commands**
gateway	Enable/disable or set the default gateway
help	Display summaries of the network subcommands
ip	Set the IP address
mac	Set the Mac Address
mask	Set the subnet mask
show	Show network parameters
http	Enable/disable http access to the unit
reboot	Reboot the unit
sec	**Security Commands**
help	Display summaries of the security subcommands
level	Display the current security level
password	Set the password for the current security level
update	**Firmware Update Commands**
boot	Update the Boot Monitor
csl	Update the CSL
help	Display summaries of the update subcommands

Table 6-1: Alphabetical List of Commands

NOTE: The commands shown in this section are all in lower case format. The NetClock/NTP accepts commands in upper or lower case formats.

help

The command, *help*, displays a summary of the available commands at the current security level. The user may specify a particular command or set of commands to display more detailed help information. The *help* command is intended for novice users. The novice user can use this command to aid them learning the individual syntax for system commands.

The *help* command is available at the *user* security level.

To list the available commands at the current security level, issue the *help* command as shown below:

Type: help <ent>

Example Response:
help   Commander Help Function
dir   dir [path] - list current directory
pwd   pwd - print working directory
cd   cd [path] - change directory
delete   delete [file] - remove a file
type   type [file] - print the contents of a file
sec   sec <command> <arguments> - invoke security commands
login   login <account> <password> - access secure areas
logout   logout - exit secure areas
net   net <command> <arguments> - invoke network commands

To list the files and directories in the parent directory of the current working directory, issue the *dir* command as follows:

Type: help COMMAND <ent>
Where: COMMAND = the command to obtain help on.

Example, The current working directory is */test* and it contains a file named *data.txt*.

Follow the example below to display help about the *net* command.

Type: help net <ent>
Response: the 'net' group of commands is used to access and manage the network interface

login

The command, *login*, is used to change the current security level. The user may specify the security level and password after the command or fill them in when prompted. The *login* command is intended for advanced users. The advanced user can use this command to log in to the unit at either the config or admin level.

The *login* command is available at the *user* security level.

To log in to the unit at a different security level, issue the *login* command as shown below:

Type:	login LEVEL<ent>
Response:	`Password:`
Type:	PASSWORD <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	LEVEL Level
Where:	LEVEL = the security level to log in as.
	PASSWORD = the password for the specified security level.

To log in to the unit at a different security level and be prompted for the level and password, issue the *login* command as follows:

Type:	login <ent>
Response:	`Account:`
Type:	LEVEL <ent>
Response:	`Password:`
Type:	PASSWORD <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	LEVEL Level
Where:	LEVEL = the security level to log in as.
	PASSWORD = the password for the specified security level.

Follow the example below to log in to the unit at the config security level.

Type:	login config <ent>
Response:	`Password:`
Type	config12 <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level

logout

The command, *logout*, is used to change the current security level to the user level. The *logout* command is intended for advanced users. The advanced user can use this command to restore the security level back to the user level after they have completed any commands that required a higher security level.

The *logout* command is available at the *user* security level.

To log out of the unit to the user security level, issue the *logout* command as shown below:

Type: logout <ent>
Response: Logout Successful
now at: User Level

net

The command, *net*, is used to configure the network interface. The *net* command consists of a set of subcommands that are used to get, set or change each individual network setting. Some of the network settings require config level security in order to set or change them.

To invoke one of the *net* subcommands, issue the *net* command as shown below:

Type: net SUBCOMMAND [ARGUMENTS] <ent>
Where: SUBCOMMAND =   The subcommand to invoke.
                          ARGUMENTS =   The arguments required for the specified
subcommand.

To display a list of the available subcommands for the *net* command along with a summary description of each, issue the *net* command as follows:

Type: net <ent>
Response: use the 'net help' command to see a list of net commands
                         use the 'net help <sub-command>' to get detailed help about that
                         command

help	net help - list of net commands
mask	net mask mmm.mmm.mmm.mmm - set new network mask
ip	net ip nnn.nnn.nnn.nnn - set new ip address
show	net show - display network configuration to the user
default	net default - set all net parameters back to default values
gateway	net gateway [yes,no] [address] – enable gateway
mac	net mac [xx:xx:xx:xx:xx:xx] - get or set MAC address
http[*]	net http [yes,no] – enable or disable http access to the unit

The following are the set of subcommands for the *net* command:

---

[*] This feature is only available for secure Spectracom products

net gateway

The **net** subcommand, **gateway**, is used to display, enable/disable, and/or set the IP address of the default gateway. The **gateway** subcommand is intended for advanced users. The advanced user can use this command to configure the address of the router that will be used as the default gateway for sending information beyond the local area network (LAN).

The **gateway** subcommand is available at the *user* security level to display the current setting.
The **gateway** subcommand is available at the *config* security level to set a new value.

To display the current gateway setting, issue the **gateway** subcommand as shown below:

Type:	net gateway <ent>
Response:	Network default gateway STATUS
Gateway IP:	GATEWAY_ADDRESS
Where:	STATUS =enabled or disabled.
	GATEWAY_ADDRESS =The IP address of the gateway.

To enable or disable the gateway, issue the **gateway** subcommand as shown below:

Type:	login config <ent>
Response:	Password:
Type	PASSWORD <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Where:	PASSWORD = The password for config security level.
Type:	net gateway ENABLE <ent>
Response:	SETTING default gateway: GATEWAY_ADDRESS
	Gateway command successful
Where:	ENABLE = yes or no.
	SETTING = Enabling or Disabling..
	GATEWAY_ADDRESS = The IP address of the gateway.

To enable the gateway and set the gateway IP address, issue the **gateway** subcommand as shown below:

Type:	login config <ent>
Response:	Password:
Type	PASSWORD <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Where:	PASSWORD = The password for config security level.
Type:	net gateway yes GATEWAY_ADDRESS <ent>
Response:	Enabling default gateway: GATEWAY_ADDRESS
	Gateway command successful
Where:	GATEWAY_ADDRESS = The IP address of the gateway.

Follow the example below to enable a gateway with IP address 192.168.0.200.

Type:	login config <ent>
Response:	Password:

Type	config12 <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Type:	net gateway yes 192.168.0.200 <ent>
Response:	Enabling default gateway: 192.168.0.200
	Gateway command successful

NOTE: Attempting to enable or set a gateway with an invalid IP address or an IP address that is not on the same subnet will result in an error. Be sure the desired gateway exists and is reachable on the LAN before setting/enabling it with the **net gateway** subcommand.

---

net help

The **net** subcommand, **help**, is used to display a list of the available subcommands and a brief usage summary for each of them. The **help** subcommand is intended for novice users. The novice user can use this command to aid them learning the individual syntax for **net** subcommands.

The **help** subcommand is available at the *user* security level.

To display a list of the available subcommands and brief usage of each, issue the **help** subcommand as shown below:

Type:	net help <ent>
Response:	
help	net help - list of net commands
mask	net mask mmm.mmm.mmm.mmm - set new network mask
ip	net ip nnn.nnn.nnn.nnn - set new ip address
show	net show - display network configuration to the user
default	net default - set all net parameters back to default values
gateway	net gateway [yes,no] [address] – enable gateway
mac	net mac [xx:xx:xx:xx:xx:xx] - get or set MAC address

net ip

The **net** subcommand, **ip**, is used to set the IP address for the unit. The **ip** subcommand is intended for advanced users. The advanced user can use this command to statically configure the IP address of the unit so that it may be accessed via the network.

The **ip** subcommand is available at the *config* security level to set a new value.

To set the IP address for the unit, issue the **ip** subcommand as shown below:

Type:	login config <ent>
Response:	Password:
Type	PASSWORD <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Where:	PASSWORD = The password for config security level.

Type:	net ip IP_ADDRESS <ent>
Response:	Setting new address: IP_ADDRESS
Stack IP address:	IP_ADDRESS
	New IP address set
Where:	`IP_ADDRESS` =The IP address for the unit.

Follow the example below to set the unit to have an IP address of 192.168.0.100.

Type:	login config <ent>
Response:	`Password:`
Type	config12 <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Type:	net ip 192.168.0.100 <ent>
Response:	Setting new address: 192.168.0.100
Stack IP address:	192.168.0.100
	New IP address set

NOTE: The Stack IP address reflects the value that the TCP/IP stack is set to. This should match the IP address being set.

---

net mac

The **net** subcommand, **mac**, is used to display the Ethernet MAC address for the unit. The **mac** subcommand is intended for advanced users. The advanced user can use this command to retrieve the Ethernet MAC address of the unit for uses such as network traffic monitoring.

The **mac** subcommand is available at the *user* security level to get the value.

To get the Ethernet MAC address for the unit, issue the **mac** subcommand as shown below:

Type:	net mac <ent>
Response:	MAC address: XX;XX;XX;XX;XX;XX
Where:	`XX;XX;XX;XX;XX;XX` = The Ethernet MAC address for the unit.

net mask

The **net** subcommand, **mask**, is used to set the subnet mask for the unit. The **mask** subcommand is intended for advanced users. The advanced user can use this command to configure the subnet mask of the unit so that it may be accessed via the network.

The **mask** subcommand is available at the *config* security level to set a new value.

To set the IP address for the unit, issue the **mask** subcommand as shown below:

Type:	login config <ent>
Response:	`Password:`
Type	PASSWORD <ent> (the terminal will not show what you type)

Response:	Login Successful
Security Level is now:	Config Level
Where:	PASSWORD = The password for config security level.
Type:	net mask NETMASK <ent>
Response:	Setting new netmask: NETMASK
Stack netmask:	NETMASK
	New netmask Has been set
Where:	NETMASK =The subnet mask for the unit.

Follow the example below to set the unit to have an IP address of 255.255.0.0.

Type:	login config <ent>
Response:	Password:
Type	config12 <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Type:	net mask 255.255.0.0 <ent>
Response:	Setting new netmask: 255.255.0.0
Stack netmask:	255.255.0.0
	New netmask Has been set

NOTE: The Stack netmask reflects the value that the TCP/IP stack is set to. This should match the netmask value being set.

---

net show

The *net* subcommand, *show*, is used to display a list of the available subcommands and a brief usage summary for each of them. The *show* subcommand is intended for novice users. The novice user can use this command to aid them learning the individual syntax for *net* subcommands.

The *show* subcommand is available at the *user* security level.

To display a list of the current network parameters, issue the *show* subcommand as shown below:

Type:	net show <ent>
Response:	Network Configuration
IP address:	IP_ADDRESS
Netmask address:	NETMASK
Network gateway:	STATUS
Gateway IP:	GATEWAY_ADDRESS
MAC address:	XX:XX:XX:XX:XX:XX
Where:	IP_ADDRESS =The IP address for the unit.
	NETMASK =The subnet mask for the unit.
	STATUS =enabled or disabled.
	GATEWAY_ADDRESS =The IP address for the default gateway.
	XX:XX:XX:XX:XX:XX =The Ethernet MAC address for the unit.

The example below displays the network settings for an example unit

Type:	net show <ent>
Response:	Network Configuration
IP address:	10.10.200.104
Netmask address:	255.255.0.0
Network gateway:	enabled
Gateway IP:	10.10.200.201
MAC address:	00:0c:ec:00:01:cc

net http[*]

The **net** subcommand, **http**, is used to enable or disable the HTTP protocol.

The **http** subcommand is available at the *administrator* security level only.

To display the current http setting, issue the **http** subcommand as shown below:

Type:	login admin <ent>
Response:	Password:
Type	password <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = The password for admin security level.
Type:	net http <ent>
Response:	Network HTTP status
	where status = enable or disabled

To disable HTTP issue the following command:

Type:	login admin <ent>
Response:	Password:
Type	password <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = The password for admin security level.
Type:	net http no <ent>
Response:	HTTP Disabled

To enable HTTP issue the following command:

Type:	login admin <ent>
Response:	Password:
Type	password <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = The password for admin security level.
Type:	net http yes <ent>
Response:	HTTP Enabled

---

[*] This feature is only available for secure Spectracom products

reboot [bootloader]

The *reboot* is used to warm-boot the unit without having to disconnect or reconnect the power supply. The *reboot* command is intended only for administrators, and is available at the *admin* security level. The optional *bootloader* argument is used to reboot into the bootloader for software upgrade; which cannot be performed from the application.

To reboot the unit, login as administrator, then issue the *reboot* command as shown here:

Type:	login admin <ent>
Response:	Password:
Type	PASSWORD <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = The password for admin security level.
Type:	reboot <ent>
Response:	Rebooting...

> **NOTE:** This command provides a convenient way to remotely update application software in that the unit will automatically execute the most recent image in /sys/bin/.

> **CAUTION:** Do not reboot the unit while file uploads are in progress. Do not reboot the unit with non-application images are located in /sys/bin/. If either of these conditions is not fulfilled, the unit may fail to boot the application image, which could result in a unit that function incorrectly or not at all.

sec

The command **sec** is used to configure the security feature. The **sec** command consists of a set of subcommands that are used to get, set or change each individual security feature setting. Some of the sec settings require config level security or admin level in order to set or change them.

To invoke one of the **sec** subcommands, issue the **sec** command as shown below:

Type: sec SUBCOMMAND [ARGUMENTS] <ent>
Where: SUBCOMMAND = the subcommand to invoke.
                                              ARGUMENTS = the arguments required for the specified
                                              subcommand.

To display a list of the available subcommands for the **sec** command along with a summary description of each, issue the **sec** command. Based on the security level you are in, the response will be different. We list them all in the following.

Type: sec <ent>

1. If you are in user level

Response:
level   sec level - show the current security level
help   sec help - list of sec sub-commands and detailed information   on
                                              each

2. Under config level

Response:
level   sec level - show the current security level
help   sec help - list of sec sub-commands and detailed information on
                                              each

3. Under admin level

Response:
account   sec account <Account-Name> <new-name>
level   sec level - show the current security level
password sec password <Account-Name>
help   sec help - list of sec sub-commands and detailed information on each

The following are the set of subcommands for the **sec** command:

sec level

The **sec** subcommand, **level** is used to show the current security level.

The **level** subcommand is available at the *user* security level.

To show the current security level, issue the **level** subcommand as shown below:

| Type: | sec level <ent> |
| Response: | Security Level is: User Level |

sec help

The *sec* subcommand *help* is used to list of sec sub-commands and detailed information on each. The *help* subcommand is available at the any *security* level. You will get different result based on the security level you are in now.

To get a list of *sec* sub-commands and detailed information on, issue the *help* subcommand as shown below:

1. Under *user* mode

Type:	sec help <ent>
Response:	Login Successful
Security Level is now:	Config Level

2. Under *config* mode

Type:	login config <ent>
Response:	`Password:`
Type	config12 <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level
Type:	sec help <ent>
Response:	
level	sec level - show the current security level
help	sec help - list of sec sub-commands and detailed information on each

3. Under *admin* mode

Type:	login admin <ent>
Response:	`Password:`
Type	admin123 <ent> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Admin Level
Type:	sec help <ent>
Response:	

     account   sec account <Account-Name> <new-name>
     level   sec level - show the current security level
     password   sec password <Account-Name>
     help   sec help - list of sec sub-commands and detailed information on each

sec password

The *sec* subcommand *password* is used to set an account name. The *password* subcommand is only available at the *admin* security level.

To set the account under *admin* mode, issue the *password* subcommand as shown below:

Type: login admin <ent>
Response: Password:
Type   admin123 <ent> (the terminal will not show what you type)
Response: Login Successful
Security Level is now: Admin Level
Type: sec password <ent>
Response: Account:
Type: [current account name] <ent>
Response: Old Password:
Type: [current password for this account] <ent>
Response: New Password:
Type: [New password for this account] <ent>
Response: New Password (again):
Type: [New password for this account] <ent>
Response: New Password set

update

The command, *update*, is used to install a new bootloader into the unit. The *update* command consists of a set of subcommands that are used to update each portion that can be modified. Since correct installation of the bootloader is critical to operation, this entire menu requires admin level security in order to use them.

To invoke one of the *update* subcommands, issue the *update* command as shown below:

Type: update SUBCOMMAND [ARGUMENTS] <ent>
Where: SUBCOMMAND =The subcommand to invoke.
                                        ARGUMENTS =The arguments required for the specified
                                        subcommand.

To display a list of the available subcommands for the *update* command along with a summary description of each, issue the *update* command as follows:

Type: update <ent>
Response:
help   update help - list each subcommand and its description
csl   update csl <filename> - install a new CSL image
boot   update boot <filename> - install a new bootload image
app   update app <filename> - install a new application
kern   update kern <filename> - install a new kernel

The following are the set of subcommands for the update command:

update app

The *update* subcommand, *app*, is used to update the application image for the unit. The *app* subcommand is intended only for advanced users that have been provided with an updated application image.

The *app* subcommand is only available at the *admin* security level.

To install a new CSL image into the unit, upload the image to the unit's /update directory via FTP or secure copy. Then issue the *update app* command as shown here:

Type:	login admin <ent>
Response:	`Password:`
Type	PASSWORD<ent>
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = the password for admin security level.
Type:	update app APPFILE <ent>
Response:	App image installed successfully.
Where:	APPFILE = the name of the application image.

> **CAUTION:** Do not power down or reboot the unit while running this command. Do not install files that are not application images. If a non-application image is installed it can be overwritten by re-updating with a correct application image.   The unit will operate incorrectly or completely fail to run if this command is not used with care.

update boot

The update subcommand, boot, is used to update the bootloader image for the unit. The boot subcommand is intended only for advanced users that have been provided with an updated bootloader image.

The boot subcommand is only available at the admin security level.

To install a new bootloader image into the unit, upload the image to the unit's /update directory via FTP or secure copy. Then issue the update boot command as shown here:

Type:	login admin <ent>
Response:	`Password:`
Type	PASSWORD<ent>
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = the password for admin security level.
Type:	update boot BOOTFILE <ent>
Response:	Boot image installed successfully.
Where:	BOOTFILE = the name of the Boot image.

> **CAUTION:** Do not power down or reboot the unit while running this command. Do not install files that are not bootloader images. If a non-bootloader image is installed it can be overwritten by re-updating with a correct bootloader image.   The unit will operate incorrectly or completely fail to run if this command is not used with care.

update csl

The *update* subcommand, *csl*, is used to update the CSL image for the unit. The *csl* subcommand is intended only for advanced users that have been provided with an updated CSL image.

The *csl* subcommand is only available at the *admin* security level.

To install a new CSL image into the unit, upload the image to the unit's /update directory via FTP. Then issue the *update csl* command as shown here:

Type:	login admin <ent>
Response:	`Password:`
Type	PASSWORD<ent>
Response:	Login Successful
Security Level is now:	Admin Level
Where:	PASSWORD = the password for admin security level.
Type:	update csl CSLFILE <ent>
Response:	CSL image installed successfully.
Where:	CSLFILE = the name of the CSL image.

CAUTION: Do not power down or reboot the unit while running this command. Do not install files that are not CSL images. If a non-CSL image is installed it can be overwritten by re-updating with a correct CSL image.   The unit will operate incorrectly or completely fail to run if this command is not used with care.

---

update kern

The *update* subcommand, *kern*, is used to update the kernel image for the unit. The *kernel* subcommand is intended only for advanced users that have been provided with an updated kernel image.

The *kern* subcommand is only available at the *admin* security level.

To install a new kernel image into the unit, upload the image to the unit's /update directory via FTP. Then issue the *update kern* command as shown here:

Type: login admin <ent>
Response: Password:
Type   PASSWORD<ent>
Response: Login Successful
Security Level is now: Admin Level
Where: PASSWORD = the password for admin security level.
Type: update kern KERNFILE <ent>
Response: Kernel image installed successfully.
Where: KERNFILE = the name of the CSL image.

> **CAUTION:** Do not power down or reboot the unit while running this command. Do not install files that are not kernel images. If a non-kernel image is installed it can be overwritten by re-updating with a correct kernel image.   The unit will operate incorrectly or completely fail to run if this command is not used with care.

update help

The *update* subcommand, *help*, is used to display a list of the available subcommands and a brief usage summary for each of them. The *help* subcommand is intended for novice users. The novice user can use this command to aid them learning the individual syntax for *update* subcommands.

The *help* subcommand is available at the *admin* security level.

To display a list of the available subcommands and brief usage of each, issue the *help* subcommand as shown below:

Type: update help <ent>
Response:
help   update help - list each subcommand and its description
csl   update csl <filename> - install a new CSL image
boot   update boot <filename> - install a new bootload image
app   update app <filename> - install a new application
kern   update kern <filename> - install a new kernel

6.2 Serial Data Formats

This section describes each of the data format selections available on the RS-232 (Serial Comm) and RS-485 (Remote Port) outputs. Format selection is made as part of the Serial Comm and Remote port configuration. Most applications utilize Data Format 0 or Data Format 2.

Format 0:
Format 0 includes a time sync status character, day of year, time reflecting time zone offset and DST corrections when enabled. Format 0 also includes the DST/Standard Time indicator, and the time zone offset value. Format 0 data structure is shown below:

CR LF I ^ ^ DDD ^ HH:MM:SS ^ DTZ=XX CR LF

where:

CR =	Carriage Return
LF =	Line Feed
I =	Time Sync Status (space, ?, *)
^ =	space separator
DDD =	Day of Year (001 - 366)
HH =	Hours (00-23)
: =	Colon separator
MM =	Minutes (00-59)
SS =	Seconds (00- 60)
D =	Daylight Savings Time indicator (S,I,D,O)
TZ =	Time Zone
XX =	Time Zone offset (00-23)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time sync status character I is defined as described below:

(Space) =   Whenever the front panel Time Sync lamp is green.
       ? =   When the receiver is unable to track any satellites and the Time Sync lamp is red.
       * =   When the receiver time is derived from the battery backed clock or set manual through the Setup Port Interface.

The Daylight Saving Time indicator D is defined as:

S =	During periods of Standard time for the selected DST schedule.
I =	During the 24-hour period preceding the change into DST
D =	During periods of Daylight Saving Time for the selected DST schedule
O =	During the 24-hour period preceding the change out of DST

Example: 271 12:45:36 DTZ=08
The example data stream provides the following information:

Sync Status:	Time synchronized to GPS
Date:	Day 271
Time:	12:45:36 Pacific Daylight Time
	D = DST, Time Zone 08 = Pacific Time

Format 1:

This format provides the fully decoded time data stream. Format 1 converts the received day of year data (001-366) to a date consisting of day of week, month, and day of the month. Format 1 also contains a time sync status character, year, and time reflecting time zone offset and DST correction when enabled. Format 1 data structure is shown below:

CR LF I ^ WWW ^ DDMMMYY ^ HH:MM:SS CR LF

where:

CR =		Carriage Return
LF =		Line Feed
I =		Time Sync Status (space, ?, *)
^ =		space separator
WWW =		Day of Week (SUN, MON, TUE, WED, THU, FRI, SAT)
DD =		Numerical Day of Month (^1-31)
MMM =		Month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC)
YY =		Year without century (99, 00, 01 etc.)
HH =		Hours (00-23)
: =		Colon separator
MM =		Minutes (00-59)
SS =		Seconds (00 - 60)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time sync status character I is defined as described below:

(Space) =   Whenever the front panel Time Sync lamp is green.
? =   When the receiver is unable to track any satellites and the Time Sync lamp is red.
* =   When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

Example: * FRI 20APR01 12:45:36

The example data stream provides the following information:

Sync Status: The clock is not time synchronized to GPS. Time is derived from the battery backed clock or set manually

Date: Friday, April 20, 2001
Time: 12:45:36

Format 2:

This format provides a time data stream with millisecond resolution. The Format 2 data stream consists of indicators for time sync status, time quality, leap second and Daylight Saving Time. Time data reflects UTC time and is in the 24-hour format. Format 2 data structure is shown below:

CR LF IQYY ^ DDD ^ HH:MM:SS.SSS ^ LD

where:

CR =	Carriage Return
LF =	Line Feed
I =	Time Sync Status (space, ?, *)
Q =	Quality Indicator (space, A, B, C, D)
YY =	Year without century (99, 00, 01 etc.)
^ =	space separator
DDD =	Day of Year (001 - 366)
HH =	Hours (00-23 UTC time)
: =	Colon separator
MM =	Minutes (00-59)
SS =	Seconds (00-60)
. =	Decimal Separator
SSS =	Milliseconds (000-999)
L =	Leap Second Indicator (space, L)
D =	Daylight Saving Time Indicator (S,I,D,O)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time sync status character I is defined as described below:

(Space) =   Whenever the front panel Time Sync lamp is green.
     ? =   When the receiver is unable to track any satellites and the Time Sync lamp is red.
     * =   When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The quality indicator Q provides an inaccuracy estimate of the output data stream. When the receiver is unable to track any GPS satellites, a timer is started. Table 6-2: Table of Quality Indicators lists the quality indicators and the corresponding error estimates based upon the GPS receiver 1 PPS stability and the time elapsed tracking no satellites. The Tracking Zero Satellites timer and the quality indicator reset when the receiver reacquires a satellite.

Inaccuracy Code	Time Error (mSec)	Time Since Unlock (Hours)
Space	<1	Locked
A	<10	<10
B	<100	<100
C	<500	<500
D	>500	>500

Table 6-2: Table of Quality Indicators

The leap second indicator L is defined as:

(Space) =   When a leap second correction is not scheduled for the end of the month.
      L =   When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator D is defined as:

      S =   During periods of Standard time for the selected DST schedule.
       I =   During the 24-hour period preceding the change into DST.
      D =   During periods of Daylight Saving Time for the selected DST schedule.
      O =   During the 24-hour period preceding the change out of DST.

Example: ?A01 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status: The clock has lost GPS time sync. The inaccuracy code of "A" indicates the expected time error is <10 milliseconds.

Date: Day 271 of year 2001.

Time: 12:45:36 UTC time, Standard time is in effect.

Format 3:

Format 3 provides a format identifier, time sync status character, year, month, day, time with time zone and DST corrections, time difference from UTC, Standard time/DST indicator, leap second indicator and on-time marker. Format 3 data structure is shown below:

FFFFI^YYYYMMDD^HHMMSS±HHMMD L # CR LF

where:

FFFF =	Format Identifier (0003)
I =	Time Sync Status (Space, ? *)
^ =	space separator
YYYY =	Year (1999, 2000, 2001 etc.)
MM =	Month Number (01-12)
DD =	Day of the Month (01-31)
HH =	Hours (00-23)
MM =	Minutes (00-59)
SS =	Seconds (00-60)
± =	Positive or Negative UTC offset (+,-) Time Difference from UTC
HHMM =	UTC Time Difference Hours, Minutes (00:00-23:00)
D =	Daylight Saving Time Indicator (S,I,D,O)
L =	Leap Second Indicator (space, L)
# =	On time point
CR =	Carriage Return
LF =	Line Feed

The time sync status character I is defined as:

(Space) =	Whenever the front panel Time Sync lamp is green.
? =	When the receiver is unable to track any satellites and the Time Sync lamp is red.
* =	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The time difference from UTC, ±HHMM, is selected when the Serial Comm or Remote port is configured. A time difference of -0500 represents Eastern Time. UTC is represented by +0000.

The Daylight Saving Time indicator D is defined as:

S =	During periods of standard time for the selected DST schedule.
I =	During the 24-hour period preceding the change into DST.
D =	During periods of Daylight Saving Time for the selected DST schedule.
O =	During the 24-hour period preceding the change out of DST.

The leap second indicator L is defined as:

(Space) =	When a leap second correction is not scheduled at the end of the month.
L =	When a leap second correction is scheduled at the months end.

Example: 0003 20010415 124536-0500D #

The example data stream provides the following information:

Data Format: 3

Sync Status: Time Synchronized to GPS.

 Date: April 15, 2001.

Time: 12:45:36 EDT (Eastern Daylight Time), The time difference is 5 hours behind UTC.

Leap Second: No leap second is scheduled for this month.

Format 4:

Format 4 provides a format indicator, time sync status character, modified Julian date, time reflecting UTC with 0.1 millisecond resolution and a leap second indicator. Format 4 data structure is shown below:

FFFFIMJDXX^HHMMSS.SSSS^L CR LF

where:
FFFF =	Format Identifier (0004)
I =	Time Sync Status (Space, ? *)
MJDXX =	Modified Julian Date
HH =	Hours (00-23 UTC time)
MM =	Minutes (00-59)
SS.SSSS =	Seconds (00.0000-60.0000)
L =	Leap Second Indicator (^, L)
CR =	Carriage Return
LF =	Line Feed

The start bit of the first character marks the on-time point of the data stream.

The time sync status character I is defined as:

(Space) =	Whenever the front panel Time Sync lamp is green.
? =	When the receiver is unable to track any satellites and the Time Sync lamp is red.
* =	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The leap second indicator L is defined as:

(Space) =	When a leap second correction is not scheduled at the end of the month.
L =	when a leap second correction is scheduled at the months end.

Example: 0004 50085 124536.1942 L

The example data stream provides the following information:

Data format:	4
Sync Status:	Time synchronized to GPS.
Modified Julian Date:	50085
Time:	12:45:36.1942 UTC
Leap Second:	A leap second is scheduled at the end of the month.

Format 90:

Format 90 provides a position data stream in NMEA 0183 GPGGA GPS Fix data format.
The Format 90 data structure is shown below:

$GPGGA,HHMMSS.SS,ddmm.mmmm,n,dddmm.mmmm,e,Q,SS,YY.y,+AAAAA.a,M,,,,*CC CR LF

where:

$GP =	GPS System Talker
GGA =	GPS Fix Data Message
HHMMSS.SS =	Latest time of Position Fix, UTC. This field is blank until a 3D fix is acquired
ddmm.mmmm,n =	Latitude
dd =	degress, 00...90
mm.mmmm =	minutes, 00.0000....59.9999
n =	direction, N = North, S = South
dddmm.mmmm,e =	Longitude
ddd =	degress, 000...180
mm.mmmm =	minutes, 00.0000....59.9999
e =	direction, E = East, W = West
Q =	Quality Indicator,
0 =	No 3D fix
1 =	3D fix
SS =	Number of satellites tracked, 0...8
YY.Y =	Dilution of precision, 00.0...99.9
+AAAAA.a,M =	Antenna height in meters, referenced to mean sea level
,,,, =	Fields for geoidal separation and differential GPS not supported
cc =	Check sum message, HEX 00...7F
	Check sum calculated by Xoring all bytes between $ and *.
CR =	Carriage Return
LF =	Line Feed

Example:

$GPGAA,151119.00,4307.0241,N,07729.2249,W,1,06,03.2,+00125.5,M,,,,*3F

The example data stream provides the following information:

Time of Position Fix:	15:11:19.00 UTC
Latitude:	43° 07.0241' North
Longitude:	77° 29.2249' West
Quality:	3D fix
Satellites Used:	6
Dilution of Precision:	3.2
Antenna Height:	+125.5 meters above sea level
Check Sum:	3

6.3 SW License Notices

This file is automatically generated from html/copyright.htm

Copyright Notice

[sheepb.jpg] "Clone me," says Dolly sheepishly

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 1992-2001                              *
*                                                                     *
* Permission to use, copy, modify, and distribute this software and  *
* its documentation for any purpose and 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.                                                          *
*                                                                     *
***********************************************************************
```

The following individuals contributed in part to the Network Time
Protocol Distribution Version 4 and are acknowledged as authors of
this work.

1. [1]Mark Andrews <marka@syd.dms.csiro.au> Leitch atomic clock
   controller
2. [2]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial
   line and PCI-bus devices
3. [3]Viraj Bais <vbais@mailman1.intel.com> and [4]Clayton Kirkwood
   <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
4. [5]Michael Barone <michael,barone@lmco.com> GPSVME fixes
5. [6]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
6. [7]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT
   port. Clean up recvbuf and iosignal code into separate modules.
7. [8]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
8. [9]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver,
   Trimble PARSE support
9. [10]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
10. [11]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
11. [12]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and
    help with target configuration
12. [13]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference
    clock driver, NT adj. residuals, integrated Greg's Winnt port.
13. [14]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
14. [15]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux
    port
15. [16]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for
    NTP Version 2 as specified in RFC-1119
16. [17]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
17. [18]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
18. [19]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
19. [20]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping
    overhaul
20. [21]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or
    [22]<H.Lambermont@chello.nl> ntpsweep
21. [23]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original
    author)
22. [24]Frank Kardel [25]<Frank.Kardel@informatik.uni-erlangen.de>
    PARSE <GENERIC> driver (14 reference clocks), STREAMS modules for
    PARSE, support scripts, syslog cleanup
23. [26]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX
    modifications, HPUX modifications
24. [27]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
25. [28]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox
    GPS clock driver
26. [29]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
27. [30]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
28. [31]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation
    code for Version 3 as specified in RFC-1305
29. [32]David L. Mills <mills@udel.edu> Version 4 foundation: clock
    discipline, authentication, precision kernel; clock drivers:
    Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics;
    audio clock drivers: CHU, WWV/H, IRIG
30. [33]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
31. [34]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
32. [35]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
33. [36]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
34. [37]Derek Mulcahy <derek@toybox.demon.co.uk> and [38]Damon
    Hart-Davis <d@hd.org> ARCRON MSF clock driver
35. [39]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de>
    monitoring/trap scripts, statistics file handling
36. [40]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
37. [41]Wilfredo Sánchez <wsanchez@apple.com> added support for
    NetInfo
38. [42]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
39. [43]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of
    space on the stuff in the html/pic/ subdirectory
40. [44]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
41. [45]Michael Shields <shields@tembel.org> USNO clock driver
42. [46]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock
    driver
43. [47]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure
    makeover, various other bits (see the ChangeLog)
44. [48]Kenneth Stone <ken@sdd.hp.com> HP-UX port
45. [49]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast
    support
46. [50]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock
    driver
47. [51]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic
    TrueTime clock driver
48. [52]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and

---

validated HTML documents according to the HTML DTD

---

[53]gif

[54]David L. Mills <mills@udel.edu>

References

1. mailto:marka@syd.dms.csiro.au
2. mailto:altmeier@atlsoft.de
3. mailto:vbais@mailman1.intel.co
4. mailto:kirkwood@striderfm.intel.com
5. mailto:michael.barone@lmco.com
6. mailto:karl@owl.HQ.ileaf.com
7. mailto:greg.brackley@bigfoot.com
8. mailto:Marc.Brett@westgeo.com
9. mailto:Piete.Brooks@cl.cam.ac.uk
10. mailto:reg@dwf.com
11. mailto:clift@ml.csiro.au
12. mailto:casey@csc.co.za
13. mailto:Sven_Dietrich@trimble.COM
14. mailto:dundas@salt.jpl.nasa.gov
15. mailto:duwe@immd4.informatik.uni-erlangen.de
16. mailto:dennis@mrbill.canet.ca
17. mailto:glenn@herald.usask.ca
18. mailto:iglesias@uci.edu
19. mailto:jagubox.gsfc.nasa.gov
20. mailto:jbj@chatham.usdesign.com
21. mailto:Hans.Lambermont@nl.origin-it.com
22. mailto:H.Lambermont@chello.nl
23. mailto:phk@FreeBSD.ORG
24. http://www4.informatik.uni-erlangen.de/~kardel
25. mailto:Frank.Kardel@informatik.uni-erlangen.de
26. mailto:jones@hermes.chpc.utexas.edu
27. mailto:dkatz@cisco.com
28. mailto:leres@ee.lbl.gov
29. mailto:lindholm@ucs.ubc.ca
30. mailto:louie@ni.umd.edu
31. mailto:thorinn@diku.dk
32. mailto:mills@udel.edu
33. mailto:moeller@gwdgv1.dnet.gwdg.de
34. mailto:mogul@pa.dec.com
35. mailto:tmoore@fievel.daytonoh.ncr.com
36. mailto:kamal@whence.com
37. mailto:derek@toybox.demon.co.uk
38. mailto:d@hd.org
39. mailto:Rainer.Pruy@informatik.uni-erlangen.de
40. mailto:dirce@zk3.dec.com
41. mailto:wsanchez@apple.com
42. mailto:mrapple@quack.kfu.com
43. mailto:jack@innovativeinternet.com
44. mailto:schnitz@unipress.com
45. mailto:shields@tembel.org
46. mailto:pebbles.jpl.nasa.gov
47. mailto:harlan@pfcs.com
48. mailto:ken@sdd.hp.com
49. mailto:ajit@ee.udel.edu
50. mailto:tsuruoka@nc.fukuoka-u.ac.jp
51. mailto:vixie@vix.com
52. mailto:Ulrich.Windl@rz.uni-regensburg.de
53. file://localhost/backroom/ntp-stable/html/index.htm
54. mailto:mills@udel.edu

This file is part of the OpenSSH software.

The licences which components of this software fall under are as
follows. First, we will summarize and say that all components
are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)
```
    * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
    *                    All rights reserved
    *
    * As far as I am concerned, the code I have written for this software
    * can be used freely for any purpose.  Any derived versions of this
    * software must be clearly marked as such, and if the derived work is
    * incompatible with the protocol description in the RFC file, it must be
    * called by a name other than "ssh" or "Secure Shell".
```

[Tatu continues]
```
    *  However, I am not implying to give any licenses to any patents or
    * copyrights held by third parties, and the software includes parts that
    * are not under my direct control.  As far as I know, all included
    * source code is used in accordance with the relevant license agreements
    * and can be used freely for any purpose (the GNU license being the most
    * restrictive); see below for details.
```

[However, none of that term is relevant at this point in time. All of
these restrictively licenced software components which he talks about
have been removed from OpenSSH, i.e.,

    - RSA is no longer included, found in the OpenSSL library
    - IDEA is no longer included, its use is deprecated
    - DES is now external, in the OpenSSL library
    - GMP is no longer used, and instead we call BN code from OpenSSL
    - Zlib is now external, in a library
    - The make-ssh-known-hosts script is no longer included
    - TSS has been removed
    - MD5 is now external, in the OpenSSL library
    - RC4 support has been replaced with ARC4 support from OpenSSL
    - Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this
software are publicly available on the Internet and at any major
bookstore, scientific library, and patent office worldwide. More
information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these

TTS200 Manual Rev C 93