SPECTRACOM

PUBLIC SAFETY | SECURITY | GOVERNMENT

MODEL 9183

NetClock/GPS Master Clock

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 9183-5000-0050
Manual Revision J
October 2006

Current to software version 2.3.0 (refer to 2.3.1 Addendum)

Specifications subject to change or improvement without notice.

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.

The Model 9183 is called an NTP time server as it provides disciplined timing using NTP (Network Time Protocol), and is also called a Master Clock as it meets or exceeds the NENA (National Emergency Numbers Association) master clock standard.

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 browser user interface-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 Windows 2003, 2000 and XP, 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.

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

- ☐ Unit
- ☐ User manual
- ☐ CE/UL-approved power supply for international use
- ☐ Standard DB9F to DB9M RS-232 cable pinned as straight thru (Used for initial configuration)
- ☐ AC power cord
- ☐ Rack-mount kit (2 ears, 4 side screws)
- ☐ Rubber footpads for desktop installation
- ☐ 3-pin terminal block connector for RS-485 connections
- ☐ 10-pin terminal block connector
- ☐ Jeweler's type screwdriver (For tightening the screws on the terminal blocks)
- ☐ Terminating Resistors, 120Ω

Spectracom models that have the modem dial-out feature (Option 3) enabled will also receive the following:

- ☐ Serial Modem kit
- ☐ Null modem adapter

1.4 Model 9183 Specifications

Note: The specifications listed are based on the NetClock operating in the "standard mode" of operation while tracking at least four qualified GPS satellites. Operating the NetClock with less than four qualified satellites will reduce the accuracies and capabilities of the unit.

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 Serial Setup Interface Port

Function:	Accepts commands to locally configure the IP network parameters for initial connectivity. Also used as the interface to the dial-out modem (Option 3).
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 / SNTP and remote monitoring, diagnostics, configuration and upgrade.

1.4.4 Protocols supported

NTP:	Networked NTP Stratum 1 Time Server (RFC 1305), SNTP (RFC 2030).
Security:	MD5 Security.
Loading:	~390 requests per second without encryption. ~340 requests per second with encryption.
Accuracy:	Output jitter within +/-50 microseconds of UTC typical.
Clients supported:	The number of users supported depends on the class of network and the subnet mask for the network. A gateway greatly increases the number of users.

HTTP, HTTPS Servers:	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:	Supports v1, v2c, and v3.
Telnet:	For limited remote configuration per RFC 854.
Security Features:	Up to 16-character Telnet password, Telnet Disable, FTP Disable, Secure SNMP, SNMP Disable, HTTPS, HTTP Disable, SCP 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 Data Formats 0, 1, 3 and 8. Data Formats 2, 4 and 7 within ±1 millisecond of UTC.
Configuration:	Baud rate and output Data Formats are selected using the web browser user interface. Bit rate selections are 1200, 2400, 4800 and 9600 baud. There are eight 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 in Data Formats 0, 1, 3 and 8. Data Formats 2, 4 and 7 within ±1 millisecond of UTC.
Configuration:	Baud rate and output Data Formats are selected using the web browser user interface. Bit rate selections are 1200, 2400, 4800, and 9600 baud. There are eight Data Format selections available.

1.4.7 Front Panel Display

Display Type:	Two separate Back-lit LCD displays.
Display Options:	Each display is configurable via the web browser user interface Interface. Choices consist of Time, Date, Day of Year, Software Versions, Fonts, and Date Formats.

1.4.8 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: Network activity.

1.4.9 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 available. Timer events that are hourly, daily or weekly only count as a single event so many events can be programmed.

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.

1.4.10 IRIG Output

Signal:	Selectable IRIG B or IRIG E, amplitude modulated sine wave (AM) or pulse-width-coded (TTL).
AM Carrier:	IRIG B-1000 Hz. IRIG E-100 Hz or 1000 Hz.
AM Signal Level:	Adjustable from 0 to 10 Vp-p mark amplitude into loads of 600 ohms or greater. Factory set to 2.0 V p-p.

Accuracy:	IRIG-B, IRIG-E 1000 Hz AM: ±20 microseconds of UTC. IRIG-E 100 Hz AM: ±200 microseconds of UTC. IRIG-B, IRIG-E TTL: ±2 microseconds of UTC.
Connector:	BNC female.
Configuration:	IRIG Formats B or E in AM or TTL levels. Time data is configurable with Time Zone Offsets and DST rules. Signature Control may also be placed on the output signal. This feature removes the modulation code from the IRIG output whenever the selected alarm condition is present. The output is restored when the fault is corrected.

1.4.11 1PPS Output

Signal:	One pulse-per-second square wave derived from the GPS receiver.
Signal Level:	TTL compatible into high impedance loads, 1.5 V base-to-peak into 50 ohms.
Pulse Width:	200 milliseconds.
Accuracy:	Positive edge within ± 500 nanoseconds of UTC when locked to GPS.
Connector:	BNC female.

1.4.12 Frequency output

Signal:	10 MHz sinewave.
Signal Level:	350mVrms into 50 ohms.
Harmonics:	Better than -30 dB down.
Spurious:	Better than -35 dB down.

Accuracy:

TCXO oscillator (Standard): $1x10^{-10}$ typical 24-hour average locked to GPS.

OCXO oscillator (Option 5): $1x10^{-11}$ typical 24-hour average locked to GPS, $2x10^{-9}$ per week typical aging unlocked.

Rubidium oscillator (Option 4): $1x10^{-12}$ typical 24-hour average locked to GPS, $1x10^{-11}$ per month typical aging unlocked.

Connector:	BNC female
Signature Control:	This configurable feature removes the output signal whenever a major alarm condition or loss of time sync condition is present. The output is restored when the fault condition is corrected.

1.4.13 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.
	The Spectracom P/N for the power supply is PS06-0E0J-DT01
DC input:	9.5 to 30 VDC, 10 watts, through a CE/UL/CSA-approved power adapter (supplied).
	Rubidium (Option 4) uses T00061, 24 VDC nominal (+22.5 - +30 VDC) @ 2.5 amps.
Connector:	Barrel, 5.5mm O.D., 2.5 mm I. D.
Polarity:	Negative shell, positive center.

1.4.14 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).
	The Rubidium option (Option 4) is 3.5” H (88mm) [2U] and 8 lbs (3.6 kg).
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

1.4.15 Agency Approvals

CE Mark:	EN60950, EN55022, EN55024
FCC:	Part 15
UL/CSA:	listed power adapter.

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

---

2 Installation

2.1 Installation Summary

This section provides an overview summary of the installation process. The installation of the NetClock Master Clock consists of the following steps:

1) If desirable - install the rack-mount ears on the two sides of the front panel and install the unit in a standard 19 inch rack cabinet.

2) Connect the DC power input jack to a standard AC outlet with the supplied power supply. (Refer to Section 2.3).

3) From the network administrator, obtain an available static network IP address, the network subnet mask and the IP address of the immediate gateway (if installed) if the subnet needs to be able to access the NetClock.

4) Assign the IP address, net mask and gateway settings by using the rear panel Serial Setup Interface DB9F connector interfaced to a PC with the provided serial cable (PC should be running either Microsoft HyperTerminal or ProComm). (Refer to Section 3.1).

5) Connect the NetClock's front panel Ethernet port to an available hub/switch on the network with a standard network cable. Verify the green Good Link lamp next to the Ethernet connector illuminates.

6) Install the GPS antenna, surge suppressor, antenna cabling and preamplifier if required. Refer to Section 2.4.
   A. If using a window-mount antenna (Model 8228), place the antenna in a window that has no metallic tinting or screening in or on the glass and then place the unit in single-satellite mode. (Refer to section 3.6.1).

Note: Use of a window-mount antenna with a Model 9183 NetClock is not recommended if using an OCXO (Option 5) or Rubidium (Option 4) type oscillator in the NetClock.

7) Connect the GPS cable to the rear panel antenna input jack on the back of the NetClock.

8) Verify the NetClock front panel Sync lamp turns green within about 20 minutes.

9) If supplied with Option 3 Dial-out Modem, connect the dial-out modem to the rear panel Setup port. Change the console/modem mode of operation to Modem and power cycle. (Refer to Section 8.1).

10) Configure the NetClock front panel LCD's as desired. (Refer to Section 3.5).

11) Interface the NetClock to wall display clocks and other peripheral devices as needed.

12) Configure each of the rear panel outputs to these devices for desired local times, baud rates and Data Formats using either the web browser user interface user interface or the Serial Setup Port (Each port is separately configured so each port used may need to be configured for your desired configuration). (Refer to Section 3.7 for web browser user interface or Section 7 for Serial Setup Interface port configuration). (Refer to Table 2-1 for information regarding local time).

13) Synchronize the network PC's via NTP using the Ethernet port as desired. (Refer to the Support dropdown page at www.spectracomcorp.com for assistance). (Refer to Table 2-1 for information regarding local time).

14) Review your security configuration settings (refer to Section 3).

Data Output	Port available from	Time Zone Offset for local time	Automatic Daylight Saving Time adjustment capable	Additional Notes
Network Time Protocol (NTP)	Ethernet port on front panel	NOT AVAILABLE	NO	NTP is always UTC. Must set Local time/DST correction on each PC via the Date/Time properties window.
Data Format 0	Remote/Serial on rear panel	00-23 Hours	YES	None
Data Format 1	Remote/Serial on rear panel	+/-12:00	YES	None
Data Format 2	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 2 always reflects UTC. It can't be configured as local time.
Data Format 3	Remote/Serial on rear panel	+/-12:00	YES	None
Data Format 4	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 4 always reflects UTC. It can't be configured as local time.
Data Format 5	Remote/Serial on rear panel	+/-12:00	YES	None
Data Format 7	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 7 always reflects UTC. It can't be configured as local time.
Data Format 8	Remote/Serial on rear panel	00-23 Hours	YES	None
Data Format 90	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 90 always reflects UTC. It can't be configured as local time.
IRIG B	IRIG port on rear panel	+/-12:00	YES	None
IRIG E	IRIG port on rear panel	+/-12:00	YES	None

Table 2-1: Time Zone Offsets available for Data Outputs

2.2 Required Tools and cables

1) Phillips screwdriver to install the unit's rack-mount ears.

2) Screwdriver to mount the unit in a standard 19-inch rack.

3) Wire strippers for the RS-485 cabling.

4) Supplied jeweler's type screwdriver for tightening the RS-485 wiring terminal block connectors (Located in the ancillary kit).

5) RS-232 straight-thru DB9 to DB9 cable (supplied)

6) Ethernet cables (Refer to Section 2.5).

2.3 Power and Ground Connection

An external AC to DC power adapter powers the NetClock.

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

Rack-mount ears are provided in the ancillary kit if the NetClock will be installed in a standard 19 inch rack.

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.

2.4 GPS Antenna Installation

2.4.1 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.

2.4.2 Cable Lengths

Using Spectracom CAL7xxx or Times Microwave LMR-400 coax, the maximum antenna cable length permitted is 200 feet because the Model 9183 allows 12 dB of 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. Refer to Figure 2-1for recommended cable lengths.

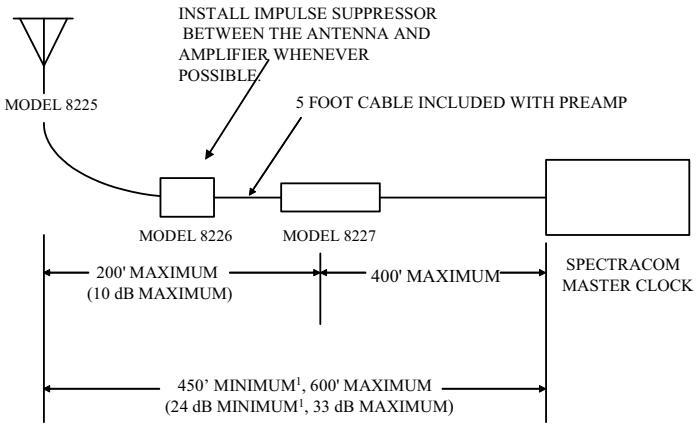


Figure 2-1: Cabling recommendations

2.4.3 Model 8224 GPS splitter

The GPS Antenna Splitter, Model 8224 is designed for use with an existing antenna/cable setup. It eliminates the need and expense for a second antenna/cable run when two synchronization systems are desirable. The Model 8224 should be installed indoors.

2.4.4 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.

Two LMR-400 field-installable N type connectors are provided with the Model 8226 to splice in the surge suppressor wherever it needs to be placed. However, the recommended method to avoid having to cut the antenna cable is to determine the desired location of the Model 8226 ahead of time and then order two lengths of pre-terminated cables instead of just one long cable that spans the entire distance between the antenna and the Master Clock.

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.

Spectracom offers a grounding kit that includes grounding cable, clamps, mounting bracket and ground plane. The Spectracom Part Number for this kit is 8226-0002-0600. Contact our Sales department for additional information.

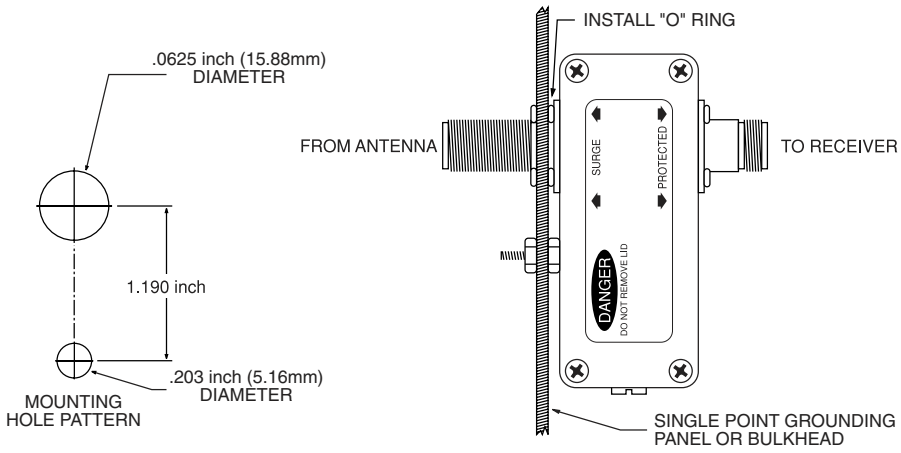


Figure 2-2: Model 8226 Impulse Suppressor

Refer to the Model 8226 Manual for proper installation.

2.4.5 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, extends the maximum cable length to 600 feet. The Model 8227 provides 20 dB of gain and is powered by the NetClock receiver.

Figure 2-3: Model 8227 Inline Amplifier

Two LMR-400 field-installable N type connectors are provided with the Model 8227 to splice in the amplifier wherever it needs to be placed. However, the recommended method to avoid having to cut the antenna cable is to determine the desired location of the Model 8227 ahead of time and then order two lengths of pre-terminated cables instead of just one long cable that spans the entire distance between the antenna and the Master Clock.

A five foot N type connector cable is also supplied with the Model 8227 to allow it to be installed after the Model 8226 surge suppressor . The Model 8227 should always be installed after the surge suppressor to prevent lightning or surge damage to the preamp.
Refer to the Model 8227 Manual for proper installation.

2.5 Ethernet Network Cabling

Spectracom NetClock Master Clocks provide a 10/100 Ethernet port for full NTP functionality as well as full web browser user interface 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.

2.5.1 Optional CNC3000 cable kit:

Spectracom offers an available cable kit called the CNC3000. This kit consists of three cables:

1) Six foot RS-232 Setup port cable DB9M to DB8F for initial configuration

1) Six foot Cat 5 crossover LAN cable for direct PC connection

1) Six foot Cat 5 patch LAN cable for LAN hub link.

Contact our Sales department if you would like to obtain the CNC3000 kit.

2.6 Remote port and Serial comm port output pin-outs and wiring

This section contains wiring and pin-out information for the rear panel Remote RS-485 and Serial RS-232 Comm ports.

2.6.1 Serial Comm ports

The rear panel of the Model 9183 has two RS-232 SERIAL COMM ports that are available to synchronize peripheral devices. These ports can provide RS-232 output data to synchronize external devices that can accept RS-232 Data Formats as an input. The available Data Formats are listed in Section 6.

The Serial ports can provide RS-232 data in one of two modes. The Interrogation mode provides a one-time RS-232 time stamp each time that the port receives a request character from the external device. In between the requests for time, there is no output. The Multicast mode broadcasts the time stamp every second. The Interrogation mode is the factory default. This mode should be changed to Multicast mode in the web browser user interface if the external device being synchronized does not send a request character for the time but rather just "listens" for the time to be sent every second.

The configuration of the data, including the baud rate, the Data Format, the request character in the Interrogation mode, Time Zone Offsets and Daylight Saving Time rules is chosen from the web browser user interface. Refer to Section 3.7 for information regarding port configuration.

The SERIAL COMM ports have a standard RS-232 pin configuration as shown in Figure 2-4 and Table 2-2.

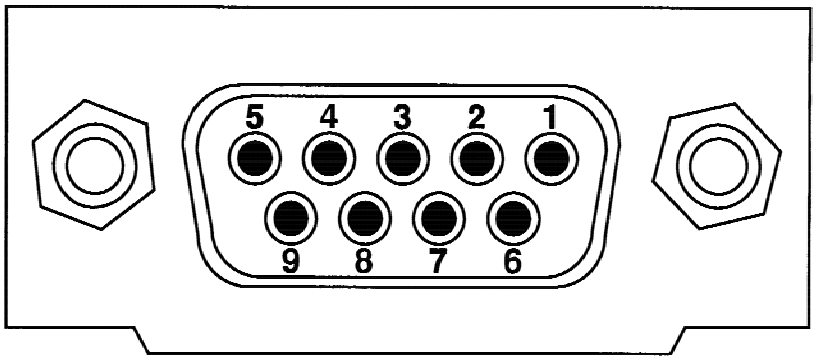


Figure 2-4: Serial port connector

PIN	SIGNAL	I/O	DESCRIPTION
2	RXD	O	Receive Data (RS-232 output data to a device)
3	TXD	I	Transmit Data (RS-232 input data from a device)
5	GND	-	Signal Common
6	DSR	O	Data Set Ready
7	RTS	*	Request to Send
8	CTS	*	Clear to Send

Table 2-2: Serial Port Pin Assignments

2.6.2 RS-485 Remote port

The NetClock has two Remote Connections labeled "RS-485 PORT 1" and "RS-485 PORT 2". 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 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 3.7 for configuring these outputs.

A 3-position terminal block is supplied in the ancillary kit for each of the Remote Connections. Also included in the ancillary kit is a jeweler's type screwdriver to tighten the screws. Connector pin assignments are shown in Figure 2-5.

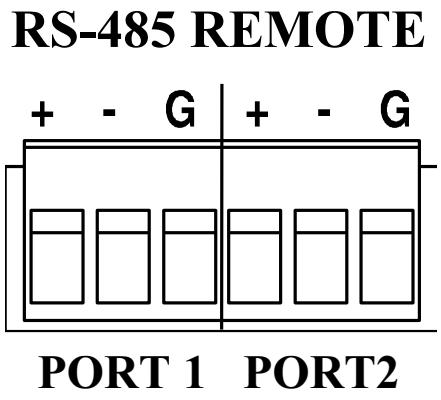


Figure 2-5: Remote Outputs

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 2-6 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.

Error! Objects cannot be created from editing field codes.
Figure 2-6: 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, Ethernet Time Servers, and radio link products to meet various time applications and requirements. For information on Remote Output usage refer to Section 2.6.2.

2.6.3 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, Ethernet Time Servers, RS-485 to RS-232 converters and radio link products that utilize the RS-485 data stream as an input.

Figure 2-7 and Figure 2-8 illustrate typical RS-485 time data bus interconnections. Follow the guidelines listed below when constructing the RS-485 data bus.

2.6.4 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 2-3 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 2-3: 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 2-4 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 2-4: Cable Sources for RS-485 Lines Under 1500 Feet

2.6.5 Connection Method

The RS-485 transmission line must be connected in a daisy chain configuration as shown in Figure 2-7: 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.

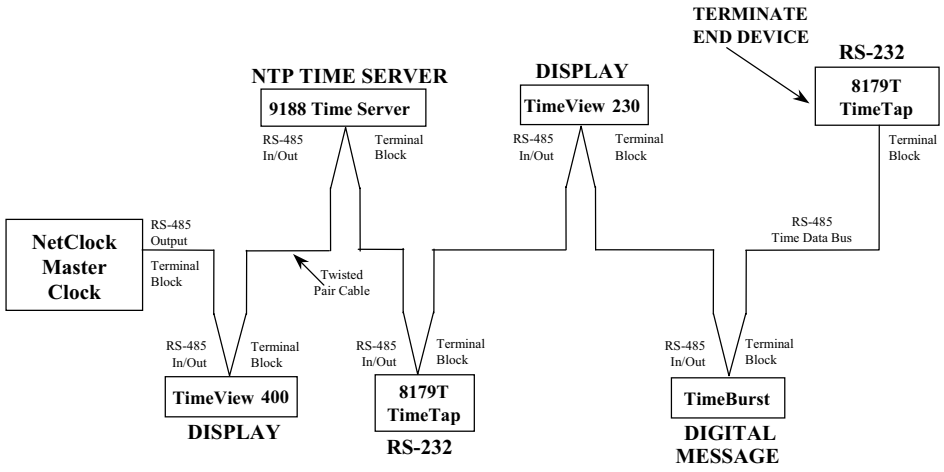


Figure 2-7: One-Way Bus Installation

The RS-485 Output can be split in a total of two directions as shown in Figure 2-8. This allows the NetClock to be centrally located. Connecting in this method can simplify installation and possibly reduce the amount of cable required.

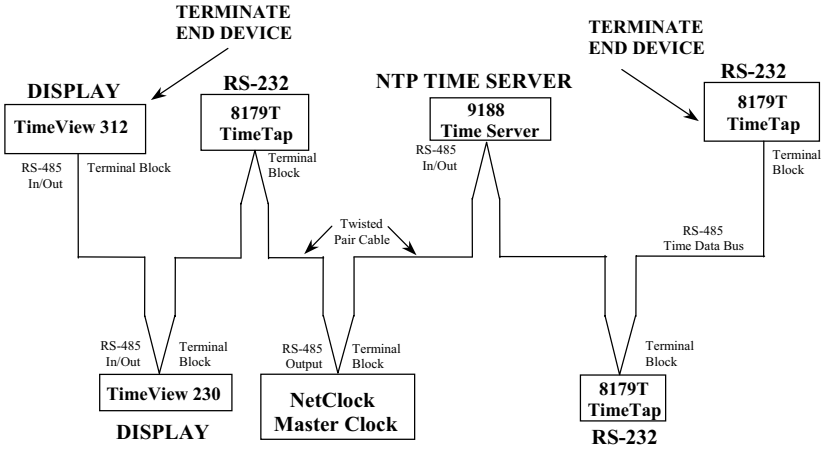


Figure 2-8: Split Bus Configuration

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 2-9. Wrapping the wires in this manner prevents smaller gauge wires from breaking off when exposed to handling or movement.

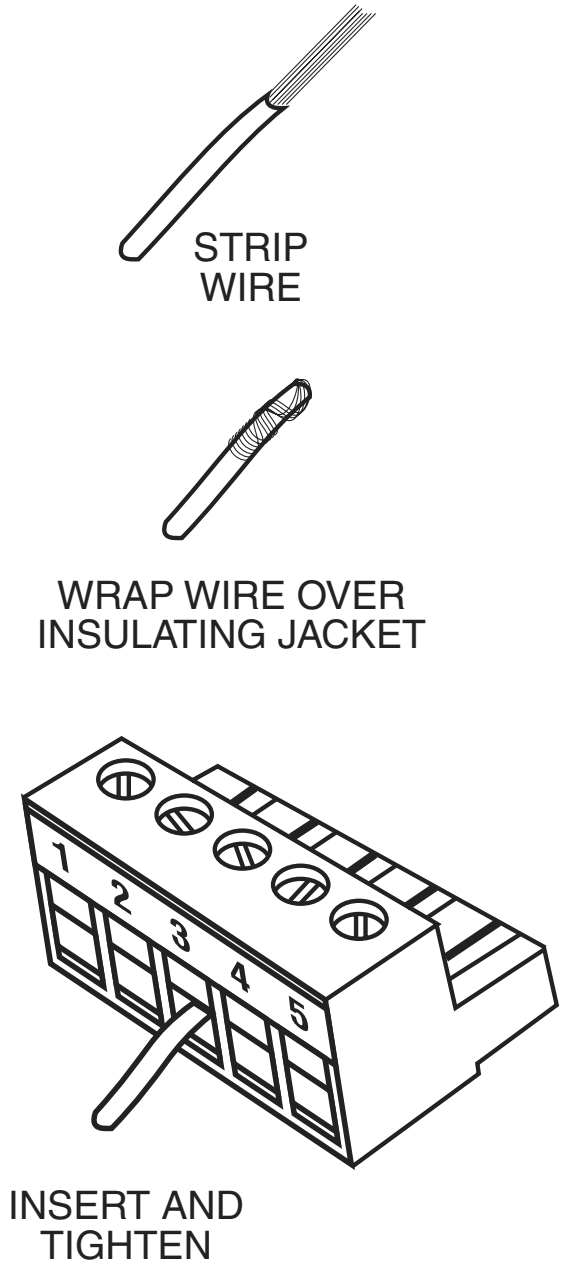


Figure 2-9: Wire Strain Relief

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 2-10. The TimeView display clocks accept only Data Formats 0 or 1.

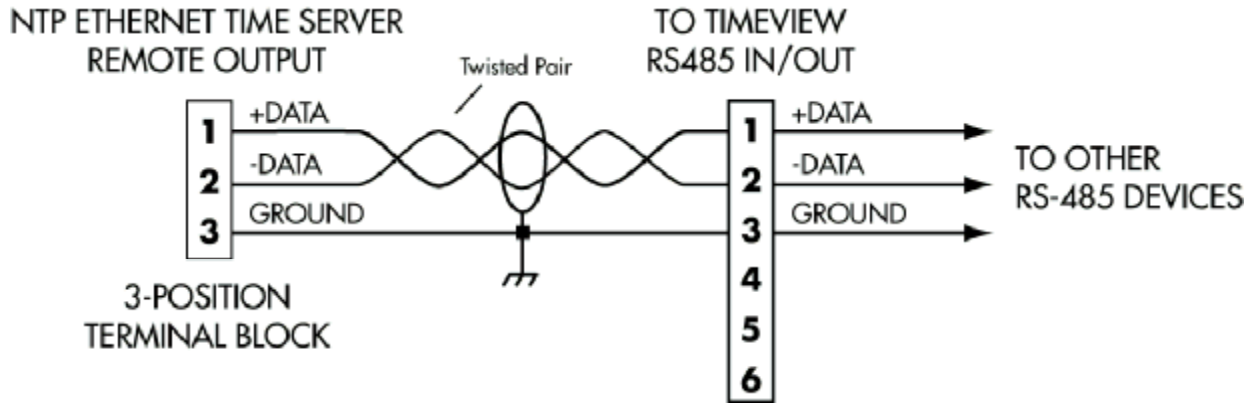


Figure 2-10: TimeView RS-485 Interface

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 2-11.

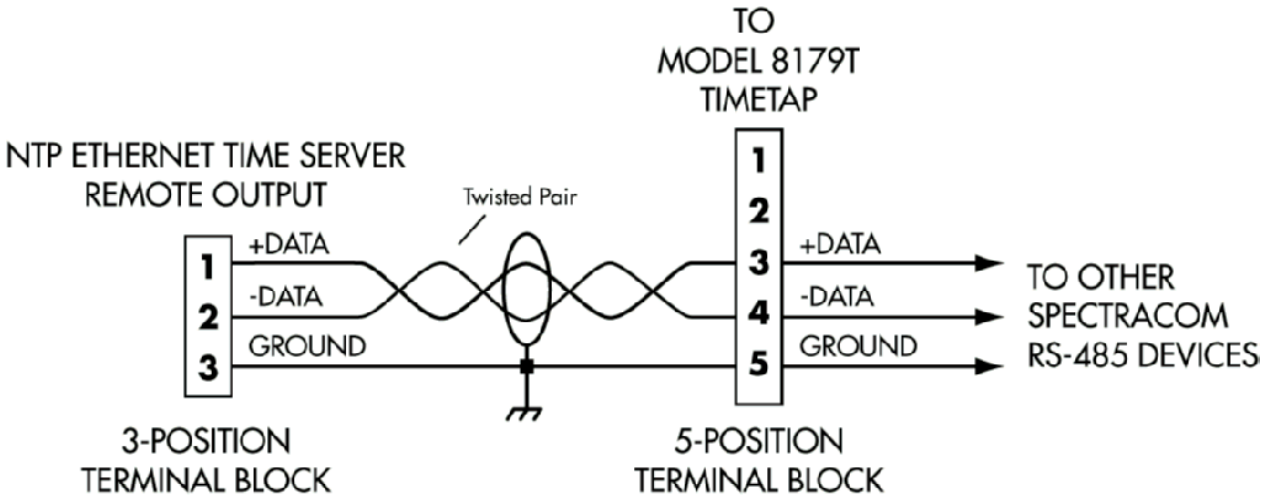


Figure 2-11: Model 8179T TimeTap RS-485 Interface

Spectracom Model 9188 is an Ethernet Time Server that supports NTP and SNTP time protocols. The Model 9188 accepts Format 0, Format 2 or Format 8 (Format 8 is not available on all Model 9188's- contact Tech Support for additional information) and connects to the RS-485 data bus through a three-position terminal block. Connect the Model 9188 to the NetClock as shown in Figure 2-12.

.

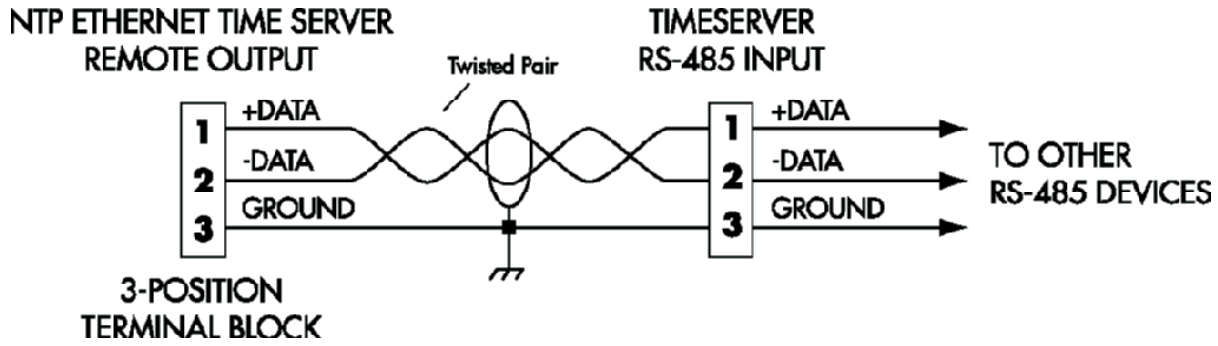


Figure 2-12: Model 9188 RS-485 Interface

The Model 8185, TimeBurst™, provides a digital time-of-day data burst to a radio transmitter. The TimeBurst accepts Data Format 0 or 1. Connect the TimeBurst to the RS-485 data bus using a 3-position terminal block as shown in Figure 2-13.

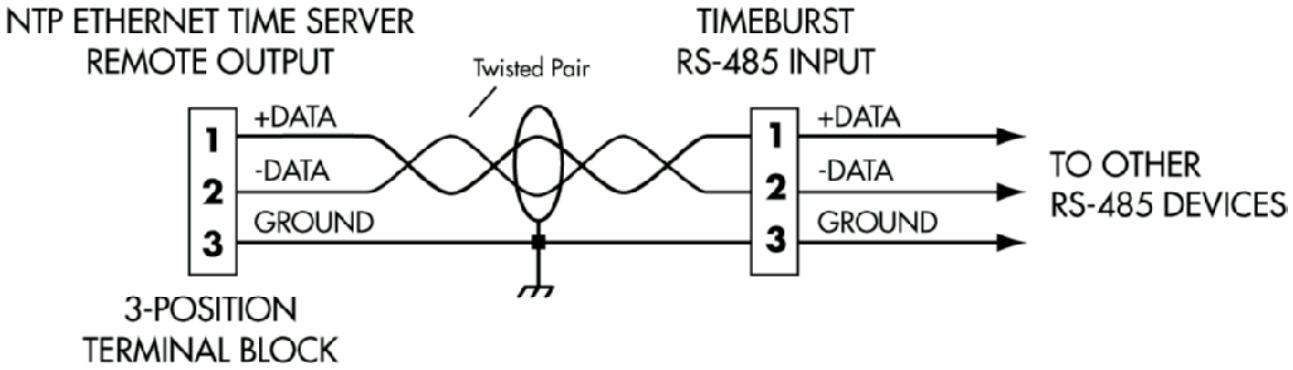


Figure 2-13: TimeBurst RS-485 Interface

2.6.6 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 2-7), terminate the last device on the bus. The RS-485 data bus can be split in two directions as shown in Figure 2-8. 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 or a resistor is supplied with the equipment if no termination switch is available.

3 Product Configuration

3.1 Network Configuration

The product has a 10/100 Mbps Ethernet port, which can be used to connect the unit to a network. The NetClock's network settings will need to be initially configured via the rear panel setup port or with a direct connect to a stand-alone PC (such as a laptop). These settings can thereafter be modified through either the serial port or web browser user interface as desired. 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 static 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. (For security reasons HTTP should be disabled when HTTPS is the desired connection method to the web browser user interface).

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

Before the NetClock can provide NTP time stamps to synchronize the network as well as access to the web browser user interface Server for configuration and logs can be obtained, the IP address of the NetClock has to be changed from the factory default to the new static address for your particular network.

The IP address and subnet values can be changed using either the rear panel setup port with a serial cable and a terminal emulator program (recommended) OR they can be changed using a PC's network interface card (NIC) connected directly to the front panel Ethernet port with a network cross-over cable. The PC will need to be configured in Network Settings with the IP address of 10.10.200.x (Where x is any number from 2 to 254) and a subnet mask of 255.255.255.000.

3.1.1 To configure the product to work on a network via the Serial Setup port

Connect the serial comm port of your PC to the 9-pin Serial Set-up Interface connector. The pin-outs for this connector are shown below.

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. If you have any difficulty with either the terminal emulator program or communicating with the port, refer to the HyperTerminal Application Note at:
http://www.spectracomcorp.com/support/applicationNotes.php.

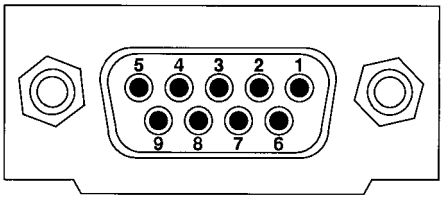


Figure 3-1: Serial Setup Interface port connector

PIN	SIGNAL	I/O	DESCRIPTION
2	RXD	O	Receive Data (RS-232 output data to PC)
3	TXD	I	Transmit Data (RS-232 input data from PC)
5	GND	-	Signal Common
6	DSR	O	Data Set Ready
7	RTS	*	Request to Send
8	CTS	*	Clear to Send

Table 3-1: Serial Setup port pin-outs

3.1.2 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. Config mode provides limited configuration privileges and admin provides full configuration privileges.

To Login with administrator-level permissions with the 'login' command:

1) If "**Spectracom login:**" is not currently displayed, press the <enter> key.
2) The unit will respond with "**Spectracom login:"**
3) After Spectracom login:" type: **admin** <enter>
(**Note**: User logins and passwords are case sensitive).
4) The unit will respond with "**Password:**"
Type **admin123** <enter>
(**Note**: For security reasons, the unit will not show what you type).
6) The unit will then display "**welcome to the Command Line Interface**" followed by a "**>**"
(Known as the Command prompt).

Note: For config mode login, replace the phrase of admin with the phrase of **config** and replace the password phrase of admin123 with the phrase of **config12**.

At the command prompt (>), perform the following to configure the network settings:

3.1.2.1 To display or configure the IP address:

To display the current IP address, type **net ip** <enter> (factory default is 10.10.200.1)
To change the IP address to the desired IP address, type **net ip xxx.xxx.xxx.xxx** <enter> (where x is the desired address).

3.1.2.2 To display or configure the Net Mask:

To display the current subnet mask, type **net mask** <enter> (factory default is 255.255.255.0)
To change the current subnet to the desired subnet mask, type **net mask xxx.xxx.xxx.xxx** <enter> (where x is the desired subnet mask).

3.1.2.3 To display or configure the Gateway settings:

To display the current gateway configuration, type **net gateway** <enter> (factory default is disabled).
To enable the gateway, type **net gateway yes xxx.xxx.xxx.xxx** <enter> (where x is the immediate network gateway's IP address).

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.

To disable the gateway, type **net gateway no** <enter>

3.1.2.4 To display the current network configuration

To display the entire current network configuration, type **net show** <enter>

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.

Connect to the serial port of the unit.

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

Type **net ip 10.10.200.5 <enter>** to set the IP address.

Type **net mask 255.255.255.128** <enter> to set the subnet mask.

Type **net gateway no** <enter> to disable the gateway feature.

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.

To configure the product to work on a network via web browser user interface:
Connect a PC to the Ethernet port using a network cross-over cable. In Windows "network settings" configure the PC with a static address of 10.10.200.x (Where x is any number between 2 an 254) and a subnet mask of 255.255.255.0. Then, connect to the web browser user 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 URL 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 Section 1.1for instructions on web browser user 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:

Connect to the web browser user interface of the product.

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

Enter ‘10’, ‘10’, ‘200’, and ‘5’ in the corresponding IP Address fields.

Select ‘255.255.254.0’ from the Subnet Mask pull-down menu.

Choose the Gateway “Enabled” radio button.

Enter ‘10’, ‘10’, ‘200’, and ‘10’ in the corresponding Gateway Address fields.

Choose the Telnet “Disabled” radio button.

Choose the FTP “Enabled” radio button.

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

Note: If changing the IP address of the NetClock to a different subnet, when you hit submit, the NetClock will immediately start using the new IP address. This will cause the web browser user interface to stop responding. Move the NetClock to the network and you should then be able to re-access the web browser user interface with any networked PC by using the new IP address.

3.1.3 Default and Recommended Configurations

The factory default configuration settings were chosen for ease of initial setup. Refer to the recommended settings listed here as applicable for your unit. The web browser user interface and the command line interface allow "Admin" users with full function read/write privileges (such as setting up the unit's network settings) and "Config" users possessing a subset of Admin privileges (such as no access to network settings, but access to the front panel clock setup).

Configuration	Default	Recommended	Where Enabled
HTTP	Enabled	Disabled	Web User Interface or Command Line Interface
HTTPS	Enabled – Using customer-generated certificate and key or default Spectracom self-signed certificate and common public/private key SSH/SCP/SFTP enabled with unit unique 1024 bit keys		Web User Interface
SNMP	Disabled	Disabled or Enabled with: – SNMP v3 w/ encryption* and –Host IPs identified for host restriction	Web User Interface
NTP	Enabled – With no MD5 Values Entered	Enabled – Use MD5 authentication with user-defined keys	Web User Interface
Command Line Interface			
Console Port	Available – Unless dial-out modem connected (uses this port)	Available	Not Applicable
Telnet	Enabled	Disabled – Use SSH instead	Web User Interface
SSH	Enabled (default keys provided)	Enabled	Web User Interface
File Transfer			
FTP	Enabled	Disabled – Use SFTP or SCP	Web User Interface
SCP	Available	Available	Not Applicable
SFTP	Available	Available	Not Applicable

Table 3-2: Default and Recommended Configurations

*We recommend secure clients use *only* SNMPv3 with authentication for secure installations.

3.2 Login

The default mode for the web browser user interface is Read only. Any user can view the unit's configuration and status logs without the ability to make changes to the configuration. There are two available login modes that require the user to know a login password:

Configuration Mode allows non-critical system changes.
Administrator Mode allows full control over all parameters. This mode should only be used by advanced users. Changes made while in this mode may be detrimental to the proper operation of the NetClock.

Note: Only one user is allowed into the web browser user interface at a time. If you try to access the web browser user interface with someone else already in the browser, a screen will display the IP address of the computer that is currently accessing the browser.

Refer to Figure 3-2 for a sample list of the login permission requirements. This list is also displayed on the web browser user interface screen under the login mode buttons.

Note: For security reasons, the Admin and Config mode login lasts for 15 minutes or until the NetClock is rebooted (Whichever occurs first). You will be exited out of the login after 15 minutes as the connections reset every 15 minutes.

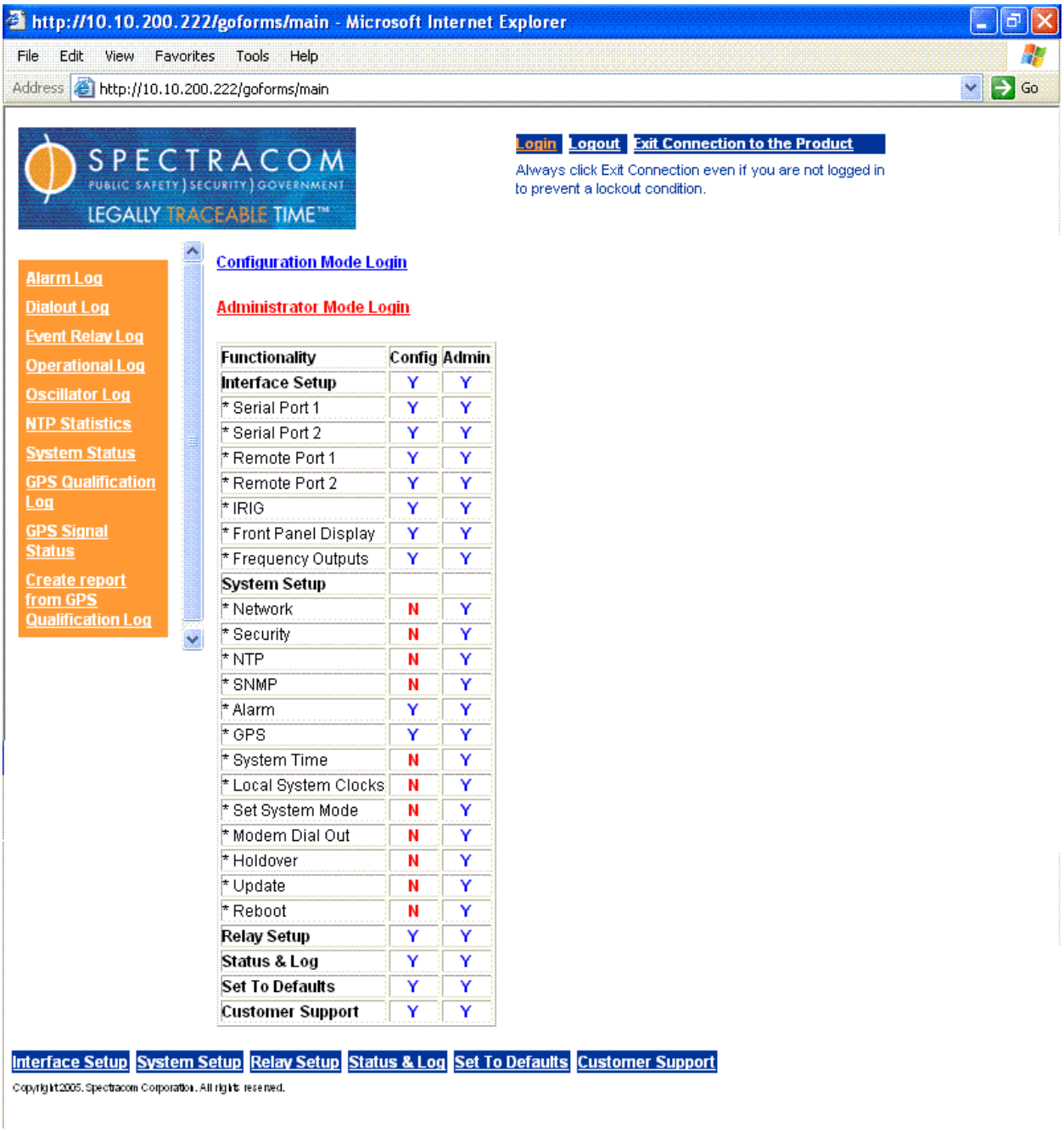


Figure 3-2: Log-in Permissions

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.

Chose the “administrator mode” to login as admin mode or chose “configuration mode” to login as the config mode. Figures 3.1-2 and 3.1-3 display the appropriate login screen for the desired login mode. Type the password for the mode selected. Note that the password is capital-letter sensitive.

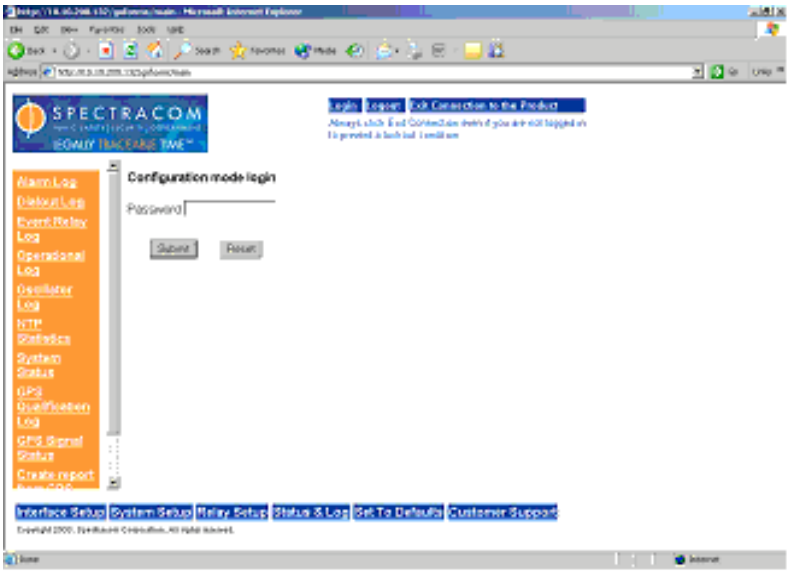


Figure 3-3: Configuration mode Log-in

Figure 3-4: Administrator mode Log-in

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

Default Passwords
The default access passwords for the *Configuration* and *Administrator Modes* are:

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

For security reasons, we recommend you change the passwords and don't lose them! If the passwords are written down, they should be stored in a secure location such as a safe for later retrieval by authorized personnel.

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

3.2.1 To Change the Default Login Password Values

For security reasons, the account passwords cannot be changed using either the web browser user interface 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:

To change the admin password, type:
sec password admin <enter>

To change the config password, type:
sec password config <enter>

The unit will then ask you to type in the old password and then to type the new password (twice).

Example:

Type:	sec password <enter>
Response:	Account:
Type:	[current account name] <enter>
Response:	Old Password:
Type:	[current password for this account] <enter>
Response:	New Password:
Type:	[New password for this account] <enter>
Response:	New Password (again):
Type:	[New password for this account] <enter>
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 user interface when you are finished viewing the NetClock 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.

3.2.2 To reset the current Login Password Values back to the factory default values

Once the config and admin passwords have been changed from their default factory values, the passwords can always be changed again in the future to new desire values as long as the current passwords are still known (Refer to Section 3.1.4). However, the changed passwords may not be known by the current user so the procedure to change the passwords described in section 3.1.4 will not be available.

If the current admin level password is unknown, both of the config and admin level passwords can be reset to the factory defaults and then changed to the desired passwords. Perform the following to reset the passwords back to the factory defaults to allow the passwords to be edited.

Connect to the Serial Setup Interface with a standard straight-thru serial cable and a PC running HyperTerminal or Procomm (As described in Section 3.1.1).

With "**Spectracom Login:"** displayed, type **defaults** <enter> (If the login prompt is not displayed, hit the enter key).

When the NetClock prompts for "**Password**:" just hit the enter key (Don't enter a password).

The unit will respond with "**passwords reset**". The admin password is now set back to **admin123** and the config password is now set back to **config12**.

Using these current password values, follow the procedure in Section 3.2.1 to change these passwords to the desired values.

3.3 Alarms

3.3.1 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.

3.3.1.1 System Status displayed on a web browser user interface

Dynamic system information including the current state of the alarms and time sync status 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".

3.3.2 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 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 (Standard) or OCXO (Option 5) time base oscillator requires an adjustment to maintain operation within specifications. This is a **Minor** alarm.

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 interface:

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.

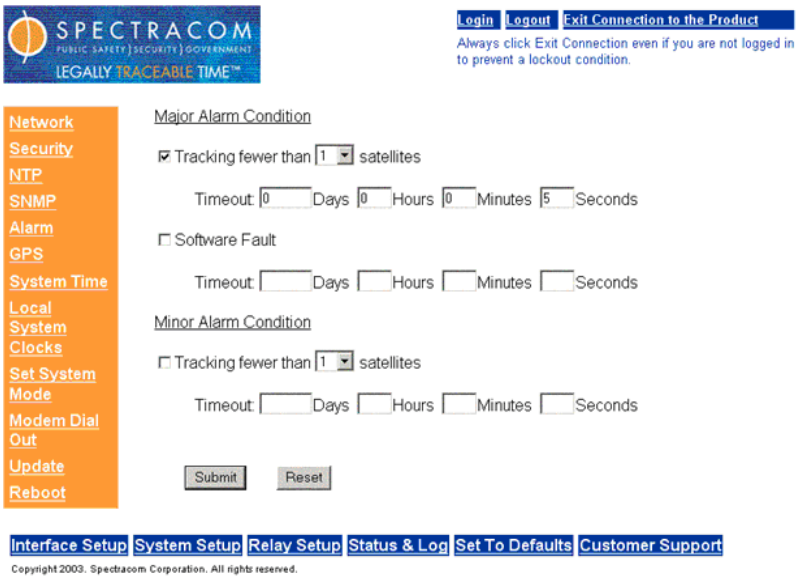


Figure 3-5: Alarm Setup Screen

User-defined alarms are configured using the Alarm Setup screen (Figure 3-5) from the web browser user interface. 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.

3.4 Event Timer

3.4.1 Configuring the Event Timer

The web browser user 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 3.13.1 for details on relay configuration).

To configure the events:
Connect to the web browser user 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.

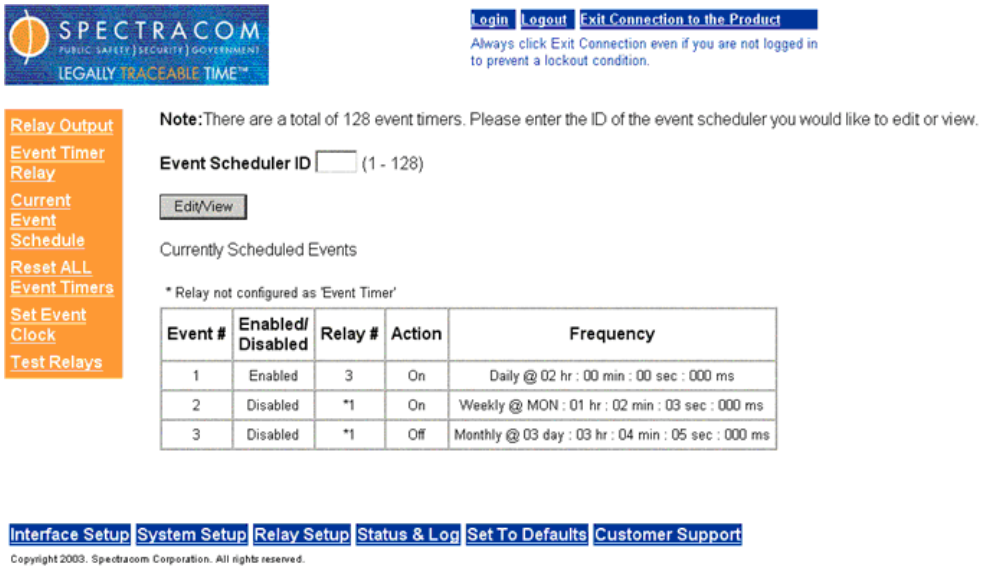


Figure 3-6: Event Timer Relay Screen

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 3.5 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.

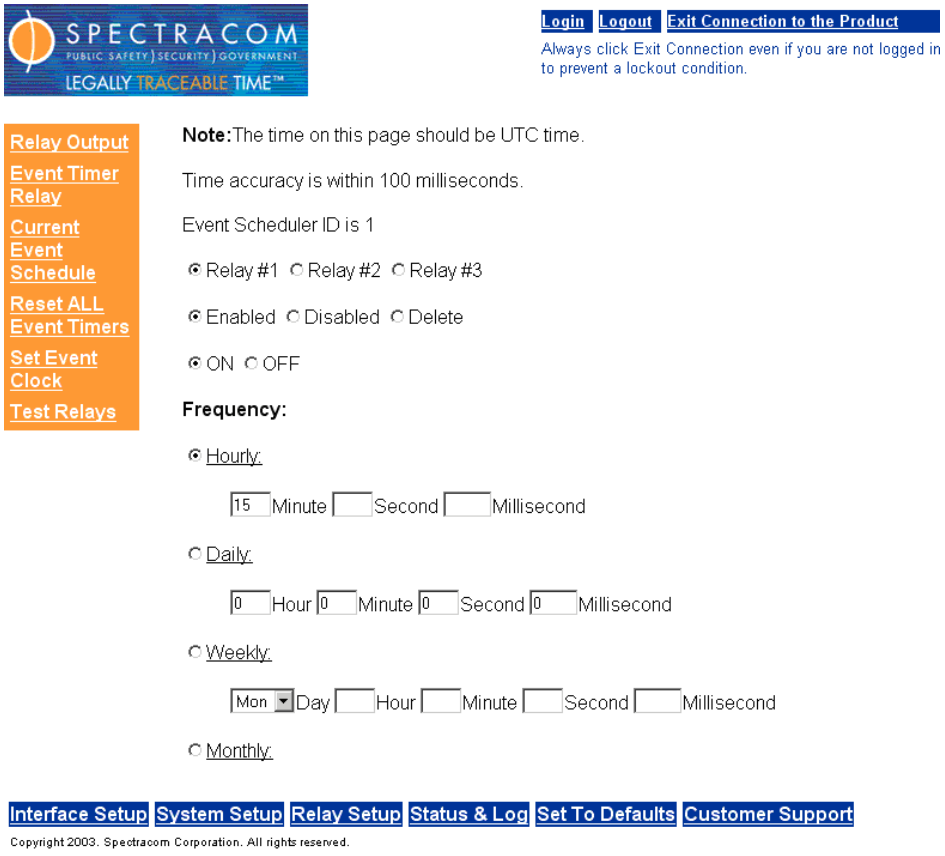


Figure 3-7: Event Timer Relay Screen

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 1st 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 browser user 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.

3.5 Front Panel Display

The NetClock has two front panel LCD displays. Both of these front panel displays are separately configurable. This section explains how to configure the optional front panel displays.

Using the web browser user interface to configure the Front Panel Display:

You can change the Front Panel Display formats to suit your needs. Both of the displays are independently programmable. The left side display is LCD 1, the right side is LCD 2.

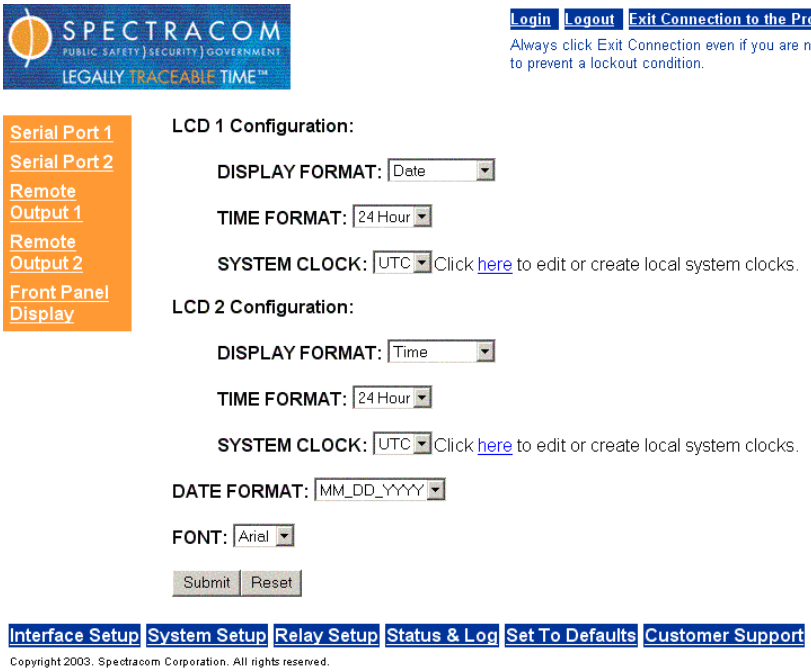


Figure 3-8: Front Panel Display Screen

LCD # Display Format:
Each of the two LCD Displays has a user selectable Display Format. This display format defines the type of information provided the user. The following is description of the nine available display options:

None - No Display is shown, LCD is blank.
Product - Product Name, Hardware Revision and Firmware Revision is shown for several seconds after which the default display is resumed.
Revision - Firmware Revision of Data Port outputs is shown for several seconds after which the default display is resumed.
Time View - Time is displayed with Large Font for Hours:Minutes and Small Font for Seconds.
Time - Time is displayed in Large Font for Hours:Minutes:Seconds.

Day of Year - Day of Year (DOY) is displayed in Large Font.
Date - Date is displayed in a user selectable format in a Large Font.
Date-Time - Date and Time are displayed in a Small Font. Date is displayed in the user selected format.
DOY-Time - Day of Year and Time are displayed in a Small Font.

LCD1 Display Format Setup:
This field allows the user to select the Display Formats described above to be used for this LCD screen.

LCD2 Display Format Setup:
This field allows the user to select the Display Format described to be used for this LCD screen.

Date Format Setup:
This field allows the user to select the Date Format. The available choices are as follows (Where YY=Year, MM=Month, DD=Day):
MM_DD_YY, DD_MM_YY, YY_MM_DD, MM_DD_YYYY, DD_MM_YYYY, YYYY_MM_DD

Time Format Setup:
This field allows the user to select 12 Hour or 24 Hour time format.

Font Setup:
This field allows the user to select one of the supported Fonts for the Numeric display fields for Date, Time and Day of Year. The available choices are as follows:
Arial - Arial style font (This is the factory default)
Mark - Curved, strong font
LED - LED Style rectangular thick font
Thin - LED Style rectangular thin font

System Clock Setup:
This field allows the user to manually select which Time Zone Offset to use when displaying time. See Section 3.5 on Local System Clocks.

Note: When selecting a System Clock for time to be displayed on one LCD display and date on the other LCD display, use the same System Clock selection in both LCD displays (If setting the time to local time, change the date to local time as well). Otherwise the "new day" time and "new date" rollover may not coincide with each other. (One will occur at a different time than the other).

To configure a product's Front Panel Display via web browser user interface:

Connect to the web browser user 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 “Front Panel Display” 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.

Example 1: To configure the Front Panel Display to show Day of Year and Time View displays using an Arial font while displaying 12 Hour, Local time.

Connect to the web browser user interface of the unit.
Login to configuration- or administrator-level mode and browse to the Front Panel Display page.
Select 'Day of Year' from the LCD1 Display Format pull-down menu.
Select 'Time View' from the LCD2 Display Format pull-down menu.
Select '12 Hour' from the Time Format pull-down menu.
Select ‘Arial’ from the Font pull-down menu.
Select the Time Zone by selecting the appropriate System Clock in the pull-down menu.
Review the changes made and click Submit. The browser will display the status of the change.

3.6 GPS

This section contains information on configuring the GPS receiver.

How to set up the GPS receiver:
Using the web browser user interface, 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.

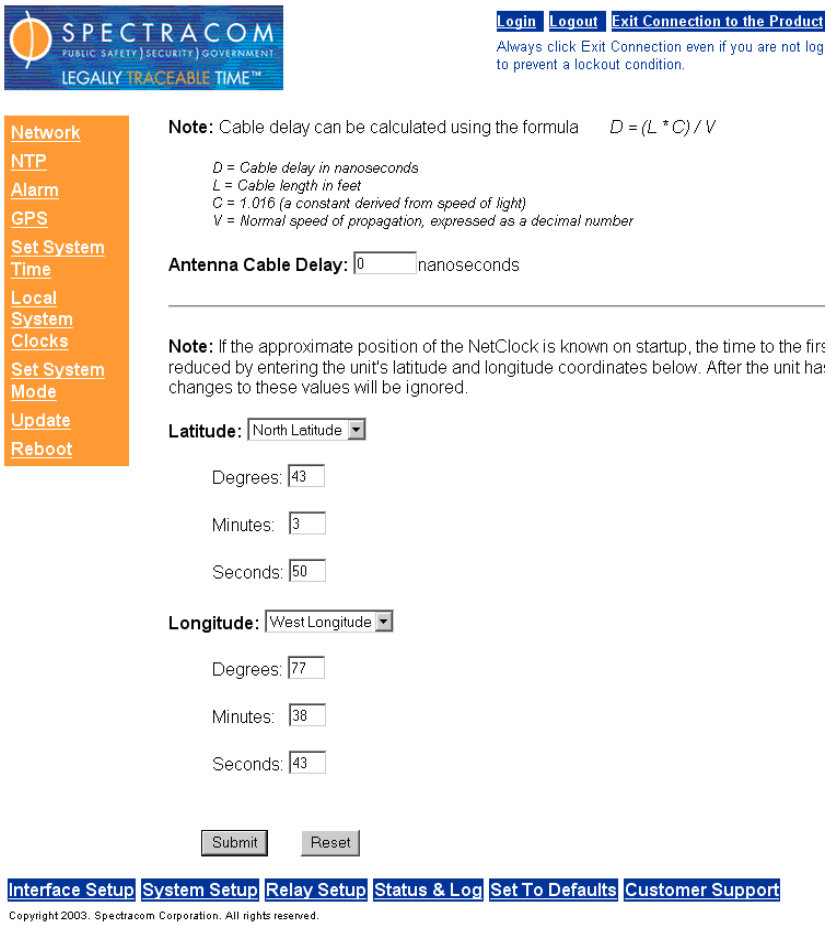


Figure 3-9: GPS Set-up Screen

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 nanoseconds, 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.

Note: The antenna cable is delay is nominal and beyond the accuracy specs of the GPS receiver. The antenna cable delay does not normally need to be set.

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 shown 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.

3.6.1 Set System Mode

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

Use single satellite mode if you are using a window mount antenna and cannot receive at least four satellites. This will switch the qualification algorithm used, and allow the system to operate with a fewer number of satellites, but the accuracy and capabilities of the optional Rubidium (Option 4) and OCXO (Option 5) oscillators will be decreased because of the poor GPS antenna visibility.

Caution: Single Satellite mode compromises the accuracy of the NetClock and the full capabilities of the optional OCXO and Rubidium oscillators. Always use standard mode if you are using a roof mount antenna and can get at least four satellites. This is the factory default.

To set the System Mode using the web browser user interface:
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).
Press the "Enter Main Page" button.
Select the login link on the top right corner to login as administrator.
On the lower menu line select the "System Setup" item.
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.

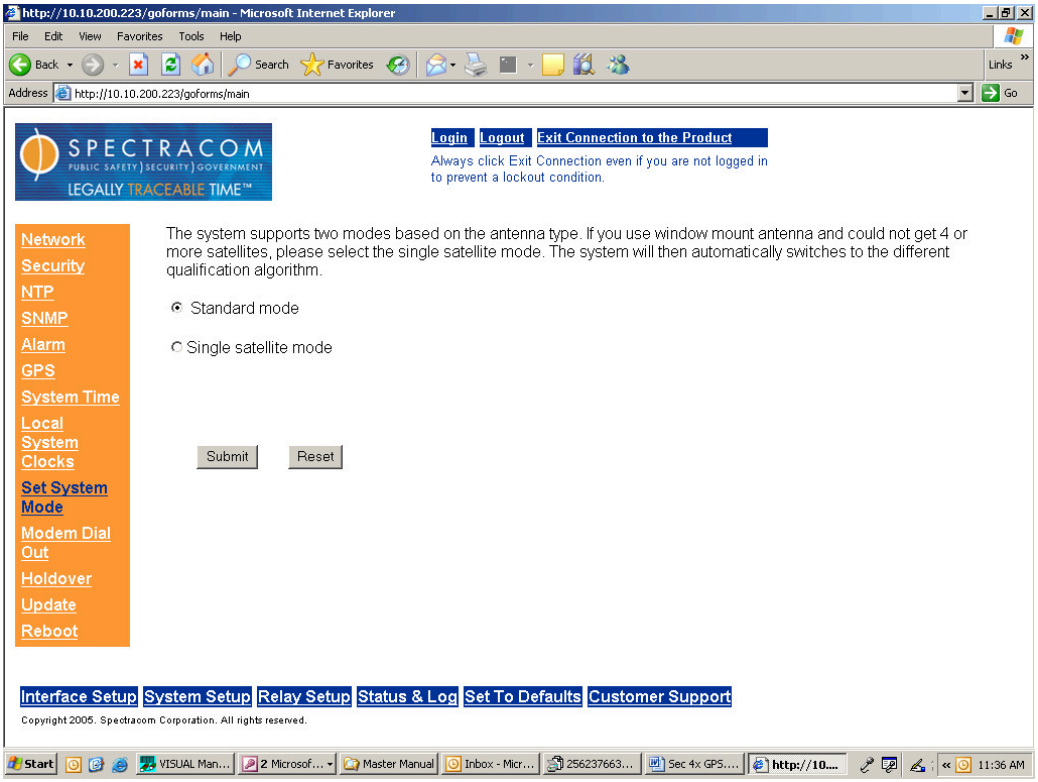


Figure 3-10: Set System Mode

3.6.2 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.

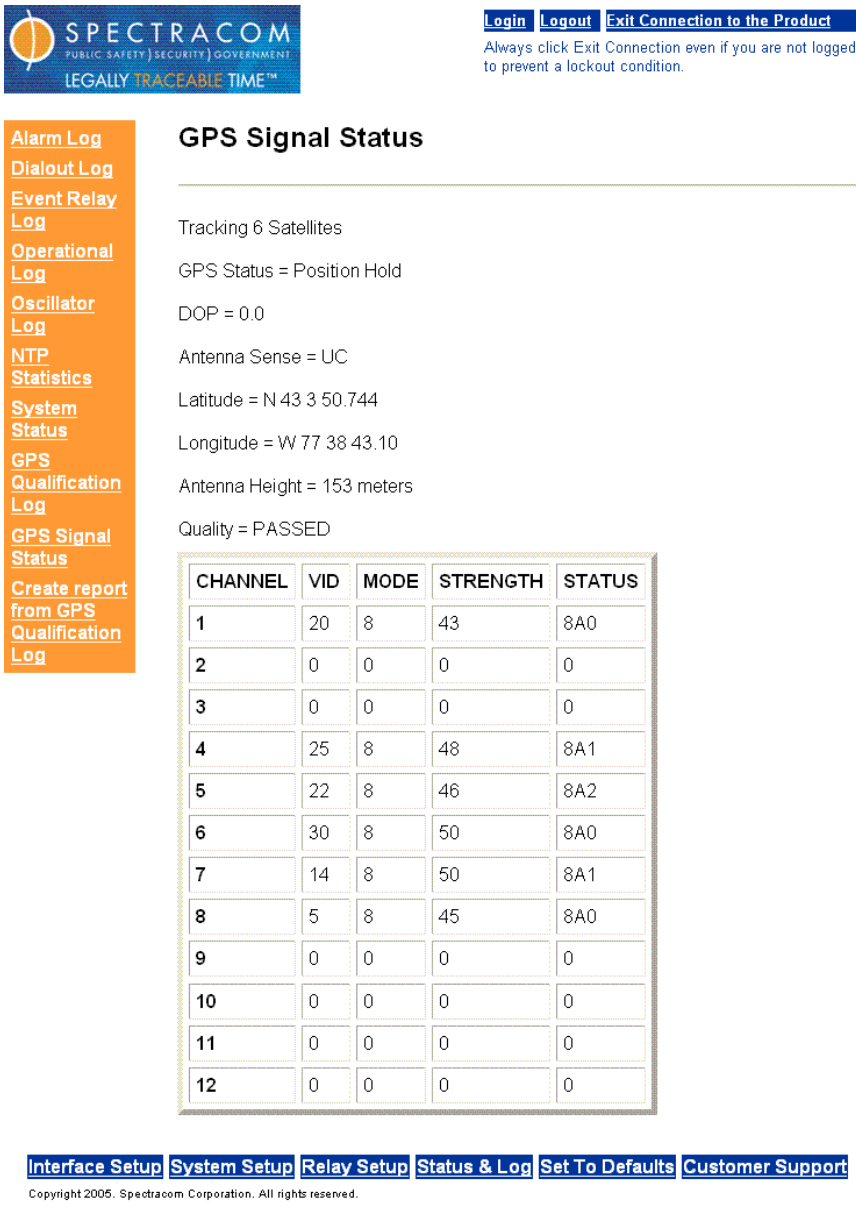


Figure 3-11: GPS Signal Status Setup Screen

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

Note: This condition will also be present if a GPS antenna splitter that does not contain a load to simulate an antenna being present is being used.

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 of at least 4 that are available for Position Fix Usage while in the normal mode of operation (Or at least 1 satellite that is available for position fix when the unit is single satellite mode).

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

Note: For assistance with GPS reception issues, refer to Section 0.

3.7 Interface Setup

This section contains information on configuring the Remote and Serial ports.
To verify operation of either of the two Serial ports, refer to Section 0.

3.7.1 Configuration parameters for the Remote and Serial Interfaces

The NetClock has two RS-232 ports (also called Serial Ports) and two RS-485 ports (also called Remote Output Ports) that support independent output of date/time stamps. The web browser user 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 Data Format in which date/time stamps are outputted. Available Formats are 00, 01, 02, 03, 04, 07, 08 and 90; and are described in detail in the "Data Format" section 6 . Format 00 is the default.

Note: Because Data Format 2 is ALWAYS a UTC output, it cannot have a Time Zone Offset or Daylight Saving Time rule enabled. Conversion to Local Time is accomplished by the device receiving Data Format 2. An error message will be generated if a Time Zone Offset or DST rule is attempted when selected to Data Format 2.

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'.

Change this setting to Multicast if the external device needs to receive the tine stamp every second (It does not send a request character to the Master Clock when it desires a time stamp).

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 3.5 Local Systems Clocks for more information on how to set these.

3.7.1.1 To configure a product's Interface via web browser user interface:

Connect to the web browser user interface after booting the unit. Login to either 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.

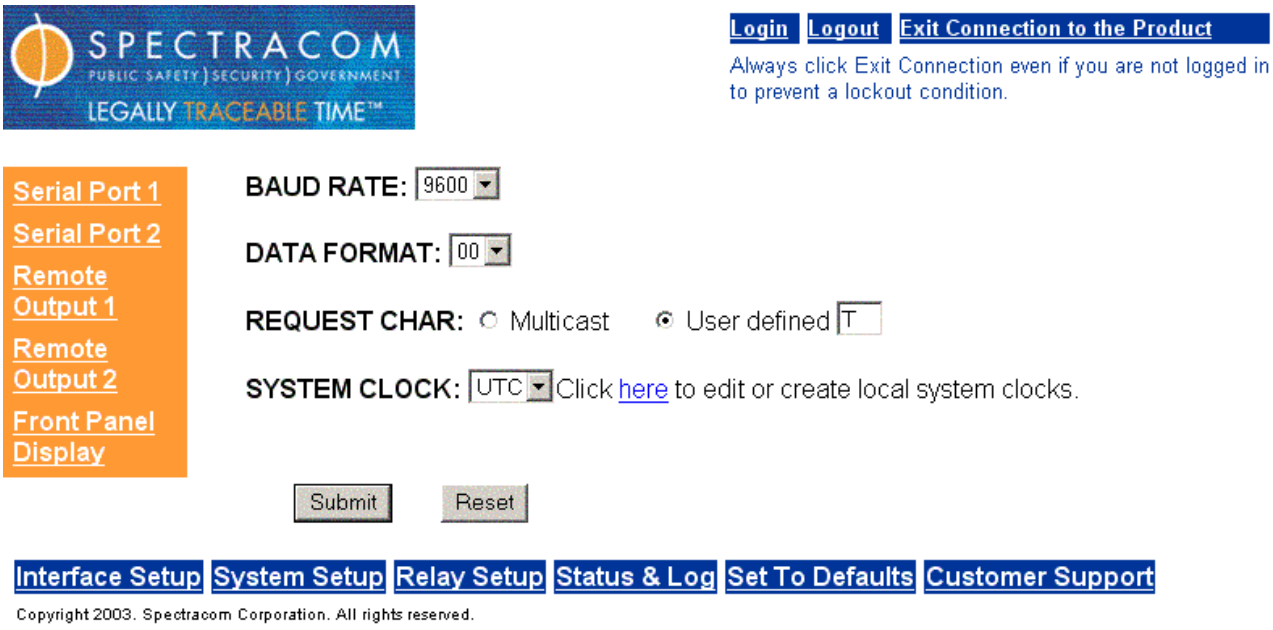


Figure 3-12: Interface Screen

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 browser user 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.

3.7.2 "Set To Defaults" web browser user interface

The "Set To Defaults" web browser user interface screen is used to return the Serial Port 1, Serial Port 2, Remote Port 1, Remote Port 2, Front Panel Displays, IRIG and the Frequency Outputs back to their product defaults. To return these configurations back to the factory defaults values, login as the administrator mode, select "set to defaults" on the bottom blue bar, and the press the "Restore to factory defaults" button.

Figure 3-13: Restore Interface setup back to factory defaults

3.8 IRIG Port

IRIG is an acronym for Inter-Range Instrumentation Group. In the late 1950's this group created a series of time code standards suitable for use with recording oscillographs, magnetic tape and real time transmission. Each IRIG code specifies a carrier frequency that is modulated to encode date and time, as well as control bits to time stamp events. Initially, IRIG applications were primarily military and government associated. Today, IRIG is commonly used to synchronize voice loggers, recall recorders and sequential event loggers found in emergency dispatch centers and power utilities.

The NetClock is able to provide an IRIG B or IRIG E code in amplitude modulated (AM) or pulse width coded (TTL) formats. A signature control feature may be enabled for any IRIG output. Signature control removes the modulation code when a Time Sync Alarm is asserted. Refer to section 3.8.1 for a detailed description of the IRIG B Format and section 3.8.2 for a detailed description of the IRIG E Format.

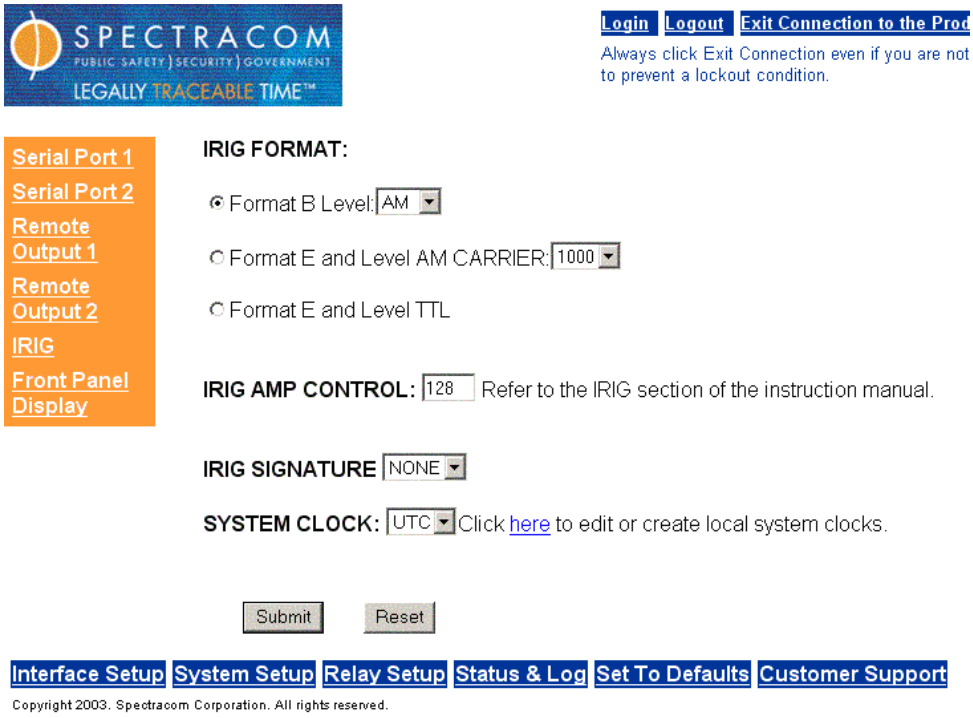


Figure 3-14: IRIG Screen

To configure a product's IRIG Port via web browser user interface:

Connect to the web browser user interface after booting the unit.

Login to configuration- or administrator-level mode if changes are desired.

Choose "Interface Setup" from the bottom frame, and “IRIG” from the left frame.

IRIG configuration options include: Format, Amplitude Control, Signature Control, Time Zone, and DST corrections.

Format: choose the format, level and carrier desired.

Amplitude Control: the peak-to-peak output voltage level into a 600 ohm load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The table below shows typical output levels for digital control values from 0 – 255.

Note: These values are only nominal and may vary from unit to unit. To precisely adjust the level, connect an oscilloscope to the output connector when adjusting.

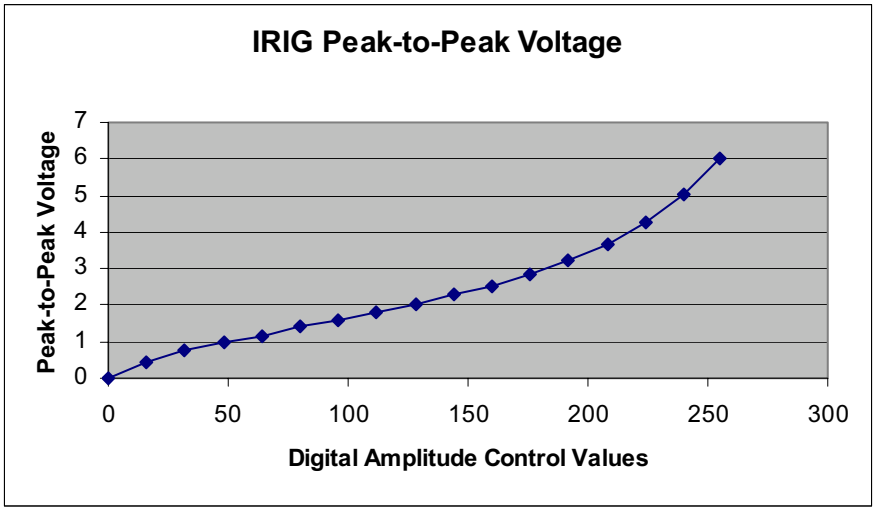


Figure 3-15: IRIG Output Level

Signature Control: when set to Sync, the modulation is removed when the Time Sync Alarm is asserted. When set to None, the modulation will be present even if the Time Sync Alarm is asserted.

Time Zone Setup:
This field allows the user to manually select which time zone to use when displaying time. 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.

.

3.8.1 IRIG B Output

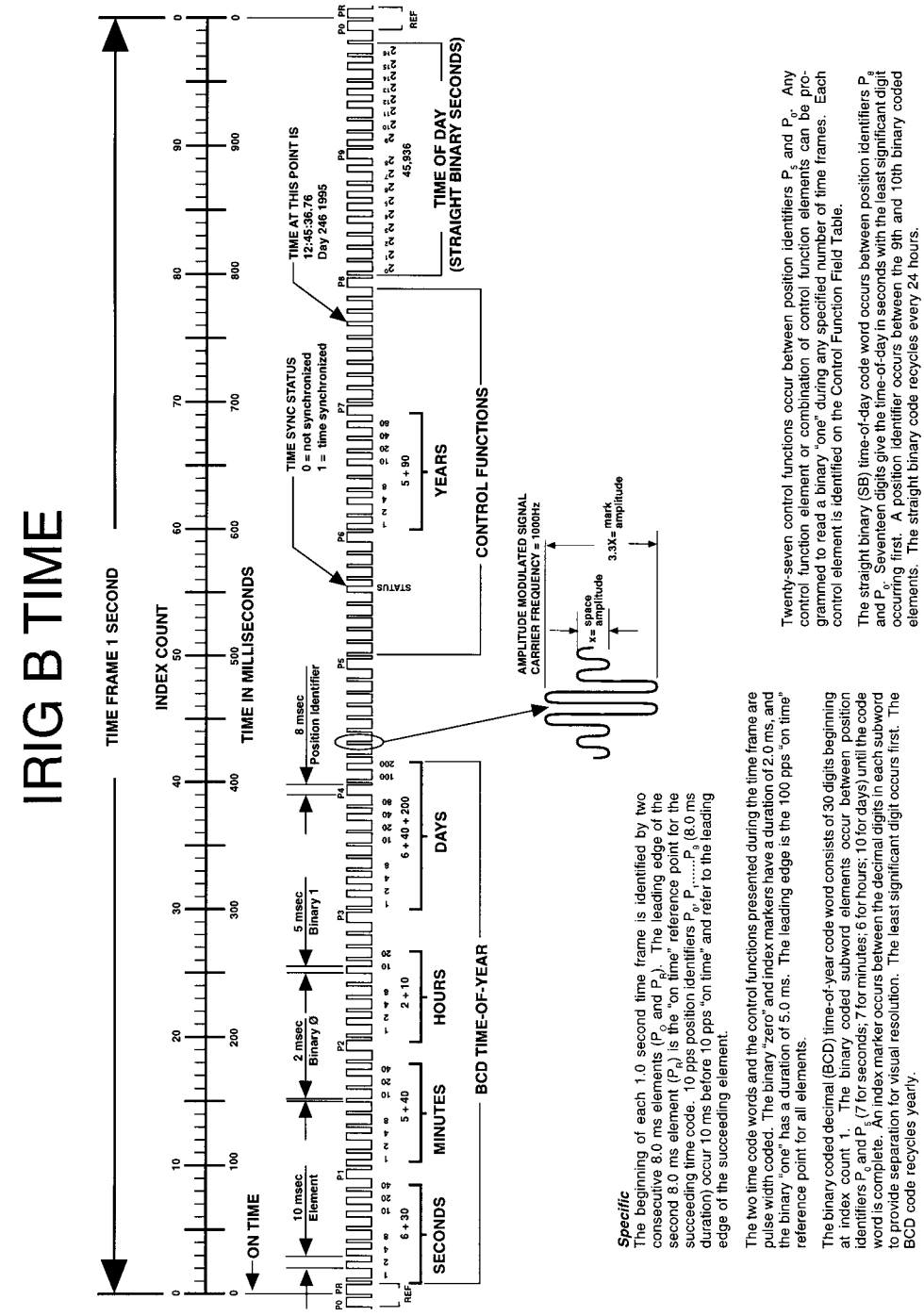


Figure 3-16: IRIG B Time Code description

The IRIG B code contains the Binary Coded Decimal (BCD) time of year, Control Function (CF) field and the Straight Binary Seconds time of day. The following figure illustrates the IRIG B data structure. The BCD time of year provides the day of the year, 1-366, and the time of day including seconds. The hour of the day is expressed in 24 hour format. The SBS time is the number of seconds elapsed since midnight. The Control Function field contains year information and a time sync status bit.

1. Time frame: 1.0 seconds.
2. Code digit weighting:
    A. Binary Coded Decimal time-of-year.
    Code word - 30 binary digits.
    Seconds, minutes hours, and days.
    Recycles yearly.

    B. Straight Binary Seconds time-of-day.
    Code word - 17 binary digits.
    Seconds only, recycles daily.
3. Code word structure:

BCD: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P_0 and P_5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

CF: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The NetClock uses the Control Functions to encode year information and time sync status.

Table 3-3 below lists the Control Function Field and each element's function.

Element 55 is the time sync status bit. Element 55 is a Binary 1 when the front panel time sync lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 97, 98, 99 etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first. All unused Control Functions are filled with a space (Binary 0).

SBS: Word begins at index count 80. Seventeen Straight Binary Coded elements occur with a position identifier between the 9th and 10th binary coded elements. Least significant digit occurs first.

4. Pulse rates:

Element rate: 100 per second.
Position identifier rate: 10 per second.
Reference marker rate: 1 per second.

5. Element identification: The "on time" reference point for all elements is the pulse leading edge.
Index marker (Binary 0 or uncoded element): 2 millisecond duration.
Code digit (Binary 1): 5 millisecond duration.
Position identifier: 8 millisecond duration.
Reference marker, 1 per second. The reference marker appears as two consecutive position identifiers. The second position identifier marks the on-time point for the succeeding code word.

6. Resolution:

Pulse width coded signal: 10 milliseconds.
Amplitude modulated signal: 1 millisecond.

7. Carrier frequency: 1 kHz when modulated.

ELEMENT #	C.F. DIGIT #	FUNCTION
50	1	Space
51	2	Space
52	3	Space
53	4	Space
54	5	Space
55	6	Time Sync Status
56	7	Space
57	8	Space
58	9	Space
59	PID P6	Position Identifier
60	10	Years Units Y1
61	11	Years Units Y2
62	12	Years Units Y4
63	13	Years Units Y8
64	14	Space
65	15	Years Tens Y10
66	16	Years Tens Y20
67	17	Years Tens Y40
68	18	Years Tens Y80
69	PID P7	Position Identifier
70	19	Space
71	20	Space
72	21	Space
73	22	Space
74	23	Space
75	24	Space
76	25	Space
77	26	Space
78	27	Space

Table 3-3: IRIG B Control Function Field

3.8.2 IRIG E Output

The IRIG E code contains the Binary Coded Decimal (BCD) time of year and Control Functions.

Figure 3-17 illustrates the IRIG E data structure. The BCD time of year provides the day of year, 1-366, and time of day to tens of seconds. The hour of the day is expressed in 24 hour format. The Control Function field includes a time sync status bit, year information and SBS time of day.

1. Time frame: 10 seconds.

2. Code Digit Weighting:
   Binary Coded Decimal time of year.
   Code world - 26 binary digits.
   Tens of seconds, minutes, hours, and days.
   Recycles yearly.

3. Code Word Structure: BCD word tens of seconds digits begin at index count 6. Binary coded elements occur between position identifier elements P_0 and P_5 (3 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

4. Control Functions: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG E has 45 Control Functions located between elements 50 and 98. The NetClock uses the Control Function field to encode year data, time sync status, and SBS time data. Table B-2 lists the Control Function Field and each element's function.

Element 55 is the time sync status bit. Element 55 is a Binary 1 when the front panel time sync lamp is green, and a Binary 0 when the lamp is red.

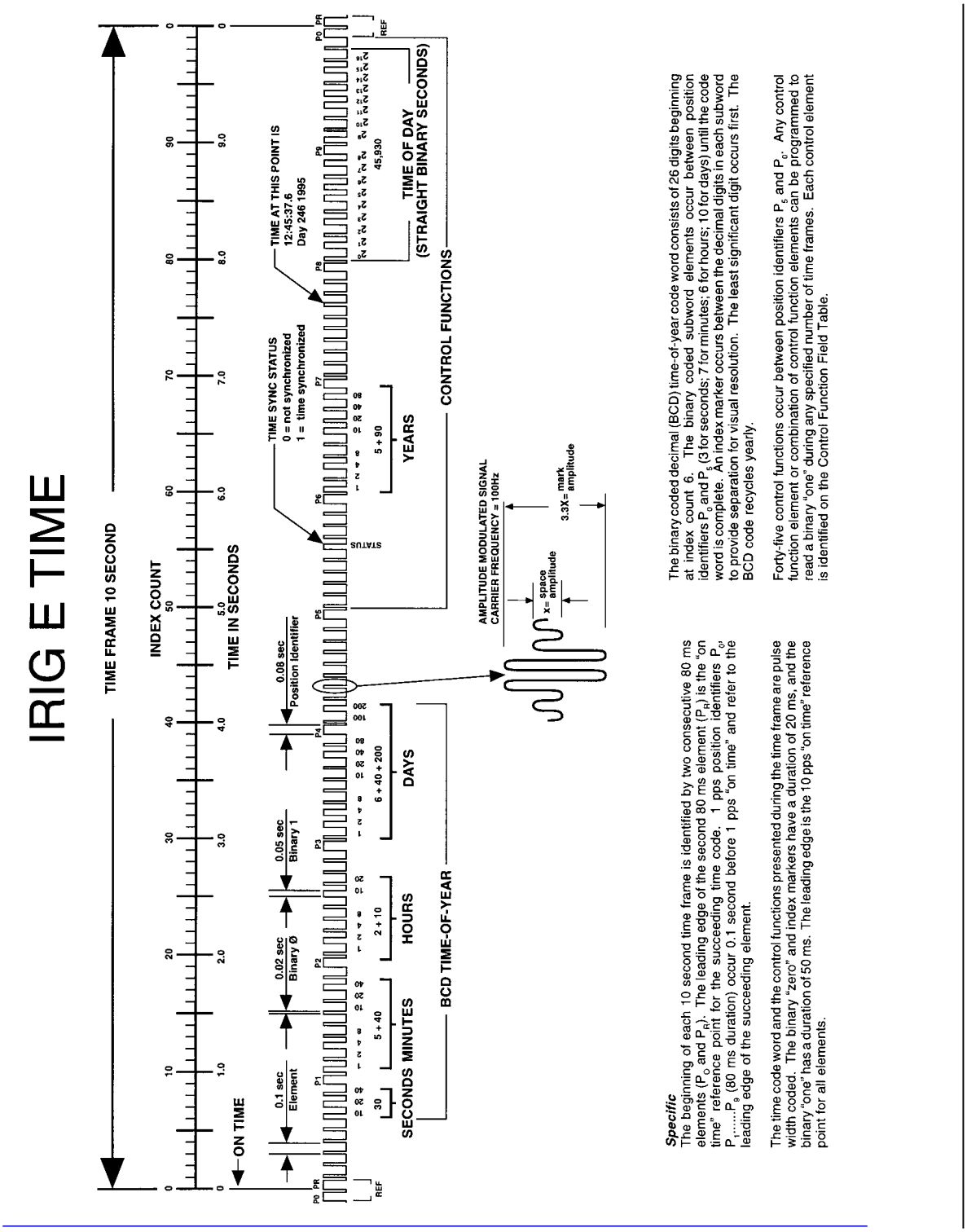
Year information consists of the last two digits of the current year (i.e. 98, 99, etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first.

Elements 80 through 97 are encoded with the Straight Binary Seconds (SBS) time data. The SBS time data is incremented in 10-second steps and recycles every 24 hours.

5. Pulse rates:
   A. Element rate: 10 per second.
   B. Position identifier rate: 1 per second.
   C. Reference marker rate: 1 per 10 seconds.

6. Element identification: The "on time" reference point for all elements is the pulse leading edge.
Index marker (Binary 0 or uncoded element): 20 millisecond duration.

Code digit (Binary 1): 50 millisecond duration.
Position identifier: 80 millisecond duration.
Reference marker: 80 millisecond duration, 1 per 10 seconds. The reference marker appears as two consecutive position identifiers. The second position identifier or reference marker is the on-time point for the succeeding code word.



Specific

The beginning of each 10 second time frame is identified by two consecutive 80 ms elements (P_0 and P_R). The leading edge of the second 80 ms element (P_R) is the "on time" reference point for the succeeding time code. 1 pps position identifiers P_0, P_1.....P_9 (80 ms duration) occur 0.1 second before 1 pps "on time" and refer to the leading edge of the succeeding element.

The time code word and the control functions presented during the time frame are pulse width coded. The binary "zero" and index markers have a duration of 20 ms, and the binary "one" has a duration of 50 ms. The leading edge is the 10 pps "on time" reference point for all elements.

The binary coded decimal (BCD) time-of-year code word consists of 26 digits beginning at index count 6. The binary coded subword elements occur between position identifiers P_0 and P_5 (3 for seconds; 7 for minutes; 6 for hours; 10 for days) until the code word is complete. An index marker occurs between the decimal digits in each subword to provide separation for visual resolution. The least significant digit occurs first. The BCD code recycles yearly.

Forty-five control functions occur between position identifiers P_5 and P_R. Any control function element or combination of control function elements can be programmed to read a binary "one" during any specified number of time frames. Each control element is identified on the Control Function Field Table.

Figure 3-17: IRIG E Time Code description

BIT #	CF ELEMENT #	FUNCTION
50	1	SPACE
51	2	SPACE
52	3	SPACE
53	4	SPACE
54	5	SPACE
55	6	TIME SYNC STATUS
56	7	SPACE
57	8	SPACE
58	9	SPACE
59	PID P6	POSITION IDENTIFIER
60	10	YEAR UNITS Y1
61	11	YEAR UNITS Y2
62	12	YEAR UNITS Y4
63	13	YEAR UNITS Y8
64	14	SPACE
65	15	YEAR TENS Y10
66	16	YEAR TENS Y20
67	17	YEAR TENS Y40
68	18	YEAR TENS Y80
69	PID P7	POSITION IDENTIFIER
70	19	SPACE
71	20	SPACE
72	21	SPACE
73	22	SPACE
74	23	SPACE
75	24	SPACE
76	25	SPACE
77	26	SPACE
78	27	SPACE
79	PID P8	POSITION IDENTIFIER
80	28	SBS 2^0
81	29	SBS 2^1
82	30	SBS 2^2
83	31	SBS 2^3
84	32	SBS 2^4
85	33	SBS 2^5
86	34	SBS 2^6
87	35	SBS 2^7
88	36	SBS 2^8
89	PID P9	POSITION IDENTIFIER
90	37	SBS 2^9
91	38	SBS 2^{10}
92	39	SBS 2^{11}

93	40	SBS 2^{12}
94	41	SBS 2^{13}
95	42	SBS 2^{14}
96	43	SBS 2^{15}
97	44	SBS 2^{16}
98	45	SPACE
99	PID P0	POSITION IDENTIFIER

Table 3-4: IRIG E Control Function Field

3.9 Local System Clocks Setup

You can define up to 5 Local Clocks or Time Zones to be used with any of the Remote, Serial, IRIG 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 (Daylight Saving Time) conditions. To configure a Local Clock:

Note: The Local clock is not available for the front panel Ethernet output per the NTP specifications. NTP ALWAYS provides UTC time. Each client PC on the network will handle corrections for local time).

Connect to the web browser user 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:

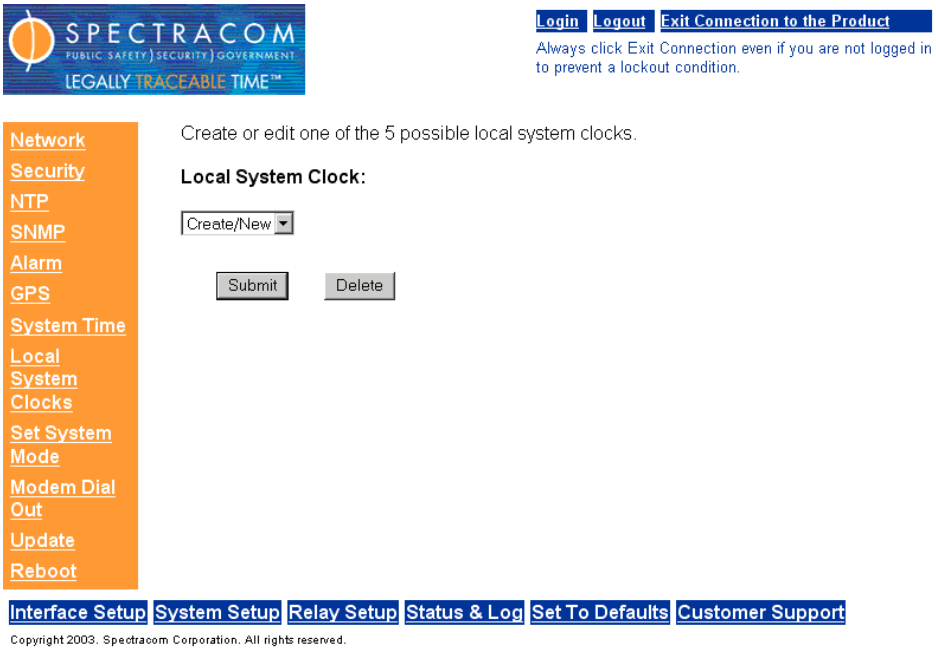


Figure 3-18: Local System Clocks Setup Screen

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

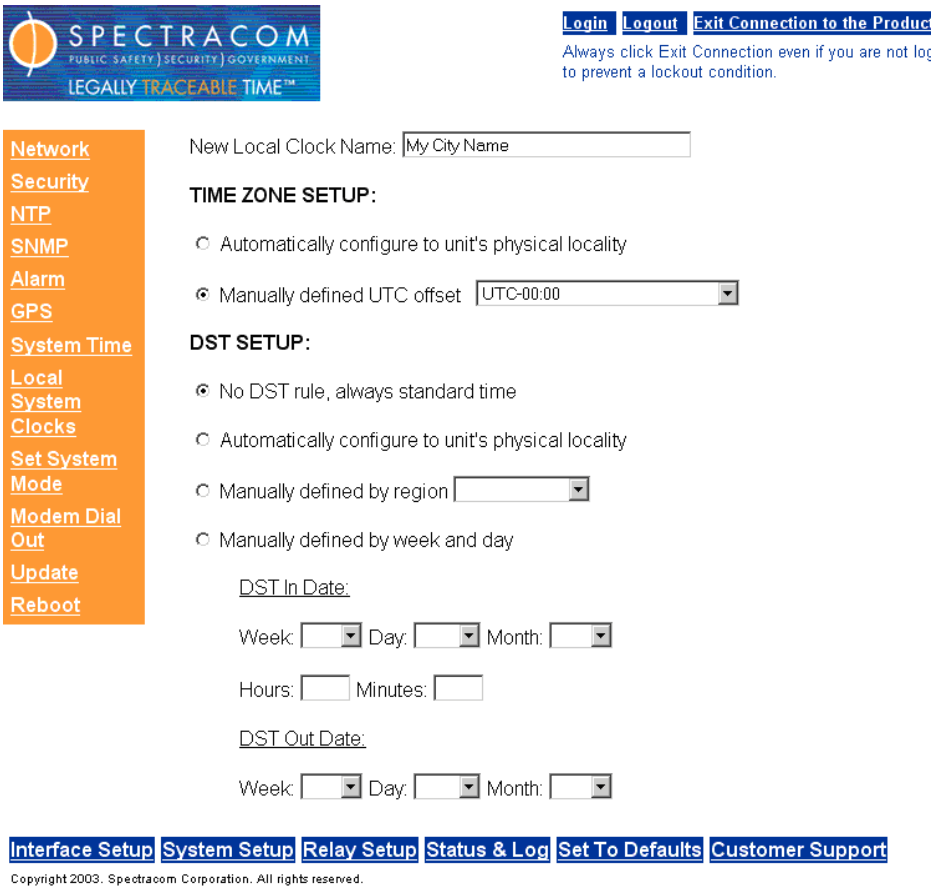


Figure 3-19: Time Zone and DST Setup Screen

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:

Connect to the web browser user interface of the unit.

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

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

Click on the “Manually Defined UTC Offset” button.

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

Select the 'No DST rule' radio button.

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:

Connect to the web browser user interface of the unit.

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

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

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

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

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

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

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

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:

Connect to the web browser user interface of the unit.

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

Select the desired Clock Name.

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

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

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

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

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

3.9.1 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 (Option 2 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: 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 user interface are configured as UTC plus or minus a set number of hours. For **Eastern**, choose UTC–5, for **Central**, choose UTC-6, for **Mountain**, choose UTC-7 and for **Pacific**, choose 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: 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 respond that the entry is an illegal date.

3.10 Logs

The following table lists the available logs (along the top header of the table) and provides a description and characteristics of each of below the corresponding log.

	Alarm Log	**Dialout Log (Modem-** Option 3)	**Event Relay Log**	**GPS Qualification Log**	**Operational Log**	**Oscillator Log**
Purpose	Reports any status change of Major or Minor alarms (On/Off).	Reports any dial out activity performed by the modem, such as dial out times, success or failure, and any time adjustments made as a result.	Reports any change in state (OPEN or CLOSE) of the event relays, such as for Major or Minor alarms, or for scheduled events programmed by the user.	Reports detailed information about GPS signal, including number of satellites tracked and for how long. Can be exported as a .CSV file via FTP.	Reports any boot of the unit, time source changes, and sync acquisition or loss. All system time adjustments are also shown here.	Reports startup at power cycle, and any coarse or fine adjustment of the oscillator.
Where	Top of left menu under Status & Log tab in web browser user interface	Next on menu under Status & Log tab in web browser user interface	Next on menu	Lower on menu	Next on menu	Next on menu
Update frequency	Per alarm state change	Per modem activity, about five per dial session	Per alarm or scheduled event.	Periodic, one per hour	Per boot up or system time change	Periodic, minimum every 100 seconds
Maximum log size	512 entries, 68 kilobytes	512 entries, 68 kilobytes	512 entries, 68 kilobytes	512 entries, 68 kilobytes	512 entries, 68 kilobytes	512 entries, 68 kilobytes
Rollover method	Per log entry, first in, first out	Per log entry, first in, first out	Per log entry, first in, first out	Per log entry, first in, first out	Per log entry, first in, first out	Per log entry, first in, first out
Log rollover typical	Months	Months	Months	21 days	Months	10-14 hours

Table 3-5: Descriptions of logs

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

3.10.1 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 counter 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.

3.10.2 Display Dial-Out Log (Applicable only to units with Option 3 – Modem)

If the NetClock has the optional Dial-Out Modem Interface (Option 3), 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= 18:00:51 DATE= 2005-07-07
Modem dial out to 9 1-303-494-4774.

TIME= 18:02:04 DATE= 2005-07-07
Dial out successful.

TIME= 18:02:06 DATE= 2005-07-07
Time Sync Success: Subsecond counter adjusted by -1.3209 ms.

TIME= 18:02:07 DATE= 2005-07-07
Time Sync Success: Sys Clock adjusted by 0 sec.

TIME= 18:02:07 DATE= 2005-07-07
No leap second detected this month

In the example above, the unit initiated a dial out at 18:00:51 to the number (9)1-303-494-4774. At 18:02:04 it successfully finished the call and disconnected the modem from the phone line. It then processed the collected time messages and adjusted the unit's PPS back by 1.3209ms. It then adjusted the system clock by 0 seconds at 18:02:07. In that same second it verified that there was no leap second for that month

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

Calibration initiated:
Calibration routine has started.

Calibration call success (#/#) calls made: Gives # of calls that have been successful and # of calls that are scheduled.

Calibration call failed: failure # of #: Gives # of calls that have failed in a row and # before calibration will fail.

Calibration failed:
Calibration has ended without setting the latency value.

Calibration Success - Latency set to # ns: Calibration was successful. The latency was set. Counter resolution means this number will always end with 00.

Call failed: [reason]:
Possible reasons are:
State Change – Modem no longer needs to synchronize system (example: GPS signal came back)
Busy Signal – Time source was busy.
Modem Error – Unspecified modem error
No carrier – No modem picked up on other end, phone # may be wrong
No dialtone – Could not get a dialtone
Netshow Request – "net show" was typed on the console port
Port Change – Switched to console mode
No Sync Message – Could not synchronize with the remote modem

Dial out successful:
Messages were successfully collected from time source.

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.

Leap Second check failed [reason]:
Only reason is BAD MESSAGE, which means that the leap second bit was not consistent across all messages. This can happen if the month rolls over during a call or if some of the message characters are lost.

Leap second detected: Leap second will be [ADDED/DELETED] at the end of the month
Leap second is to occur this month.

Modem Response Failure:
Failed to get a response from the modem at initialization.

Modem Call Failure:
Failed all call retries.

Modem dial out to #:
Gives the phone number which was dialed.

No leap second detected this month:
Whenever a successful call is made and there is no leap second.

Test Call Failure:
The test call failed at some point. The reason for failure should be evident from the other messages.

Test Call Success:
The most recent test call successfully got messages from the dialed number.

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 receives no response from the modem for two minutes, the operation is aborted. If there are retries remaining, the dial out process is restarted.

Time Sync Failure: [reason]:
The modem failed to set the time. Gives the reason why the time could not be set. Possible reasons are:

Port Switched – The port was set to console mode.
Alternate Sync – The unit got sync from another source first.
Timeout – The unit timed out while trying to reset time.
Unknown Error – ?

Time Sync Failure: Sys Clock not adjusted [reason]:
The sys clock could not be adjusted. Gives the reason why the clock could not be adjusted. Possible reasons are:

Bad Timing - The unit could not verify the timestamps. This is a rare condition and does not indicate any hardware error unless it happens frequently.

PPS error - The unit could not get a good PPS signal from itself.

Time Sync Success: Subsecond counter adjusted by # ms:
Time was successfully adjusted.

Time Sync Success: Sys Clock adjusted by # sec:
System clock (date and time) was adjusted.

Time verification success: Time within normal parameters:
While in holdover, time was verified and is still within 0.5 seconds. This implies that a leap second was not missed.

Time verification: Time too far off. Exiting Sync:
Time is off by more than 0.5 seconds. A leap second was missed or something is very wrong.

3.10.3 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.

3.10.4 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 GPS qualification log is useful in verifying receiver and antenna performance.

The GPS qualification log is outputted 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.

There 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:
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 "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.

3.10.5 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:
Spectracom Corp. Model 9189
Software Version 2.3.0 Date: 07/07/2005
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 #:
This statement is printed after each power cycle to give the version of the GPS receiver.

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 four satellites for one minute. A satellite is considered qualified if the received vehicle ID number is at least 4 and if all four satellites can be used for Position Fix. The time and date contained in the log reflect UTC time. If the unit is operating in the single satellite mode (not recommended), the minimum number of satellites for qualification drops to only 1 satellite required for one minute.

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

Clock adjusted by # seconds:
A log entry is made in this log for any system time adjustment larger than 1 second.

Clock time source changed to [source]:
A log entry is made every time the clock's reference is changed. For example, the unit is synchronized to GPS but someone tries to manually set the time. The log will indicate that the input was "user".

Clock entering sync:
This entry will be made when the unit acquires time sync

Leap second inserted at end of month:
The reference input had detected that a leap second was to occur at the end of the month and the NetClock added the necessary correction to account for the leap second.

Leap second removed at end of month:
The reference input had detected that a leap second was to occur at the end of the month and the NetClock removed the necessary correction to account for the leap second.

GPS SOFTWARE RESET:
This log entry indicates the GPS receiver stopped responding so the unit has performed a software reset of the GPS receiver daughter-board to try to restart the receiver.

GPS HARDWARE RESET:
This log entry indicates the GPS receiver stopped responding so the unit has performed a hardware reset of the GPS receiver daughter-board to try to restart the receiver.

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

3.10.6 Display Oscillator Log

Note: The oscillator log is not available for rubidium-based (Option 4) 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 adjusts 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 or logging of oscillator data 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.

3.11 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.

3.11.1 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 browser user interface.

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

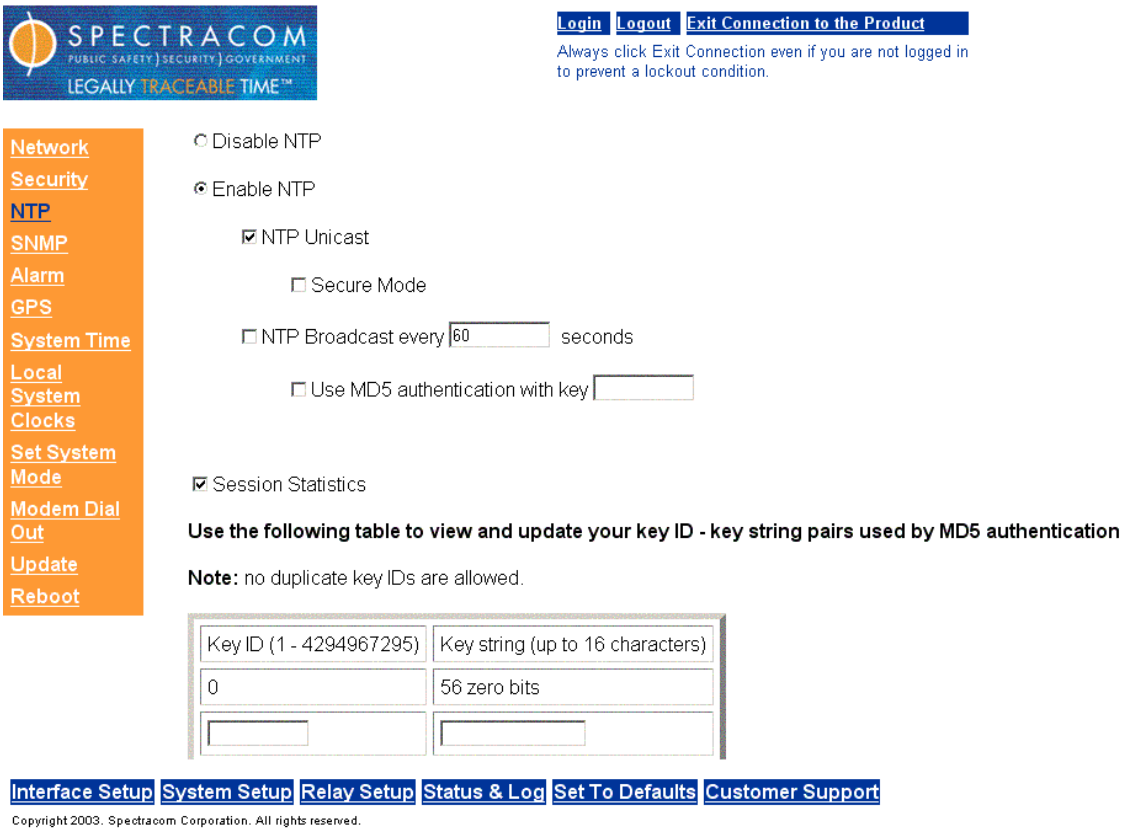


Figure 3-20: NTP Screen

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.
To enable Unicast operation, place a checkmark in the box labeled "NTP Unicast".
To enable multicast operation, place a checkmark in the box labeled "NTP Broadcast …".
To enable both modes, be sure that both boxes have a checkmark.

In **Unicast mode**, the NTP server will "listen" for NTP request messages from NTP clients on the network. When an NTP request packet is received, the NTP server will send an NTP response time packet to the requesting client. Under typical conditions, the Spectracom NTP server can service up to 390 NTP requests per second, without MD5 encryption enabled (read below).

In **multicast mode**, the NTP server will send out unsolicited NTP time packets to the local broadcast address at a user-specified rate. Enter the desired frequency in seconds into the Broadcast field on the setup page.

Note: Unicast Mode is the predominant mode of operation when synchronizing a network. Multicast is reserved for specialized software requirements and is not commonly used.

By default, the NTP server supports authenticated NTP packets via an MD5 authenticator. This feature does not encrypt the time packets, but attaches an authenticator, which consists of a key identifier and an MD5 message digest, to the end of each packet. This can be used to guarantee that NTP packets came from a valid NTP client or server, and that they were not tampered with during transmission.

To use the MD5 authentication in Unicast mode, both the NTP client and the Spectracom NTP server must contain the same key ID / key string pair 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 may contain any alphanumeric characters and can be from 1 to 16 characters long. Duplicate key IDs are not permitted.

When operating in Unicast mode, the Spectracom NTP server supports a secure mode, which can be enabled by placing a checkmark in the box labeled "Secure Mode". With this box checked, any NTP requests received by the NTP server, which do not contain a valid "Key ID / Key String" pair will be ignored and no NTP response packet will be sent.

The following table shows how the Spectracom NTP server will respond to various unicast requests with and without secure mode enabled.

Type of NTP Request Packet	Without "Secure Mode" checked	With "Secure Mode" checked
No MD5 authenticator	Response with no MD5 authenticator	No response
Invalid MD5 authenticator	Response with valid authenticator (using key 0)	No response
Valid MD5 authenticator	Response with valid authenticator (using same key as the request)	Response with valid authenticator (using same key as the request)

When operating in multicast mode, the Spectracom NTP server can be configured to append MD5 authenticators to each packet. To enable this, check the box labeled "Use MD5 authentication with key …" under the NTP Broadcast setting, and enter the key ID to be used.

The ***Session statistics*** checkbox will enable or disable logging of NTP usage statistics. This is displayed as part of the ***status and log*** page. 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.

3.11.2 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.

3.11.3 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 NetClock, 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.**

3.12 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:

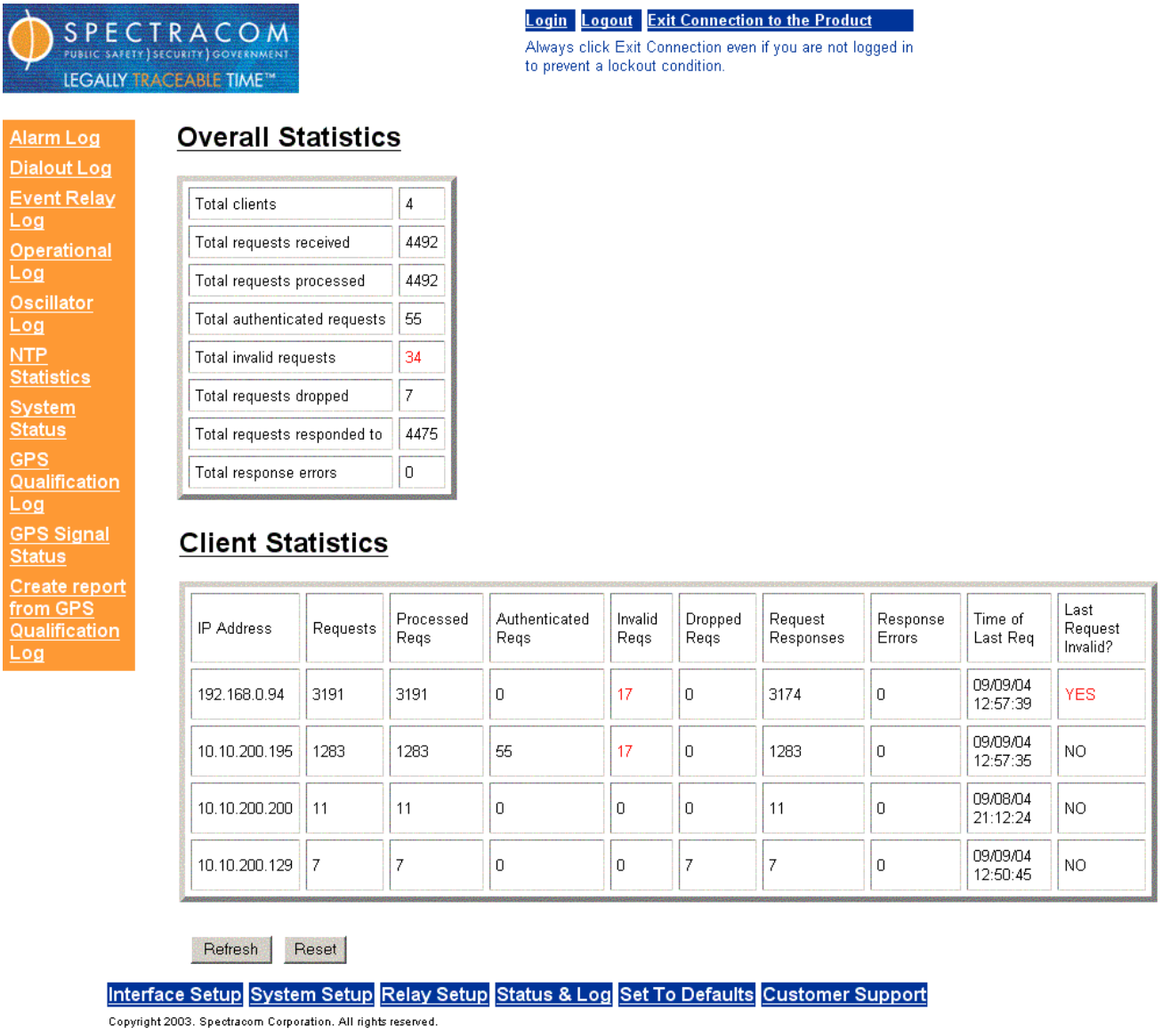


Figure 3-21: NTP Statistics

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.

The statistics log can retain the entries for up to 200 clients. Once the maximum of 200 clients has been reached, sequential clients over 200 will start to overwrite the oldest entries in the log (this may or may not be in the order listed in the log).
The following are descriptions of the fields contained in the NTP Statistics chart.

Total Clients: The total number of clients that the NetClock has received NTP packets from, up to a maximum of 200.

Requests: Number of NTP packets received by the NetClock from a client or clients.

Processed Requests: Number of NTP packets received that were processed by the NetClock. The NetClock will only process received NTP packets while NTP is enabled AND NTP Unicast is enabled. These settings can be enabled from the NTP configuration page.

Authenticated Requests: Number of NTP packets received by the NetClock that were processed, included authenticator fields, and authenticated successfully.

Invalid Requests: Number of NTP packets received by the NetClock that were processed and either (1) included authenticator fields but authenticated unsuccessfully, or (2) did not include authenticator fields and Secure Mode was enabled. Secure mode can be enabled or disabled from the NTP configuration page.

Dropped Requests: Number of NTP packets received by the NetClock that were either (1) not processed because NTP was not enabled and/or NTP Unicast was not enabled, (2) ignored because the packet length did not match the valid length for an NTP packet, (3) ignored because the NTP request specified a mode that the NetClock does not support, or (4) ignored because the NTP request specified a version that the NetClock does not support. NetClock supports requests using CLIENT mode or SYMMETRIC ACTIVE mode. NetClock supports requests using versions 1, 2, 3, or 4.

Request Responses: Number of NTP request packets received by the NetClock that were successfully responded to. A successful response is logged when the NetClock transmits an NTP response packet to the client without noting any errors.

Response Errors: Number of NTP request packets received by the NetClock that were unsuccessfully responded to. An unsuccessful response is logged when the network protocol stack is unable to successfully transmit the response packet to the client.

Time of Last Request: The time at which the last NTP packet was received from a particular client.

Last Request Invalid?: Identifies whether or not the last NTP request received from a particular client was an invalid request.

Note: To clear the NTP Statistics log, login to the administrator mode and press the “reset” radio button.

3.13 Relays

3.13.1 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 browser user 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 browser user 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.

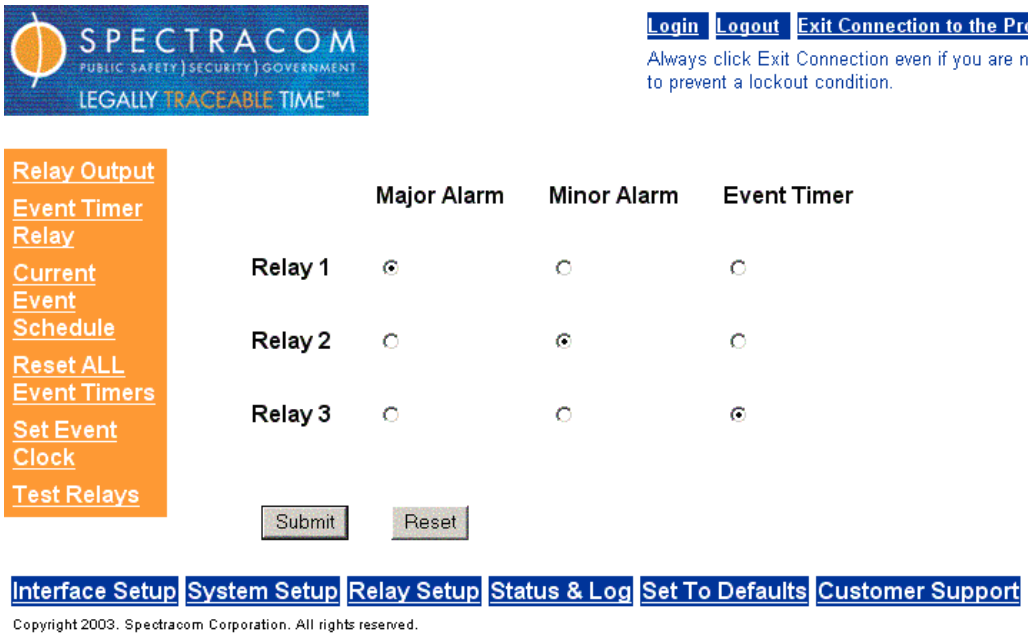


Figure 3-22: Relay Output Screen

To test the operation of the relays:

The relay operation of all three relays can be tested at any time as desired. To test the relay operation, login as administrator mode and click on “test relays” in the left orange bar. Chose the desired relay to be tested and then press submit. The selected relay should activate each time the submit button is pushed.

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.”

3.14 Security

3.14.1 Security Overview

In addition to providing login accounts with up to 16-character passwords supporting different privileges for the config and admin users, Spectracom products providing security features use OpenSSH and OpenSSL. OpenSSH is the Open Source version of the Secure Shell; which provides a set of server side tools allowing secure remote telnet like access and secure file transfer using remote copy like (RCP) and FTP like utilities. OpenSSL is the Open Source version of Secure Sockets Library; which is used to provide the encryption libraries. Together OpenSSH and OpenSSL provide industrial strength encryption allowing for secure remote administration via command line, HTTPS web pages and secure file transfers.

A convenient and simple web browser user interface is provided under the "System Setup" tab's "Network" and "Security" sub menus. Users can configure their product and control the network access to the product by selecting options found under these menus. The Network sub menu allows the user to choose to enable or disable protocols such as Telnet and FTP. The user can also as described in the Network menu section control their subnet and gateway. On the Model 9183, the user is permitted to enable or disable HTTP and SSH as well. The secure product can be configured to allow access only via NTP and the secure protocols such as HTTPS or SSH or to operate in a less secure mode. Spectracom secure products also provide a Security submenu. The security submenu provides the user with the means to configure their use of SSH and SSL.

Pop up help text is available for most Security web browser user interface features. Allow your cursor to hover over the box and help text box should appear.

3.14.2 Configuring SSH

3.14.2.1 Overview

OpenSSH implements a free version of Secure Shell. Secure Shell is a set of server and client tools supporting secure telnet like remote access and secure, authenticated file transfers using passwords and/or public key cryptography. The tools supported are SSH – secure shell, SCP – secure copy, and SFTP – secure file transfer protocol. The Master Clock implement the server components of SSH, SCP and SFTP.

For more information on OpenSSH please see www.openSSH.org.

3.14.2.2 Managing Host Keys

Overview

SSH uses Host Keys to uniquely identify each SSH server. Host Keys are used for server authentication and identification. The secure Spectracom product allows the user to create or delete RSA1 keys for the SSH1 protocol or RSA or DSA keys for the SSH2 protocol.

Deleting Host Keys

The user may choose to delete individual Host Keys. To delete a key simply select a radio button for the key you wish to delete and press submit at the bottom of the page.

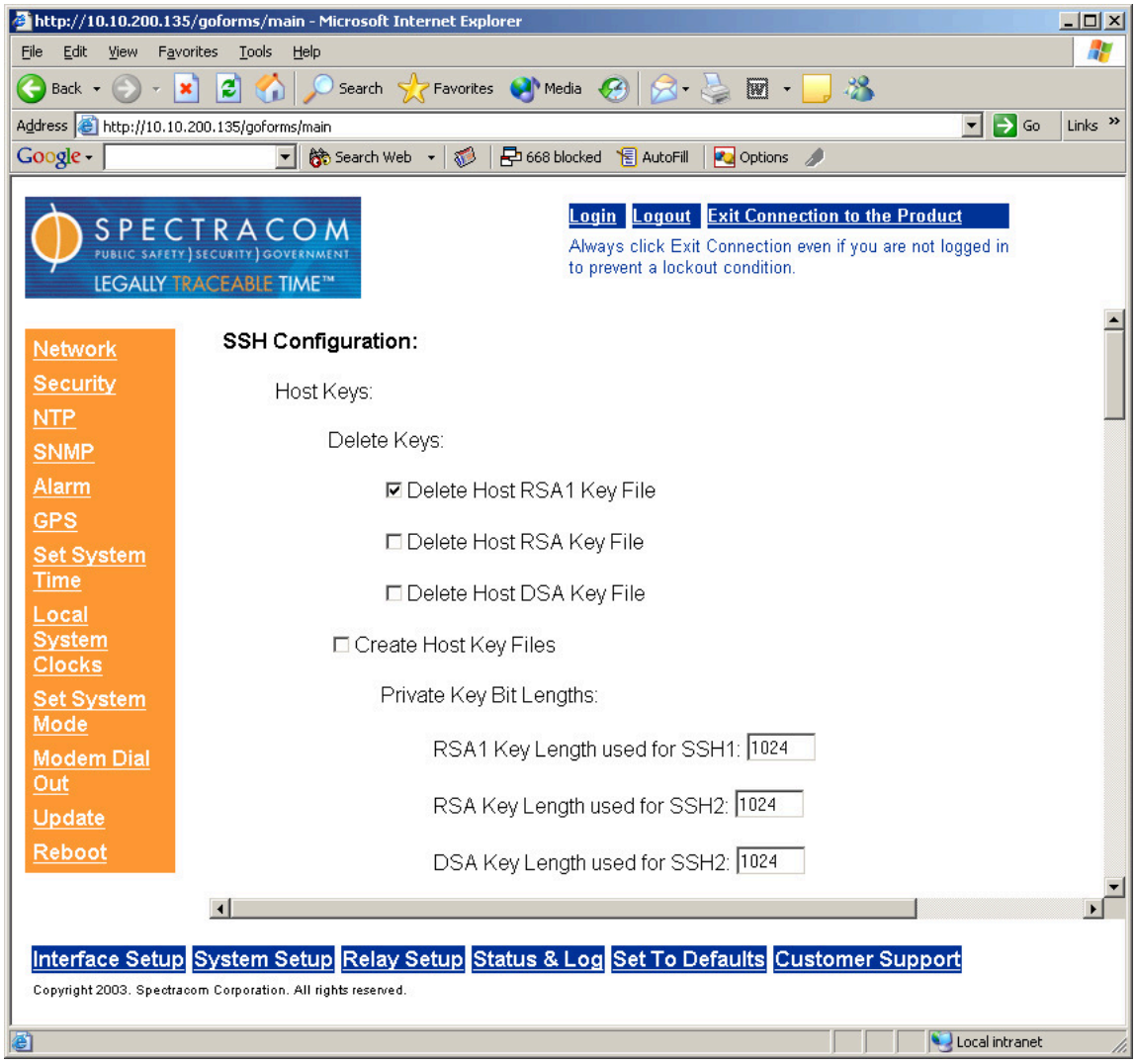


Figure 3-23: SSH configuration Screen

If the user chooses to delete the RSA1 key, the SSH1 protocol is not available and SSH1 clients will be unable to connect.

If the user chooses to delete the RSA or DSA key only the SSH2 protocol will function but that form of server authentication will not be available. If the user chooses to delete both the RSA and DSA keys the SSH2 protocol is not available and SSH2 clients will be unable to connect.

If the users chooses to simultaneously delete the RSA1, RSA and the DSA keys, SSH will not function. In addition, if SSH Host Keys are being generated at the time of deletion, the key

generation processes are stopped, any keys created will be deleted, and all key bit sizes are set to 0.

The user may choose to delete existing keys and request the creation of new keys, however it is often simpler to make these requests separately.

3.14.2.3 Creating Host Keys

The user may create individual RSA1, RSA and DSA Host Public/Private Key pairs. Host Keys must first be deleted before new Host Keys can be created. To create a new set of host keys first delete the old keys, then select the create host keys checkbox and enter the key sizes you desire. Then select the submit button at the bottom of the screen.

A typical Host Key generation request is shown below.

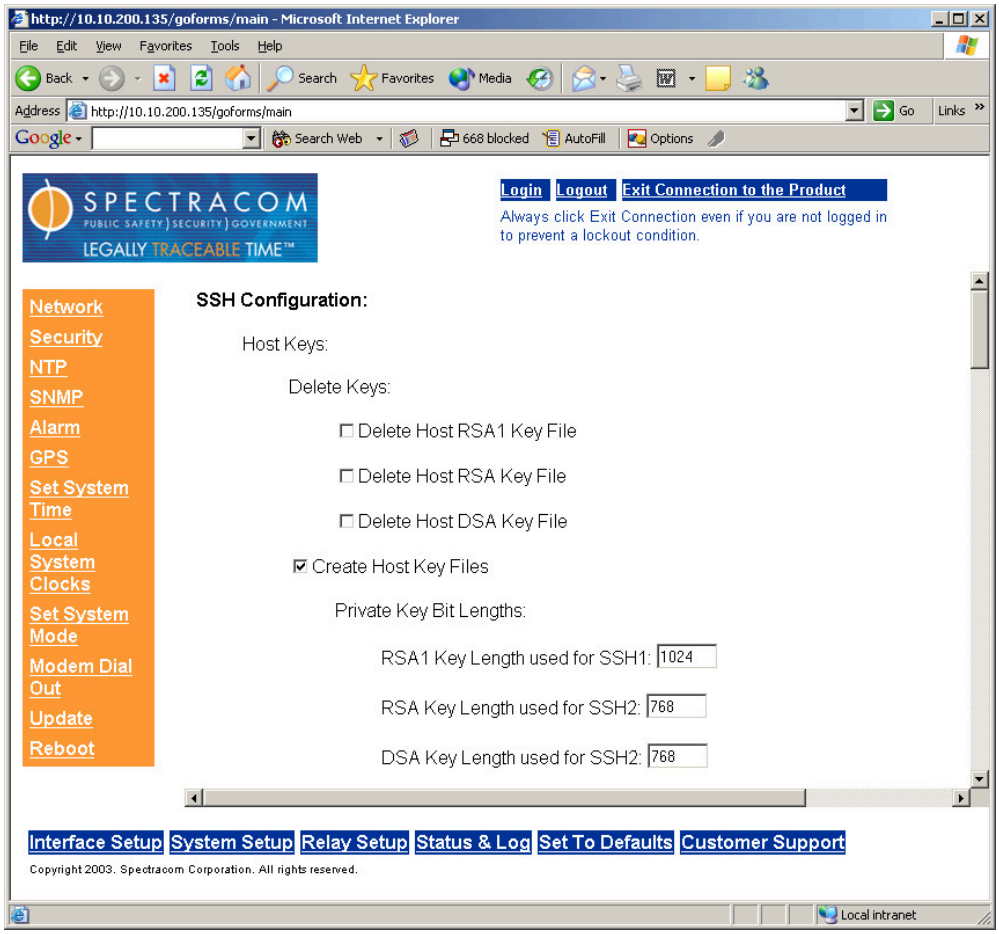


Figure 3-24: Creating SSH host key files

Spectracom secure products typically have their initial Host Keys created at the factory. The default key size for all key types is 1024. Host Key sizes can vary between 768 and 4096 bits. The recommended key size is 1024. Though many key sizes are supported, it is recommended

that users select key sizes that are powers of 2 or divisible by 2. The most popular sizes are 768, 1024, and 2048. Large key sizes up to 4096 are supported, but are discouraged because they take hours to generate.

Host Keys are generated in the background. Creating an RSA1, RSA and DSA keys each with 1024 bits length, typically takes about 10 minutes. Keys are created in the order of RSA, DSA and finally RSA1. When the keys are created you can successfully make SSH client connections. If the unit is rebooted with Host Key creation in progress or the unit is booted and no host keys exist the key generation process is restarted. The key generation process uses either the previously specified key sizes or if a key size is undefined it defaults to 1024. A key with a zero length or blank key size field is not created.

Note also that when you delete a Host Key and recreate a new one, SSH client sessions will warn you that the host key has changed for this particular IP address. The user will either have to override the warning and accept the new Public Host Key and start a new connection or they may need to remove the old Host Public Key from their client system and accept the new Host Public Key. Please consult your specific SSH client's software's documentation.

3.14.2.4 Selecting SSH Authentication Mode

The SSH client utilities SSH, SCP and SFTP allow for several modes of user authentication. SSH allows the user to remotely login or transfer files by identifying the user's account and the target machines IP address. Users can be authenticated by either using their account passwords or by using a Public Private Key Pair. Users keep their private key secret within their workstations or network user accounts and provide the Spectracom secure product a copy of their public key.

To select an Authentication mode admin users select an option from the Authentication section and select submit at the bottom of the page.

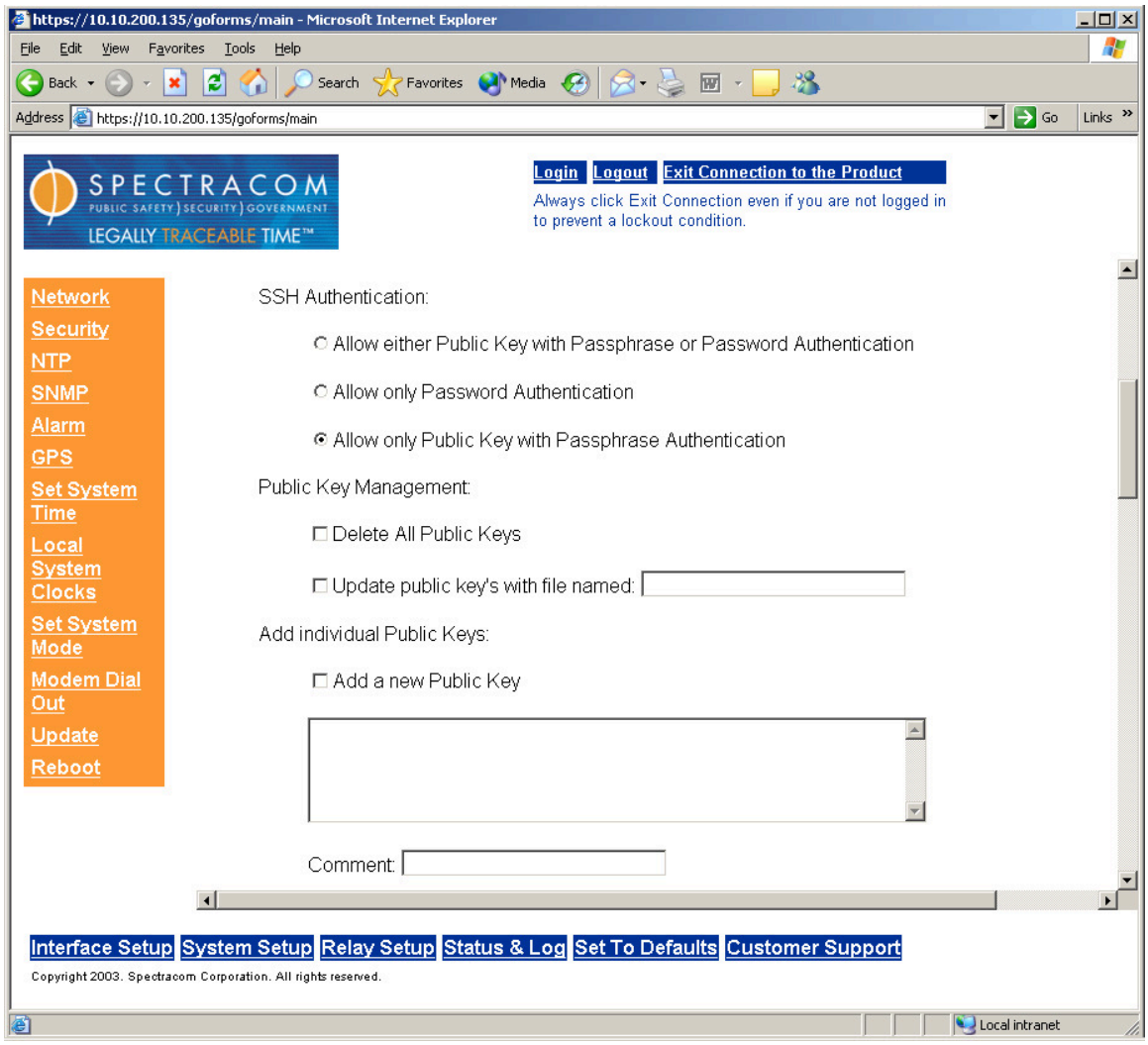


Figure 3-25: Selecting SSH authentication modes

The modes of authentication supported include:

Either Public Key with Passphrase or Login Account Password
Login Account Password only
Public Key with Passphrase only

The first option allows users to login using either method. This is the default. Whichever mode works is allowed for logging in. If the Public Key is not correct or the Passphrase is not valid the user is then prompted for the login account password. The second option simply skips public/private key authentication and immediately prompts the user for password over a secure encrypted session avoiding sending passwords in the clear. Finally the last option requires the user to load a public key into the Spectracom secure product. This public key must match the private key found in the users account and be accessible to the SSH, SCP or SFTP client

program. The user must then enter the Passphrase after authentication of the keys to provide the second factor for 2-factor authentication.

3.14.2.5 Managing Public Keys used for SSH Authentication

SSH using public/private key authentication is the most secure method of authenticating users for SSH, SCP or SFTP sessions.

The web browser user interface provides the means for the user to delete the /sys/.SSH/authorized_keys file, to add individual Public Keys and comments to the existing file, and to copy a file containing Public Keys from the /sys/update folder to a file named /sys/.SSH/authorized_keys. Using FTP, SCP or SFTP the user may also retrieve the read-only authorized_keys file from the /sys/.SSH directory.

An example of a user adding a public key to the authorized_keys file is shown below.

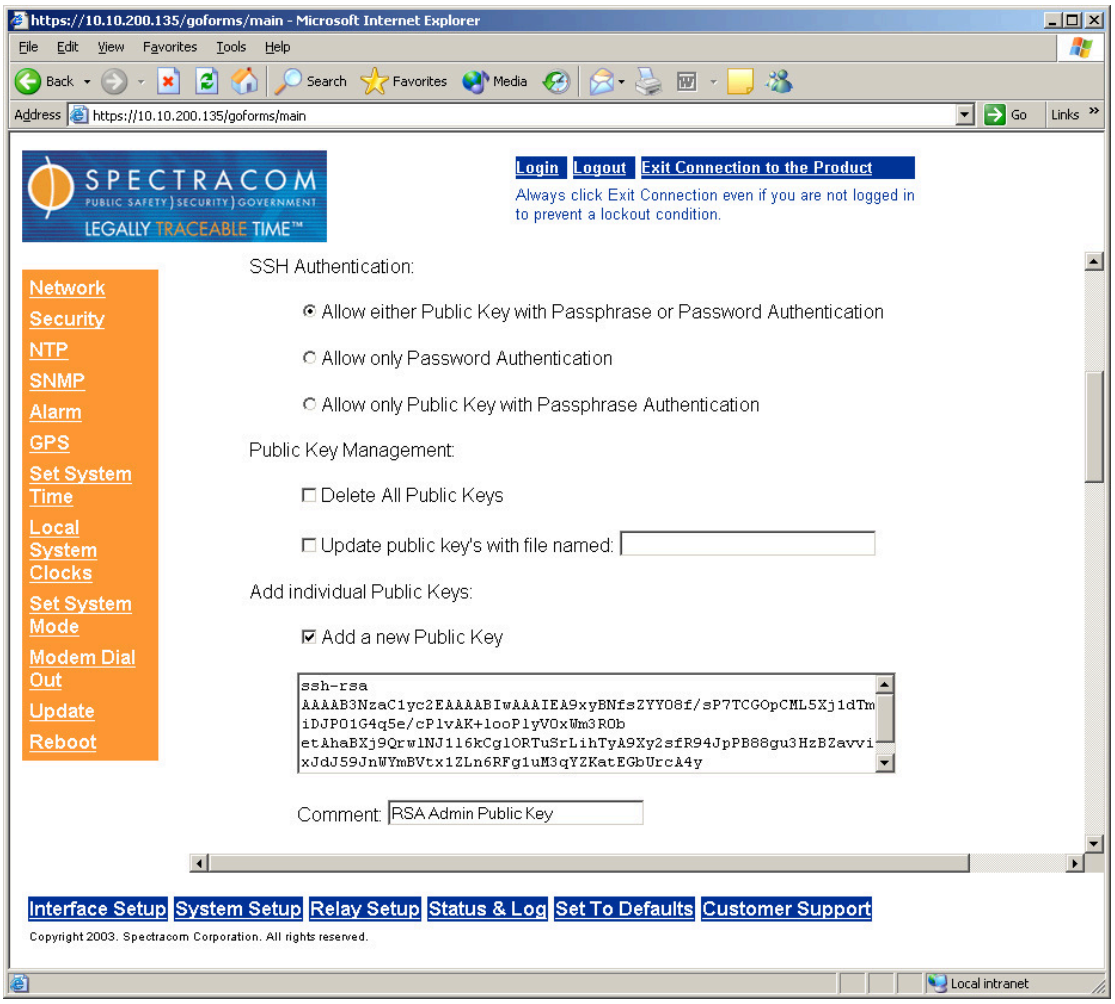


Figure 3-26: Adding SSH public key to authorized keys

Users are required to create private and public key pairs on their workstation or within a private area in their network account. These keys may be RSA1, RSA or DSA and may be any key bit length as supported by the SSH client tool. These public keys are stored in a file in the /sys/.SSH directory named authorized_keys. The file permissions are to be read-write for root and read-only for all other users. The file is to be formatted such that the key is followed by the optional comment with only one key per line. The Spectracom application terminates each line with a carriage return and separates each line with a blank line. The file format, line terminations and other EOL or EOF characters should correspond to UNIX conventions, not Windows.

If a user deletes all Public Keys Public/Private Key Authentication is disabled. If the user has selected SSH authentication using the "Public Key with Passphrase" option login and file transfers will be forbidden. The user must select a method allowing the use of account password authentication to enable login or file transfers using SCP or SFTP.

If a user wants to completely control the public keys used for authentication a correctly formatted authorized_keys file formatted as indicated in the OpenSSH web site can be loaded onto a secure Spectracom product. The user transfers a new public key file using an insecure FTP client or a secure SCP or SFTP client using only account password authentication. The user should place the new public key's file in the /sys/update directory. The user then selects the delete all public key's checkbox, selects the update public key's checkbox and enters the filename in the space provided.

An example of a user adding a new public key file is shown below.

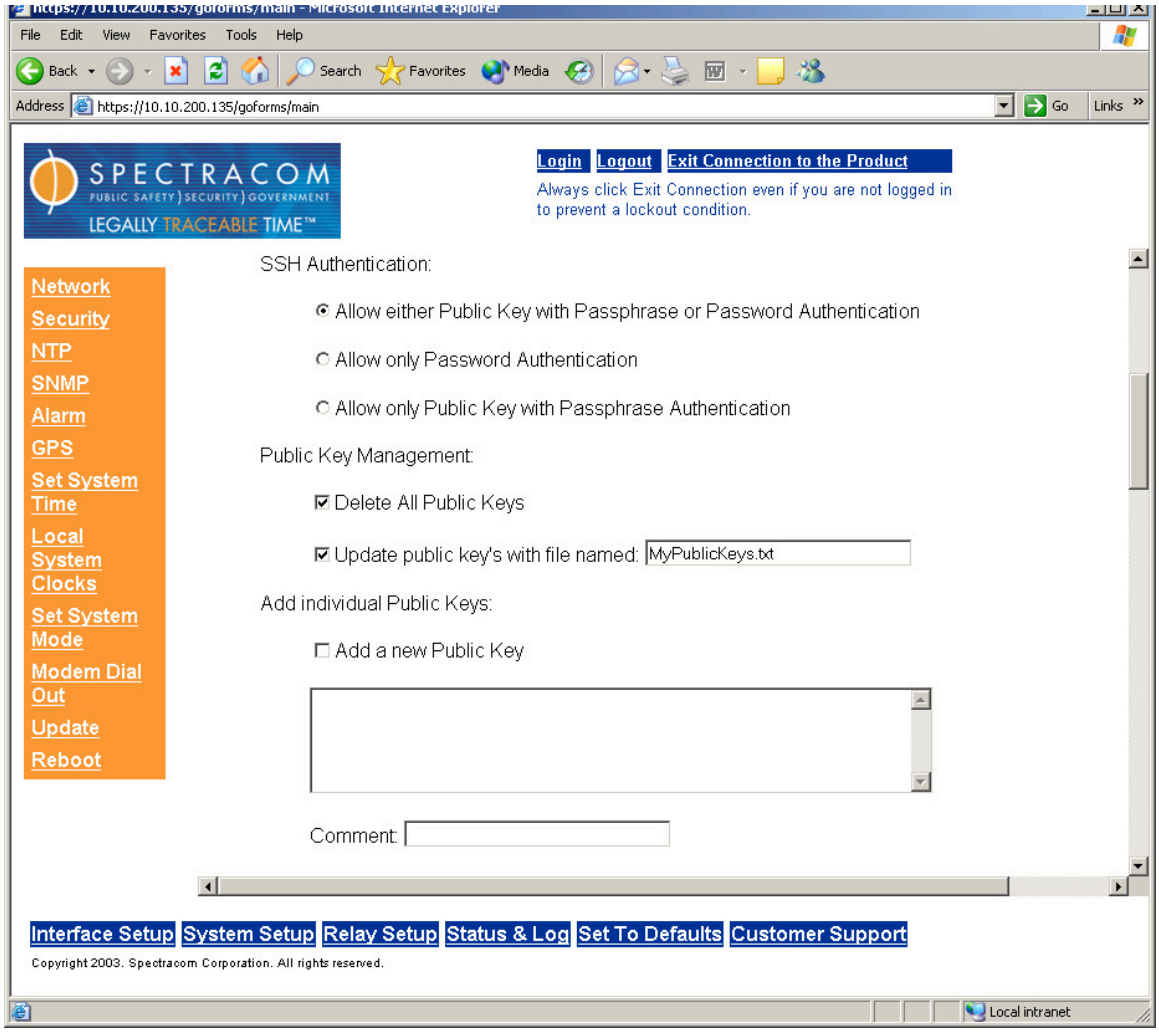


Figure 3-27: Adding a new SSH public key file

The MyPublicKeys.txt file in the /sys/update directory is renamed and placed in the /sys/.SSH directory under the new name authorized_keys after the user selects the submit button at the bottom of the screen. Users can now authenticate using Private Keys, which match these public keys if the authentication mode supports "Public Key with Passphrase" authentication.

3.14.2.6 Secure Shell Sessions

Secure shell sessions using an SSH client can be performed using the admin or config accounts. The user may use Account Password or Public Key with Passphrase authentication. Please be patient it can take a few minutes to establish a secure SSH session. The OpenSSH tool SSH-KEYGEN is used to create RSA1, RSA and DSA keys used to identify and authenticate user login or file transfers.

The following command lines for OpenSSH SSH client tool are given as examples of how to create a secure SSH session.

Creating an SSH session with Password Authentication for the admin account.
ssh admin@10.10.200.5
admin@10.10.200.5's password: admin123

The user is now presented with Boot up text and/or a ">" prompt which allows the use of the Spectracom command line interface.

Creating an SSH session with Password Authentication for the admin account.
ssh config@10.10.200.5
config@10.10.200.5's password: config12

The user is now presented with Boot up text and/or a ">" prompt which allows the use of the Spectracom command line interface.

Creating an SSH session using Public Key with Passphrase Authentication for the admin or config account.

The user must first provide the secure Spectracom product a RSA public key found typically in the OpenSSH id_rsa.pub file. The user may then attempt to create an SSH session.

ssh -i ./id_rsa admin@10.10.200.5
Enter passphrase for key './id_rsa': mysecretpassphrase

Please consult the SSH client tool's documentation for specifics on how to use the tool, select SSH protocols, and provide user private keys.

3.14.2.7 Secure File Transfer

Master Clocks provide secure file transfer using the SSH client tools SCP and SFTP. Authentication is performed using either Account Passwords or Public Key with Passphrase. However unlike SSH where the config or admin accounts are used, a special user account is provided named "SCP" for these tools. The "SCP" user account has the same password as the admin account. It differs from the admin and config accounts in that it does not run the Spectracom product shell. It is a limited account that only allows the user to transfer files to and from the /sys/update folder and to retrieve files from folders which the SCP account has read permission.

Some sample OpenSSH, SCP and SFTP client commands are shown below.

1) Perform an SCP file transfer to the device using Account Password authentication

scp publickeys scp@10.10.200.5:/sys/update
scp@10.10.200.135's password: admin123 (Always use same password as admin)

publickeys 100% |**| 5
00:00

2) Perform an SCP file transfer from the device using Public Key with Passphrase authentication.

scp -i ./id_rsa publickeys scp@10.10.200.5:/sys/update
Enter passphrase for key './id_rsa': mysecretpassphrase

publickeys 100% |**| 5
00:00

3) Perform an SFTP file transfer to the device using Account Password authentication.

sftp -i ./id_rsa scp@10.10.200.5
scp@10.10.200.135's password: admin123 (Always use same password as admin)

sftp>

The user is presented with the SFTP prompt allowing interactive file transfer and directory navigation.

4) Perform an SFTP file transfer from the device using Public Key with Passphrase authentication

sftp -i ./id_rsa scp@10.10.200.5
Enter passphrase for key './id_rsa': mysecretpassphrase

sftp>

The user is presented with the SFTP prompt allowing interactive file transfer and directory navigation.

3.14.2.8 Recommended SSH Client Tools

Spectracom does not make specific recommendations as to which specific SSH client, SCP client, or SFTP client tools. However, there are many SSH based tools available at cost or free to the user.

Two good, free examples of SSH tool suites are the command line based OpenSSH running on a Linux or OpenBSD x86 platform and the excellent (and free) putty SSH tool suite.

The OpenSSH tool suite in source code form is freely available at www.openSSH.org though you must also provide an OpenSSL library, which can be found at www.openssl.org.

The putty SSH tools and instructions regarding their use can be found at:

HTTP://www.chiark.greenend.org.uk/~sgtatham/putty/

Note that it is strongly recommended to exit all SSH client sessions preferably using the "exit" command or "control-C" to avoid leaving the sshd daemon running. Exiting the putty tool (or SSH clients tools) by selecting the windows "X" button can leave the SSHd session running and result in refused connections until it times out after extremely long timeout delays. In such a case a reboot might be preferable rather than waiting.

3.14.3 Configuring HTTPS

3.14.3.1 Overview

The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS). The OpenSSL package also provides tools and software, which is used to create x509 Certificate Requests, Self Signed Certificates and Private/Public Keys. The Master Clock uses OpenSSL library with a simple GUI interface to create certificate Requests and self-signed certificates. Users can then send these certificate requests to an external Certificate Authority (CA) for the creation of a third party verifiable certificate or use an internal corporate CA. If a Certificate Authority is not available the user can simply use the self-signed certificate that comes with the unit until it expires or create their own self-signed certificates to allow the use of HTTPS.

Each Spectracom secure product comes with a default Spectracom self-signed certificate, which will outlast the product warranty. The typical expiration of the certificate is about 10 years. HTTPS is available using this certificate until this certificate expires. If deleted however, this certificate cannot be restored.

For more information on OpenSSL please see www.openssl.org.

3.14.3.2 Deleting Certificates, Private Keys, and Certificate Requests

The user is has the option of deleting the current certificate, certificate requests and private key. To choose the delete option simply check the delete checkbox and press the submit button at the bottom of the screen. Once the current certificate is deleted HTTPS is unavailable.

Figure 3-28: Deleting SSL Certificate, Certificate Request and Private Key Files

3.14.4 Restoring Self Signed Certificates and Private Keys

The user has an option to restore the last self signed certificate and private key created by the user. To restore these files the user needs to select the "Restore User's Self Signed Certificate and Private Key" checkbox. The user then selects the submit button at the bottom of the screen. The default Spectracom self-signed certificate and private key cannot be restored when deleted.

Figure 3-29: Restoring user's Self Signed Certificate and Private Key Files

3.14.5 Creating Self Signed Certificates, a Private Key, and a Certificate Request

The user can create a customer specific x509 self-signed certificate, an RSA private key and x509 certificate request using the web browser user interface. RSA private keys are supported because they are the most widely accepted. At this time DSA keys are not supported.

The user is required to select a signature algorithm, a private key passphrase of at least 4 characters, a private key bit length, the certificates expiration in days and at least one of the remaining fields. It is recommended that the user consult their Certificate Authority for the required fields in an x509 certificate request. Spectracom recommends all fields be filled out and match the information given to your certificate authority. For example, use all abbreviations, spellings, URLs, and company departments recognized by the Certificate Authority. This helps in avoiding issues with the Certificate Authority having issues to reconciling certificate request and company record information.

If using only self-signed certificates the user should choose the fields based upon the company's security policy.

A sample input screen to create a certificate request is shown below.

Figure 3-30: Creating a new Certificate Request and Self Signed Certificate

Note that it can take several minutes for the certificate request, the private key, and self-signed certificate are created. The larger the key the longer amount of time is required. It is recommended that a key bit length be a power of 2 or multiple of 2. The key bit length chosen is typically 1024, but can range from 512 to 4096. Long key bit lengths of up to 4096 are not

recommended because they can take hours to generate. The most common key bit length is the value 1024.

The user is provided with several signature algorithm choices. The signature algorithm or message digest is most commonly MD5. Other secure options include SHA1 and RMD160.

Consult your Web Browser documentation and Certificate Authority for key bit lengths and signature algorithms supported.

If a system is rebooted during this time, the certificate will not be created. When the operation is completed, the user will see a certificate request in the certificate request text box. A digital file copy of the certificate request can be found in the /sys/update directory with the file name cert.csr. This file can be retrieved using FTP, SCP or SFTP. The certificate request can also be cut and paste from the certificate request text box on the web browser user interface.

3.14.6 Requesting Certificate Authority Certificates

Once the processing to create the certificate request, RSA private key and self-signed certificate is completed the web browser user interface will display the certificate request.

A certificate request is shown below.

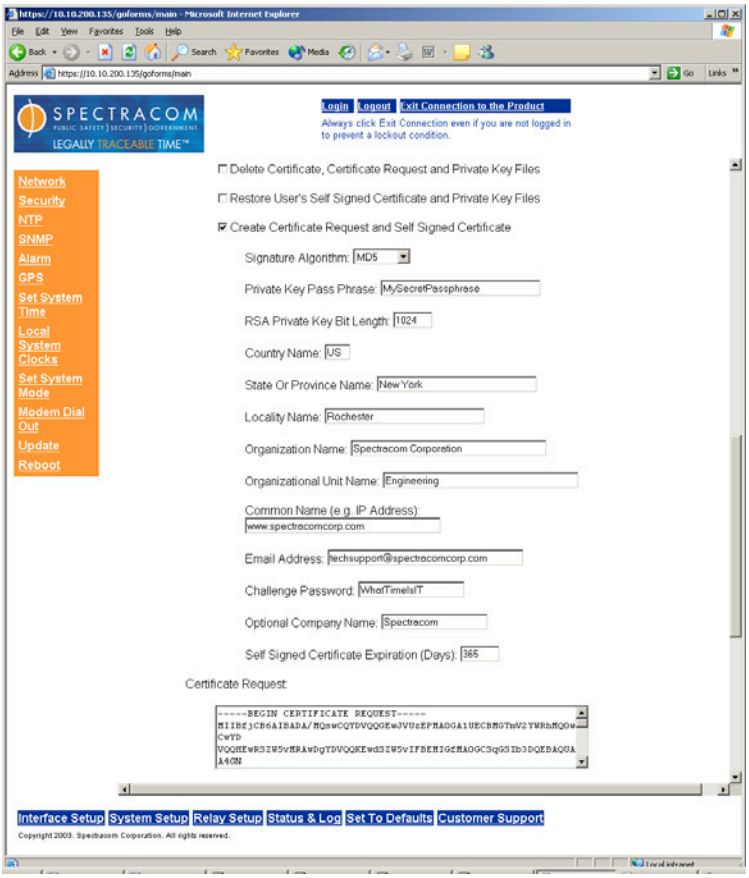


Figure 3-31: A new Certificate Request and Self Signed Certificate

The user can submit this certificate request to the company's Certificate Authority for a real verifiable, authenticable third party certificate. Until this certificate is received the user's self-signed certificate displaying the information shown above can be used.

The Master Clock web server will load this new self-signed certificate and private key after the user selects a few more web page options or when the user selects the "Exit connection to product" button at the top of the screen. The user will see a pop up window in Windows operating systems. The certificate and be installed or viewed using this pop up window. Other operating systems may vary in how they install and accept certificates. External Internet access may be required by your Certificate Authority to verify your third party certificate.

3.14.7 Installing Certificates

After your Certificate Authority issues you a Certificate you need to install it on the secure Spectracom product. Certificates may be installed via the web browser user interface and stored. Or they may be copied to the /sys/update directory using file transfer and installed using the web browser user interface.
A sample certificate installation using the Certificate text box on the web browser user interface is shown below.

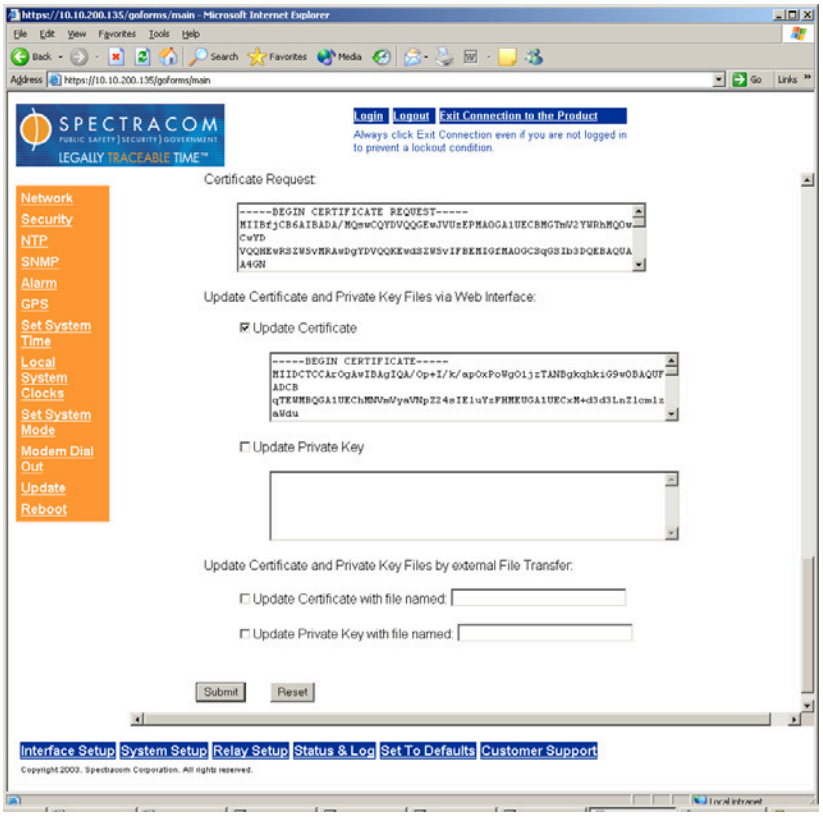


Figure 3-32: Installing a new Certificate

The user needs to cut and paste the certificate into the Update Certificate text box and select the checkbox. The user then enters submit at the bottom of the page and the current self-signed certificate is overwritten.

If the file transfer method is chosen FTP, SCP, SFTP may be used to copy the certificate text file to the /sys/update/ directory using any file name. The user then selects the "Update Certificate with file named" check box and enters the file name in the space. The user then enters submit at the bottom of the page and the current self-signed certificate is overwritten with the specified file name.

In both cases the secure Spectracom product's web server loads this new self-signed certificate and private key after the user selects a few more web page options or when the user selects the "Exit connection to product" button at the top of the screen.

3.14.8 Using Externally generated Certificates

The user is provided with another means to load certificates onto the secure Spectracom product supported. The certificate must be in PEM format.

The user may install the externally generated certificate using the web browser user interface. A sample certificate install is shown below.

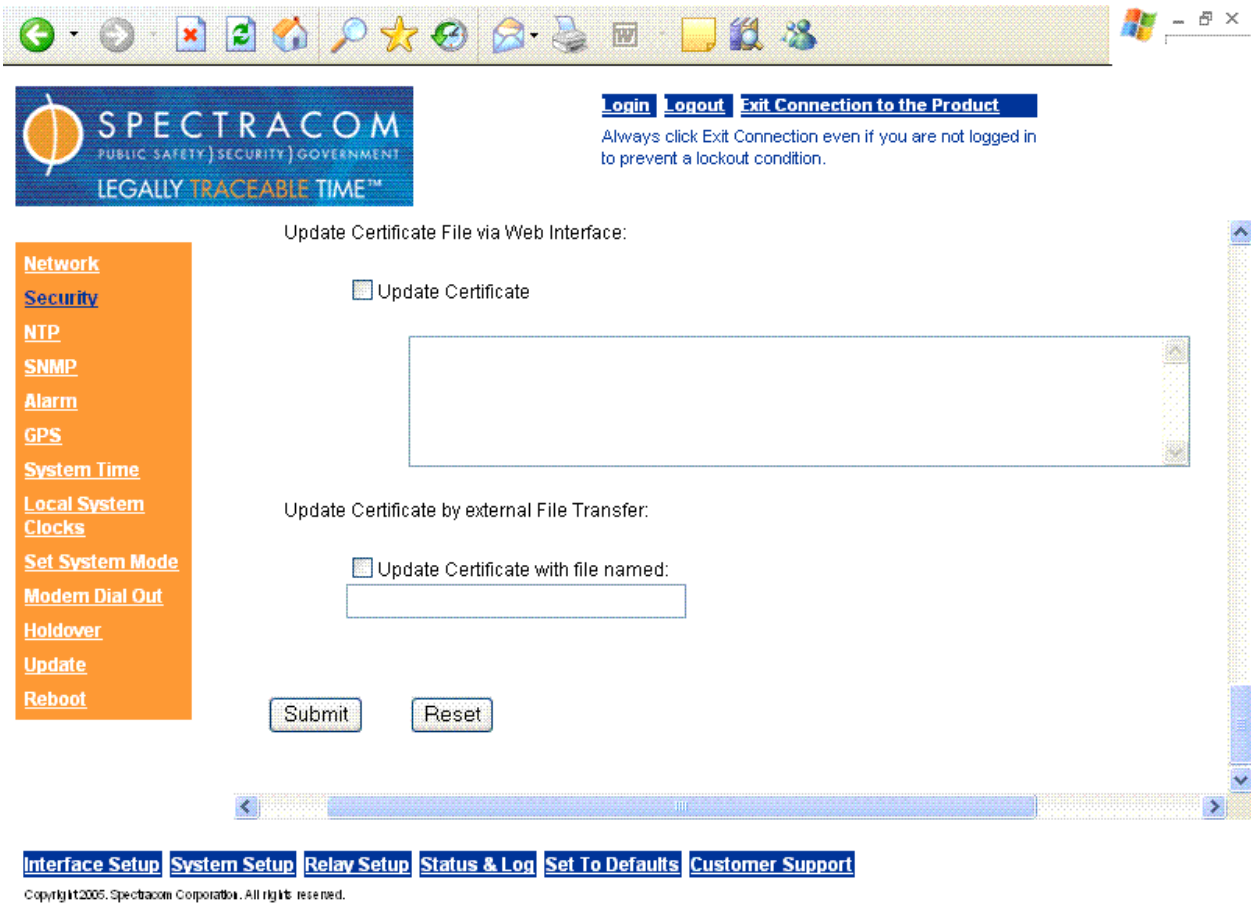


Figure 3-33: Using External Certificate

The certificate can also be installed using file transfer and the web browser user interface. The user simply needs to transfer the certificate file to the /sys/update directory using either SCP or SFTP. Once the file is transferred, the user simply selects the "Update Certificate with file named" checkbox and provides the file names. The user then enters the submit button.

In both cases the secure Spectracom product's web server loads this new self-signed certificate after the user selects a few more web page options or when the user selects the "Exit connection to product" button at the top of the screen.

To successfully use this means of certificate generation the user must correctly create a certificate which complies with the requirements of the currently used OpenSSL release.

3.14.9 What to do if you cannot get into a secure Spectracom Product

Spectracom assumes that the customer is responsible for the physical security of the product. Spectracom secure products are required to be locked in a secure enclosure, cabinet or room.

Unauthorized persons are not to be given access to the product nor should a serial cable and terminal program be attached unless the system administrator is configuring or performing maintenance.

If your company disables HTTPS, loses the system passwords, allows the certificate to expire, deletes the certificate the certificate and private keys and deletes the Host Keys or forgets the Passphrase access to the secure Spectracom product can become denied.

To restore access to your system you must utilize the setup port to restore the admin accounts default password. The admin account can then be used to enable HTTP using the “net HTTP” command. Contact Spectracom Technical Support for details on how to do this.

3.15 Signature Control for the frequency output

The rear panel 10 MHz output has the capability to be disabled upon assertion of an alarm condition. This feature is known as Signature Control. The Frequency Outputs web browser user interface page allows the user to observe the current state of the 10MHz Frequency output and configure the different Signature Control modes of operation. Refer to Figure 3-34 for more details.

The ON or OFF state of the 10MHz output is displayed on the web browser user interface screen. The Signature Control mode is selectable via a pull down menu. The user is provided with three possible configurations. These choices are described below.

None – No Signature control mode of operation. The 10MHz output is always on. The output will not be disabled if GPS reception is lost or a major alarm is present.

Major Alarm – The Signature control mode of operation disables the 10MHz output if a Major Alarm is active. When the Major Alarm is cleared, the 10MHz output is re-enabled.

Time Sync – The Signature control mode of operation disables the 10MHz output if a loss of Time Synchronization, which provides a stable 1PPS used for disciplining the 10MHz occurs. When loss of Time Sync has cleared, the 10MHz output is re-enabled.

Note: Oscillator disciplining is dependant upon a very stabile reference 1PPS input signal. Due to this, the Modem dial-out option (Option 3) available for the Model 9183 cannot be used for oscillator disciplining and hence does not result in enabling 10MHz frequency outputs when time sync is achieved via these time sources. The NetClock must be synchronized to GPS with a 3-D fix (minimum of four satellites) when the 10 MHz output is required to be disciplined for accuracy. Without a 3-D fix present and with Signature Control set to NONE, the frequency output will always be present but not disciplined for accuracy.

Because a window-mounted antenna will have difficulties maintaining at least four satellites continuously, the window-mount antenna, Model 8228, should not be used when disciplining of the 10 MHZ is desired. The antenna needs to be installed outdoors with a good view of the horizon.

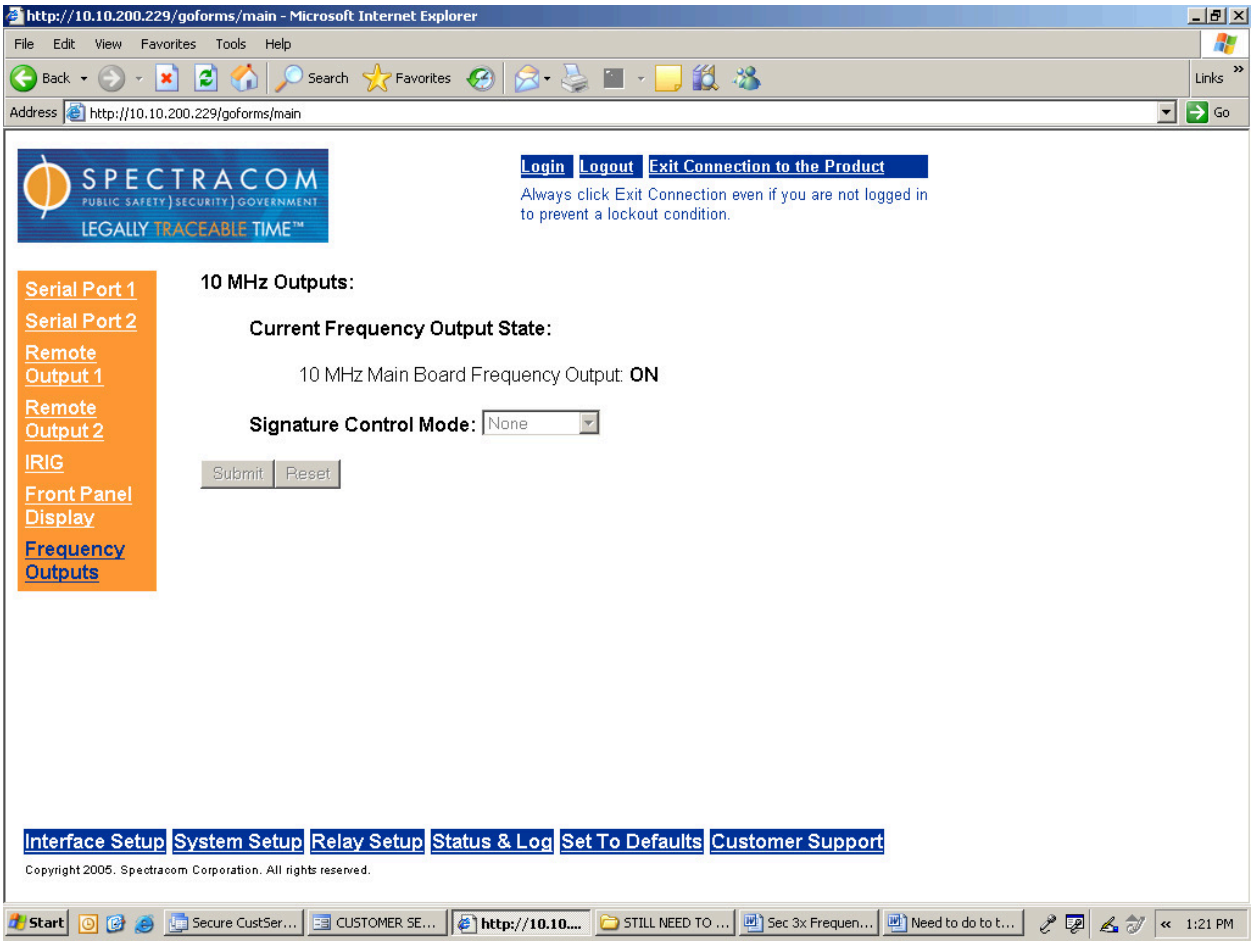


Figure 3-34: Signature Control configuration page

3.16 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 an 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).

3.16.1 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 browser user interface as administrator mode. Click on the "System Setup" link on the bottom blue bar to open the menu for system configuration. Click on the "SNMP" link on the left side of the screen to enter the SNMP setup page.

The SNMP configuration page consists of five main sections, followed by the submit button. The five sections (in order) consist of: SNMPv1 configuration, SNMPv2c configuration, Trap destination/version, trap selections and then SNMPv3. The descriptions of each of these sections are contained in the following.

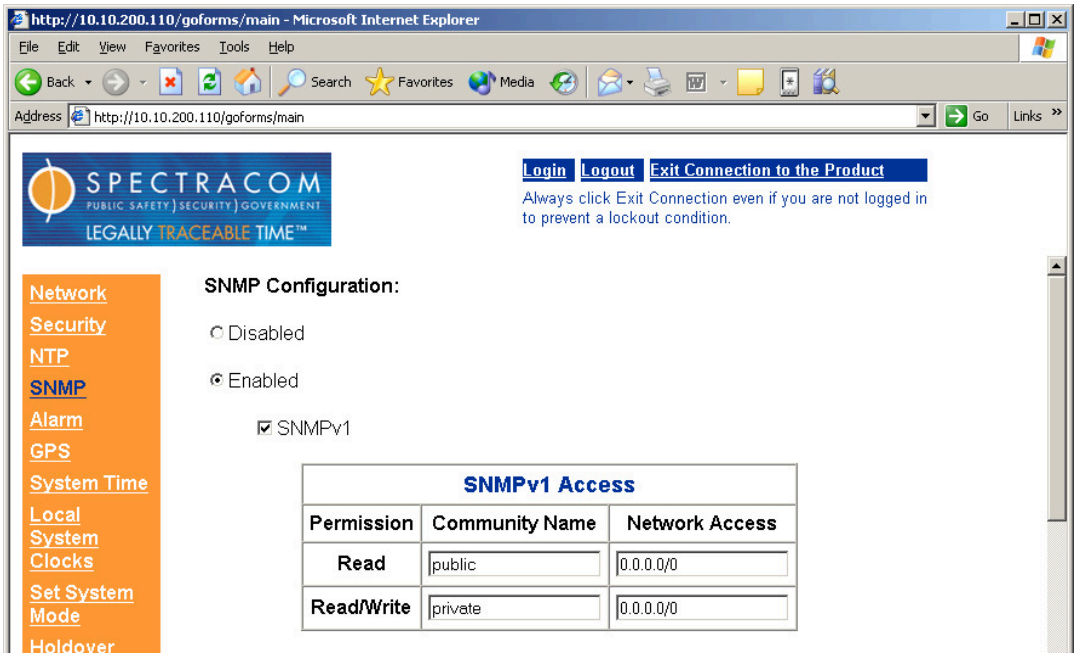


Figure 3-35: SNMPv1 Setup Screen

The radio buttons at the top of the page labeled "**Disabled**" and "**Enabled**" are used to determine if the SNMP agent is on or completely turned off.

The SNMP agent has a number of access schemes (SNMPv1, SNMPv2, SNMPv3) that can be individually enabled or disabled, depending on your specific needs. The check-box in front of each of the schemes is used to enable or disable that particular scheme. The schemes are described below.

SNMPv1 – By enabling this access scheme, SNMP network managers may use SNMP version 1 protocols to manage the device. A user-defined "Read" and a "Read/Write" community name used by SNMPv1 may be entered if desired.

Network access is used to restrict by "network IP address" who may query this SNMP agent. This feature is also known as "host restriction". If the user wishes to restrict SNMP access to one management station, say 192.168.0.1 then the network access should be set to "192.168.0.1/32". If the user wishes to allow any management station on the 192.168.0.X with subnet mask 255.255.255.0, then Network Access would be set to "192.168.0.0/24".

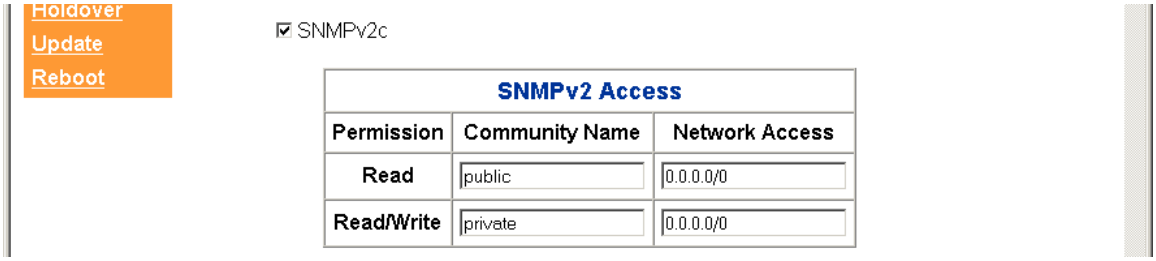


Figure 3.16-2: SNMPv2 Setup Screen

SNMPv2c – By enabling this access scheme, SNMP network managers may use SNMP version 2 protocols to manage the device. A user-defined "Read" and a "Read/Write" community name used by SNMPv2c may be entered if desired.

Network access is used to restrict by "network IP address" who may query this SNMP agent. If the user wishes to restrict SNMP access to one management station, say 192.168.0.1 then the network access should be set to "192.168.0.1/32". If the user wishes to allow any management station on the 192.168.0.X with subnet mask 255.255.255.0, then Network Access would be set to "192.168.0.0/24".

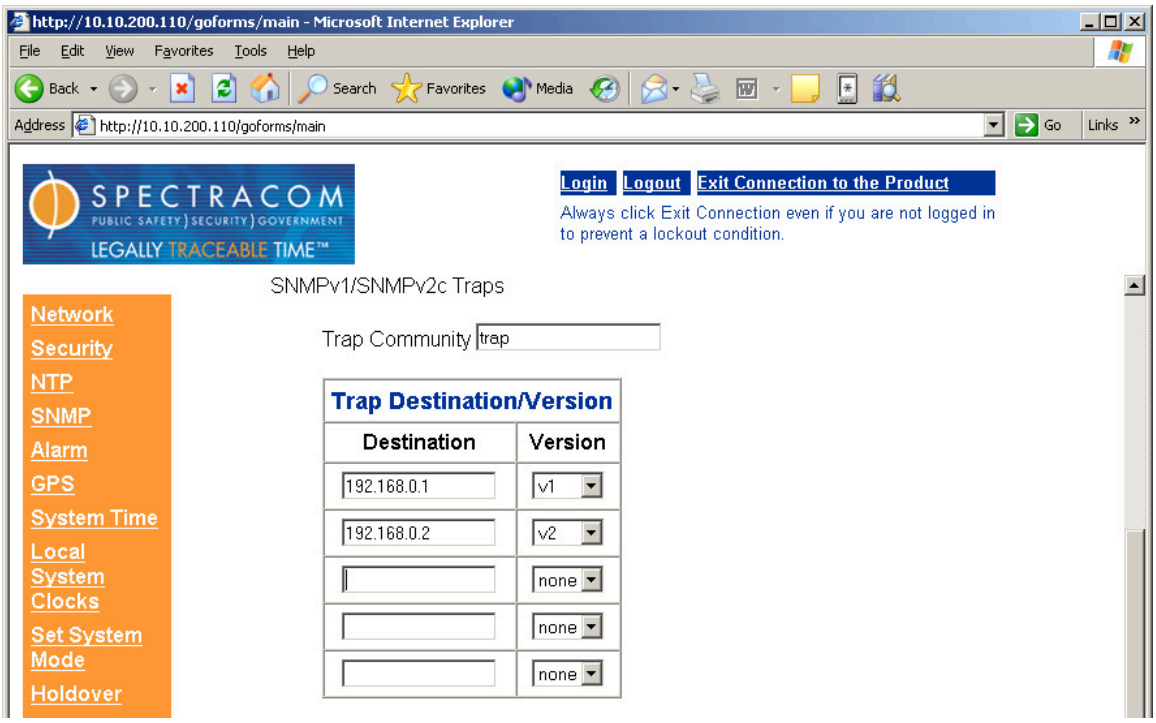


Figure 3.16-3: SNMP Trap destination Setup Screen

Further down the page is the configuration of the SNMPv1 and SNMPv2c traps. The "trap" community name is used for both v1 and v2c traps. The destination table should be used to define which SNMP managers should be sent traps and which version they should receive (v1 or v2c). Up to five different traps destinations and their versions may be entered in the table. This feature is to support a "distributed SNMP Manager scenario". For example, on a Wide Area network, traps can be sent to different geographic locations to coordinate the different Time zones and normal working hours of personnel.

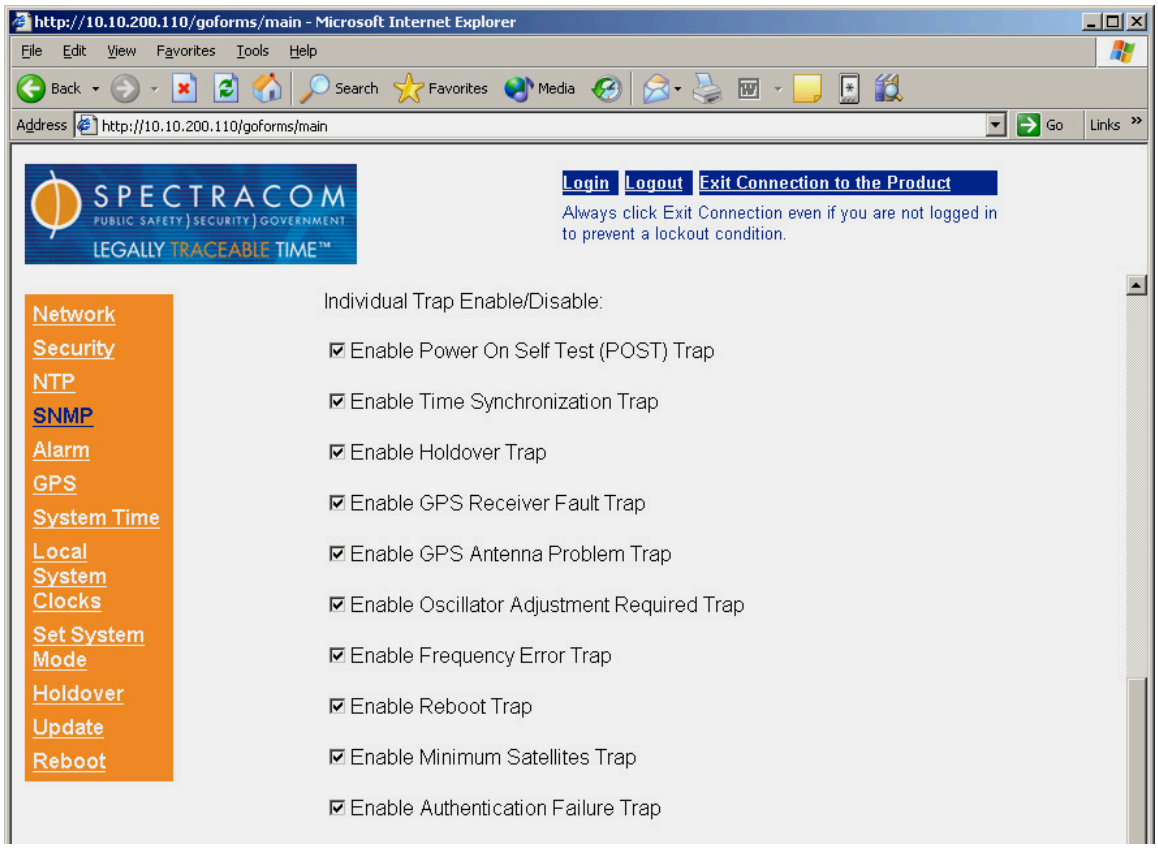


Figure 3.16-4:Trap selection Setup Screen

The “Individual Trap Enable/Disable” section allows the user to enable/disable any subset of the unit’s available traps. This list contains all of the available traps that may be sent from the NetClock. Unchecking the box in front of each trap will prevent that particular trap from being sent.

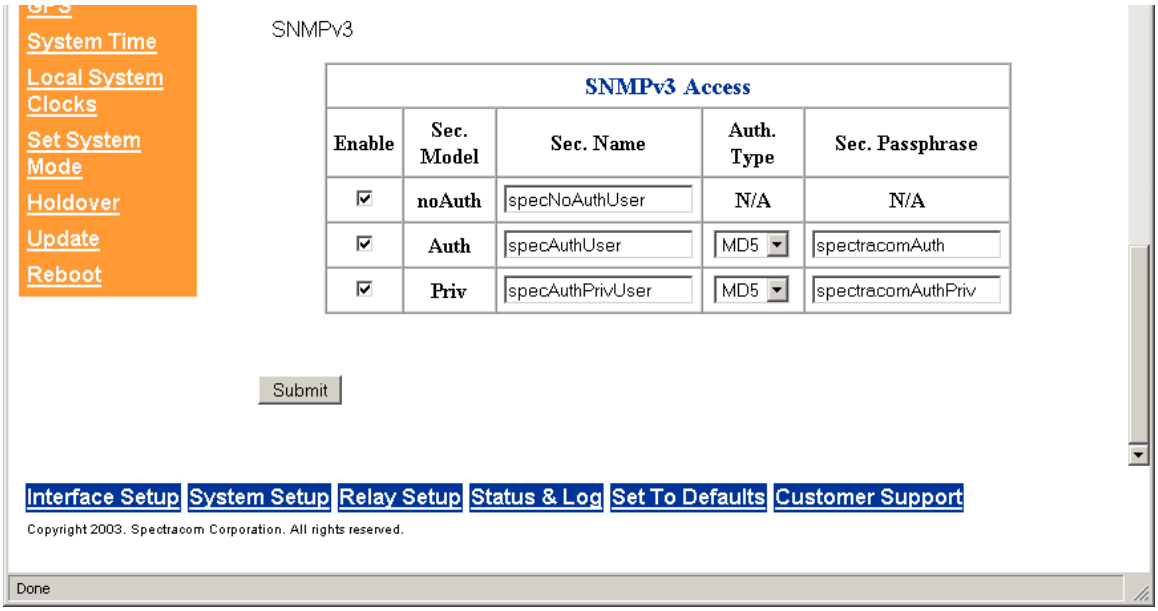


Figure 3.16-5: SNMPv3 Setup Screen

The last section is for SNMPv3 configuration. This section allows the user to enable/disable any one of the three SNMPv3 security models. These models are described below:

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.

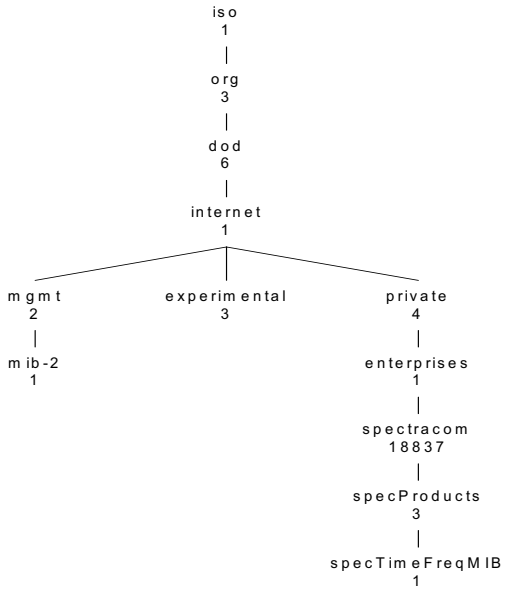
SNMPv3 (auth) – By enabling this access scheme, SNMP network managers may use SNMP version 3 protocol to manage the device. This level of SNMPv3 has you select a form of PDU authentication (MD5 or SHA) but does not use DES encryption. You may specify your own user name and pass phrase for this level 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 products that have the security option installed.

When SNMP is fully configured as desired, click the submit button.

3.16.2 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.



3.16.3 SNMP Support

Spectracom's private enterprise MIB can either be obtained from the Spectracom Customer Service department via an email or it can also be FTP'd (File Transfer Protocol) out of the NetClock using an FTP agent such as Microsoft FTP, CoreFTP or any other shareware/freeware FTP program.

To obtain the MIB file via FTP, using your FTP program, login to the administrative mode with the admin level password. Change the file transfer mode to "binary". Navigate to the "MIB" directory which is located on the root directory. The Spectracom MIB files are located in this directory. There is a Global (generic) MIB file and a NetClock specific MIB file called "Time and Frequency". FTP the files to your desired location on your PC for later transfer to the SNMP Manager. The MIB files may then be compiled onto the SNMP Manager.

Note: When compiling the MIB files, some SNMP Manager programs may require the MIB files to be named something specific other than the current name for the files**.** The MIB file names ("Global" and "Time and Frequency") may be changed or edited as necessary to meet the requirements of the SNMP Manager. Refer to the SNMP Manager documentation for more information on their requirements.

3.17 System Status

The System Status web browser user interface page provides the user with the software revision levels, the current time sync status, the results of internal unit testing as well as the features and options that are currently enabled and disabled.

To navigate to the System Status page, click on the Status and logs page on the bottom blue bar and then on System Status on the left orange bar. The System Status page cannot be edited so you do not need to be logged is as config or admin modes when viewing this page. This page is not dynamic. If a status change occurs while this page is open, the change will not be displayed. To view the current status, exit and then re-enter this page.

The System Status page consists of four main sections. A sample of each of these sections and a description of the contents of each section follows:

3.17.1 Dynamic System Information

Uptime: 0 years, 0 days, 1 hours, 54 minutes, 1 seconds
Current internal temperature: 27.75 C (81.95 F)
Major Alarm is (OFF)
Minor Alarm is (OFF)
Time Sync status: In Sync
Time Source: GPS

The **Dynamic System Information** section contains the elapsed time that the unit has been powered-up for, the internal temperature of the unit, the status of the major and minor alarms, the current Time Sync status and the current external reference identifier.

Time Source:
The Time source field contains the current source for time input. The possible inputs are as follows:

None – No Time Source has been found after startup.

GPS – The GPS receiver is the Primary Time Source for the Models 9183 and 9189.

Modem – When Option 3 is installed, the Modem maybe used as a Primary Time Source or Secondary (backup) Time Source to GPS for the Model 9183.

User – The Time Source is the result of the user setting the time from the System Setup/System Time web browser user interface page when no Time Source is present.

3.17.2 Static System Information

Product Name is Spectracom Corp. Model 9183
Application Name is 91XX
Application Rev is 2.3.0
Application Date is 07/28/2005
SSH Rev is OpenSSH_3.7.1p2, SSH protocols 1.5/2.0
SSL Rev is OpenSSL 0.9.7d 17 Mar 2004
Boot Monitor Rev is 2.3.0
Unit's Serial Number: 886
GPS Receiver Serial Number: P07ROY 2.1
MAC Address: 00:0c:ec:00:03:76

The **Static System Information** section of the System status page provides the software revisions, the NetClock's Serial Number and the MAC address.

3.17.3 System Test Results

PCB Test	PASSED (PCB rev: 5)
PCC Test	PASSED (PCC rev: 3)
CSL Test	PASSED (CSL rev: 14)
RTC Test	PASSED
GPS Startup Self-Test	FAILED (Antenna UC)
GPS Antenna Sense	PASSED
Modem Test	CONSOLE MODE
Temp Sensor	PASSED
IRIG Test	PASSED (1.02)
Serial Port 1	PASSED (2.03)
Serial Port 2	PASSED (2.03)
Remote Port 1	PASSED (2.03)
Remote Port 2	PASSED (2.03)
Front Panel LCD 1	PASSED
Front Panel LCD 2	PASSED

The **System Test Results** section contains the results of the internal tests that are run. These test are not complete checks of the entire paths (For example, the Serial port may pass even though it has been damaged by a surge).

GPS Startup Self-Test
The GPS Startup Self-Test will indicate the status of the antenna, antenna cable and the GPS receiver at the time of power-up only. If the antenna cable was not connected, shorted or open at the time of power-up, and/or if there is a problem with the GPS receiver or antenna or both at the time of power-up, this test will indicate FAILED. "Antenna UC" means the antenna was not connected and "Antenna OC" indicates there was a short in the cable at the time of power-up. "Antenna NV" means an unknown antenna problem existed at power-up. "GPS & Antenna" means that both GPS receiver and Antenna problems were detected at power-up.

GPS Antenna Sense
The GPS Antenna Sense is a current status of the antenna, antenna cable and the GPS receiver. If the antenna cable is currently not connected, shorted or open, and/or if there is a problem with the GPS receiver or antenna or both, this test will indicate FAILED. "Antenna UC" means the antenna is not currently connected and "Antenna OC" indicates a short in the cable. "Antenna NV" means an unknown antenna problem. "GPS & Antenna" means that both GPS receiver and Antenna problems were detected.

Modem Test (Applicable only to units with Option 3 - Modem installed):
The Modem Test will indicate "Console Mode" if the Serial Setup Interface is set to Console mode instead of Modem mode. This indicates that the modem is not currently being used. If the modem feature is desired, in the modem configuration page, change the mode to the Modem mode.

When the NetClock initially boots up, the mode is set to Serial Setup Interface. When the mode is set to Modem and before every modem dial-out call, the modem is sent a command. If the unit gets a response from the modem, the field is set to PASSED. If the unit gets no response or a bad response from the modem, then the field is set to FAILED and the reason is indicated as shown below:
Reasons:

Not Found – There is no modem connected, the modem is incorrectly connected, or it not turned on.

Modem Error – The modem gave a response indicating an unspecified problem.

3.17.4 System Features and Options

Security	ENABLED
Modem	ENABLED
Serial Port 1	ENABLED
Serial Port 2	ENABLED
Remote Port 1	ENABLED
Remote Port 2	ENABLED
IRIG Output	ENABLED
Front Panel Display	ENABLED
Relays	ENABLED
Oscillator Disciplining	ENABLED
10 MHZ Frequency Output	ENABLED
NTP Server	ENABLED
TCXO Oscillator	ENABLED
Motorola Oncore M12+ Timing GPS	ENABLED

The **System Features and Options** section provides the current status of all the features and options that are available for your particular NetClock. Features that are currently turned on will indicate "ENABLED". Features that indicate "DISABLED" are not enabled. However, the disabled features may be "enabled" after the original purchase. If an option, which is enabled, fails to correctly initialize and become ready to be used its status is **ERROR**.

Option 3 can be enabled in the field (Options 4 and 5 must be purchased with the unit when it is initially ordered). With the future purchase of the Modem option (Option 3), we will provide a "key hash" that will enable the feature to be turned on. Please contact our Sales department to purchase the option.

The purchase price of the modem option includes the cost for the modem as well as the key to enable the feature. The modem selection is very limited in compatibility. Not all available modems are compatible with the Model 9183 (Must be configured as Hayes AT) so we will supply you with a modem when the option is purchased. If the modem option was not initially purchased, contact our Sales department to purchase the modem option. Refer to Section 8.1 for more information regarding Option 3.

3.18 System Time

The System Time page provides a means to manually set the time for test purposes only. It also provides a handy and simple process to determine the time that the NetClock currently is set to. This feature reads the information that the NetClock is providing to the external equipment that is syncing to this device.

To navigate to the System Time page, click on System Setup on the bottom blue bar and then on System Time on the left orange bar. Refer to **Figure 3-36: System Time** for more details. **Note:** You must be logged into the administrator mode to make any changes to this page.

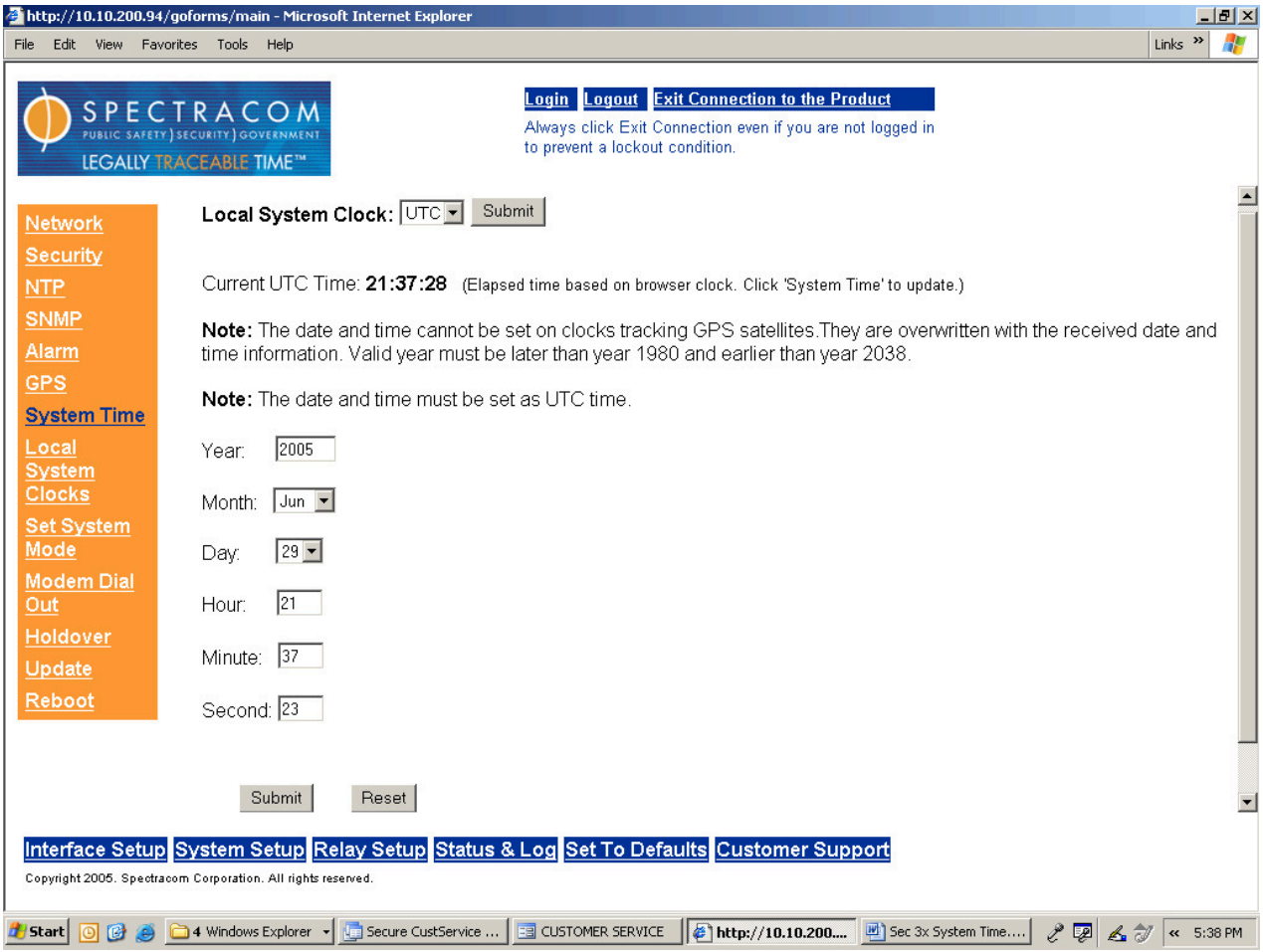


Figure 3-36: System Time

The top section of the System Time page provides the ability to set and determine the current UTC or local time that the NetClock is providing to the other devices connected to it.

Local System Clock:
This field determines if the time output is displayed as UTC or one of the 5 possible local times that can be created using the Local System Clocks screen. When a Local System clock is selected here, the time displayed below it will be displayed as configured in that particular local System Clock (i.e. Eastern time with automatic DST correction). After choosing the desired local clock from the drop-down, press the Submit button to accept the change. Click System Time again to bring the page back for viewing.

Current UTC Time: 17:59:10 (Elapsed time based on browser clock. Click 'System Time' to update.)
This line contains the current time displayed as configured in the Local System Clock dropdown. The name in the line will indicate either UTC or the name of the selected local clock. Initially, this is a free-running clock that may or may not be the correct time (The Time displayed isn't automatically corrected every second). To determine the current time at a particular moment, press System Time on the left orange bar. Pressing this button each time will cause the time displayed to be updated to the current time.

The bottom portion of the System Time page provides a means of manually setting the time and date. However, when the time and/or date is manually set by the user, the NetClock will not be synchronized and indicators in all of the outputs will be flagged as unsynchronized. Most software programs including NTP will ignore the NetClock when these status messages indicate that the NetClock is not synchronized.

When manually setting the time of the NetClock, the time is entered as UTC- not your local time. This means the time is not corrected for either Local Time or DST correction. Entering your local time will cause a several hour error in the NetClock outputs. The amount of error will depend on which Time Zone you are located in and whether we are currently in DST or in Standard time.

Manually setting the time of the NetClock is not recommended as the outputs will likely be unusable because of the time sync status characters in the outputs. When an external reference is detected, the time and date will be automatically corrected to the real values and the manually set values will be overwritten. When this occurs, a log entry will be made in the Operational log indicating the amount of correction that was made from the manually set time. This log then shows if the time was ever manually set and then corrected by another external reference.

Note: Manually setting the time while synchronizing to the Option 3 Modem will cause loss of Time Sync which will automatically trigger a dial-out call to attempt to re-sync. Manually setting the time while synchronizing to GPS will immediately set the time back to the correct time.

3.19 Variable Holdover:

The time interval between the loss of the primary external reference and the moment that the NetClock declares loss of Time Sync is known as holdover. While the unit is in the holdover mode, the time outputs are derived from an internal oscillator. Because of the internal oscillator, accurate time can still be derived even after the primary reference is removed. The more stabile the oscillator is without an external reference, the longer this holdover period can be. The benefit of holdover is that time sync and the availability of the time outputs is not immediately lost when the reference is no longer available.

The NetClock has a user configurable variable holdover period so that it can be adjusted for personal requirements and desires. A user can change the length of time that a unit waits in the holdover mode before loss of time sync. The holdover can be defined by a specific number of hours to wait, such as 4 hours and 30 minutes. It can also be defined by the estimated error. However, the estimated error feature is only enabled for the OCXO (Option 5) and Rubidium (Options 4) products.

The estimated error rates for each oscillator are listed below. These are used when displaying the current estimated error for the user and when calculating a new holdover length (Option 4 and Option 5 oscillators only).

Oscillator	Option	Estimated Error Rates	Time to reach 2 ms
TCXO	Standard	1.0 milliseconds / hour (nominal)	2 hours (typical)
TCXO	Standard	7.2 milliseconds / hour (worst case)	17 minutes*
OCXO	Option 5	72 microseconds / hour (nominal)	28 hours
Rb	Option 4	0.18 microseconds / hour (nominal)	463 days

Table 3-6: Estimated oscillator error rates

Note: The TCXO Error rate is a worst-case estimate and not typically this value. The nominal value assumed has been 1 millisecond / hour yielding 2 hours holdover times. The OCXO and Rb oscillators use the nominal values for estimated error rate to calculate error at the end of holdover on the web browser user interface. The TCXO does not estimate error for holdover. But if it did, it probably should use the nominal value, which is more typical. Typically the error rates for a disciplined oscillator at 25 degrees Celsius will be lower than these values.

Limits on the minimum and maximum length of allowable holdover have been placed on each oscillator as shown below in Table 3-7.

Oscillator	Minimum Length	Maximum Length
TCXO	15 minutes	24 hours
OCXO (Option 5)	15 minutes	30 days
Rb (Option 4)	15 minutes	730 days (2 years)

Table 3-7: Minimum and Maximum allowable holdover values

If the user sets the length below or above the limits or if the error is too small or large, they will be notified that the current setting is out of bounds.

To navigate to the Holdover configuration page, click on System Setup on the bottom (blue) bar, then click on Holdover in the left (orange) page. Configuration of this page requires admin level login.

3.19.1 Setting the variable holdover value for a TCXO oscillator

The user interface for the TCXO looks like:

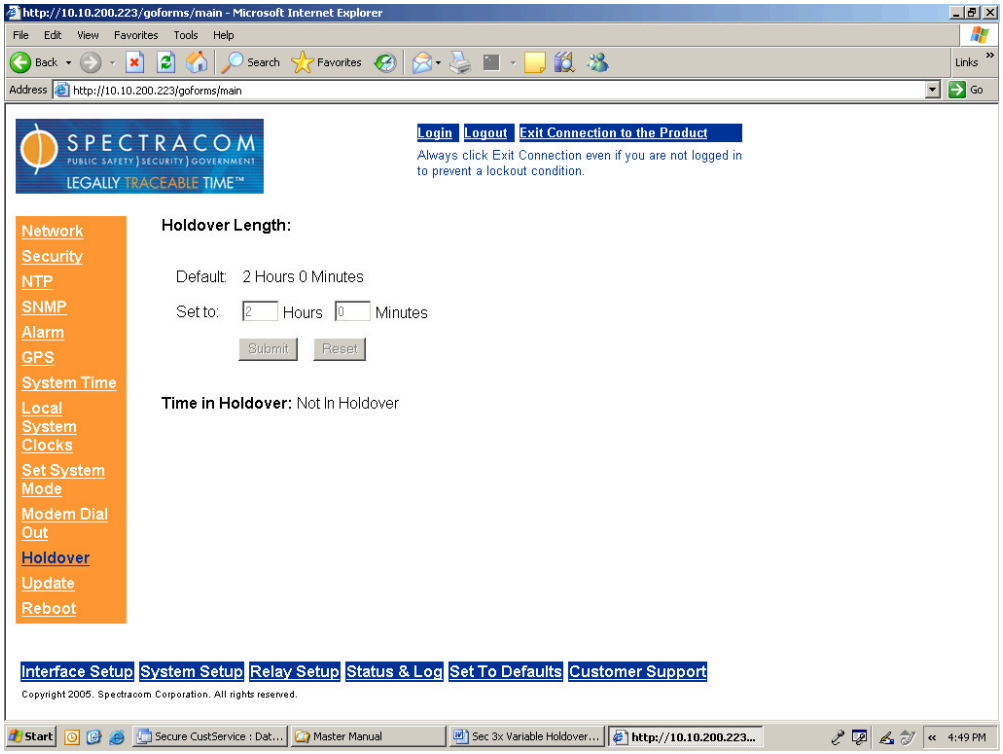


Figure 3-37: TCXO variable holdover configuration

Using the "Hours" and "Minutes" adjustable boxes, the user can set the maximum time for the holdover period. If the length is set to a value greater than 24 hours and 00 minutes, the NetClock will respond with "**Could not set holdover time. Please ensure that holdover times are greater than 15 minutes and less than 24 hours 0 minutes.**" Additionally, if the user sets this holdover time to less than the dial-out time interval for the modem (If option 3 is installed), the unit may have periods where it is in the unsynchronized state.

If the unit is currently in sync, the changes to the holdover period will take effect immediately. If the unit is in holdover, these changes will not take effect until the next holdover period. To force the changes to take effect immediately, reboot the NetClock.

3.19.2 Setting the variable holdover value for an OCXO or Rubidium oscillator

The user interface for the OCXO and Rubidium looks like:

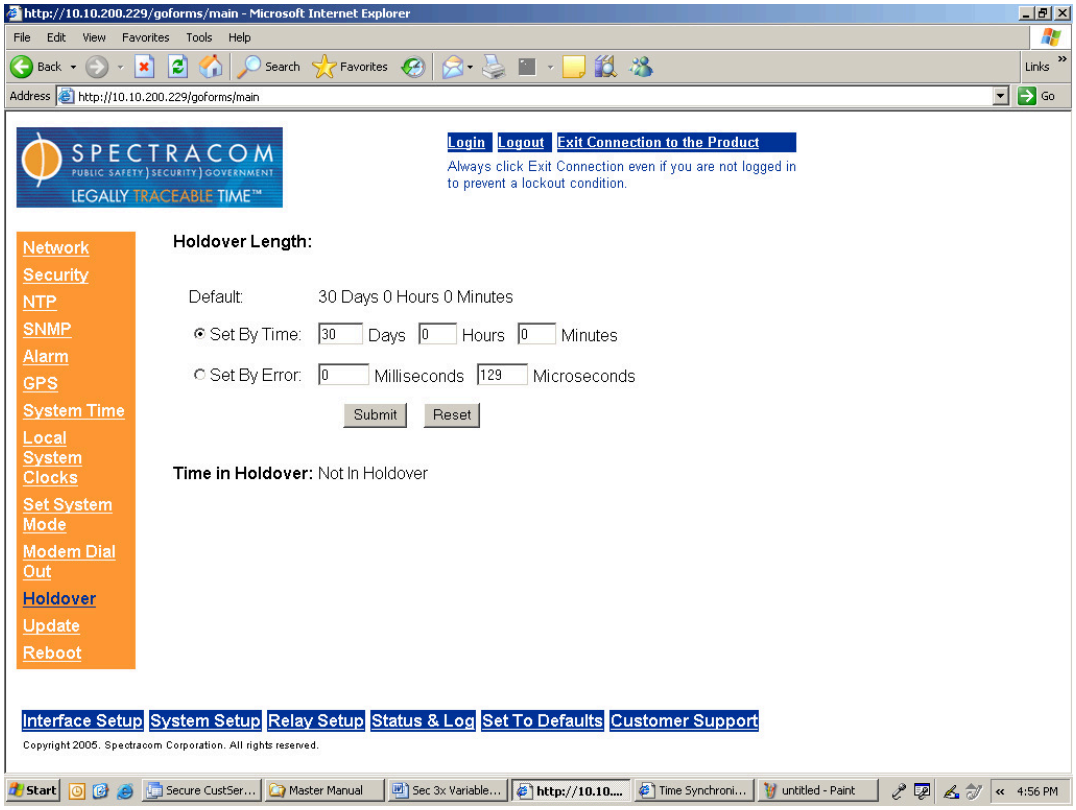


Figure 3-38: OCXO and Rb oscillator variable holdover configuration

Set by Time and Set by Hour
Using the radio option, the user can select whether the length of the holdover period is set by the elapsed time or the estimated error entered.

If the length is greater than 30 days, the user will be given a warning that leap seconds could be missed while in holdover if they do not have a modem as backup. Missing a leap second will cause a one second error in the NetClock outputs until the leap second change has been read by an external reference such as the GPS or modem feature. Additionally, if the user sets the holdover time to less than the dial out time for the modem, they will be warned that the unit may have periods where it is in the unsynchronized state.

To use the Set by Error feature, enter in the maximum desired estimated error that you want the unit to have before it declares it is out of sync and the outputs are no longer used by other devices. The higher this value, the longer the holdover period will be.The smaller this value, the

shorter the holdover period will be. To calculate the approximate time of holdover period from a desired error value, from the estimated error rate table, determine the estimated error rate for your particular oscillator and divide this value into the maximum desired value. The answer will be approximate number of hours that the unit will be able to run in holdover mode for the desired error.

If the unit is currently in sync, the changes will take effect immediately. If the unit is in holdover, the changes will not take effect until the next holdover. To force the changes to take effect immediately, reboot the NetClock.

Time in Holdover
Time in Holdover displays either the amount of time that the NetClock has been in the holdover mode, or displays a phrase that the unit is not currently in the holdover mode. If the unit is currently in the holdover mode (Lost external reference but the unit is still “synchronized”), this field will show the number of days, hours, minutes and seconds that the unit has been in the holdover mode (Elapsed time from the last good external reference).

If the unit is not currently in holdover mode because it either currently receiving an external reference or because the variable holdover period has expired and the unit is no longer “synchronized”, the phrase "**Not In Holdover**" is displayed instead.

4 Operation

4.1 Front Panel

The front panel of the NetClock consists of one Ethernet connector which has two small indicator lamps, two main status LED's and two LCD displays. The two status lights are "Sync" and "Power". The LCD's are configurable to display various time, data, version information formats. Refer to Figure 4-1 for a picture of the front panel.

The Spectracom NetClock Master Clock has two main status LED's present on the front panel. These status lights provide the user with the indication that power is applied to the unit (Power LED) and that the NetClock is currently synchronized or not synchronized (Sync LED). The power light will be blank if power is not applied or green if power is applied. The Sync light has many states to indicate the current status of the unit.

The Ethernet connector provides an interface to the network for NTP synchronization and to obtain access to the Web Browser. The Ethernet connector has two small indicator lights just above the connector. These lights are known as Good Link (Green LED) and Activity (Orange LED). The Good Link light indicates a connection to the network is present. The activity light will blink when network traffic is detected.

The states of the Power, Sync and Ethernet LED's are listed in Section 4.1.1.

Figure 4-1: Front panel display

4.1.1 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	Synchronized to GPS. Time is valid and within the Locked to GPS accuracy specs.
		Blinking Green	Holdover mode. Not synchronized to GPS but time is still within Holdover accuracy specs. Also indicates the unit is synchronized with the optional dial-out modem (Option 3).
		Yellow On	No longer synchronized 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 detected. 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 Rear Panel

The rear panel provides several different outputs that are available for interfacing the NetClock to various systems as well as a means of initially configuring the unit's network settings. The rear panel also has a power jack for the power input, a connection for the GPS antenna and relay contacts for alarm monitoring and event alerts. Refer to Figure 4-2: Rear panel illustration for a drawing of the rear panel.

The **GPS Antenna** connection is an "N" type connector for the GPS input from the antenna.

The **power jack** is the input for the DC power.

There are three configurable alarm/event relays (**Relays 1, 2, 3)** available for remote alerts and monitoring.

The **Serial Setup Interface** provides network and output port configuration capability.

The two RS-485 connectors (**RS-485 ports 1 and 2**) provide an RS-485 data output for synchronizing devices that accept an RS-485 input, such as wall display clocks and add-on Model 9188 Ethernet Time Servers.

Serial Comm 1 and **Serial Comm 2** are "DB9 female" connectors that provide RS-232 data output to devices that can accept an RS-232 input for synchronization.

IRIG is a BNC output that provides an IRIG signal for synchronizing certain model voice recorders.

1PPS is a BNC output providing a once-per-second squarewave output.

FREQ OUT is a BNC output providing a 10MHz sinewave output.

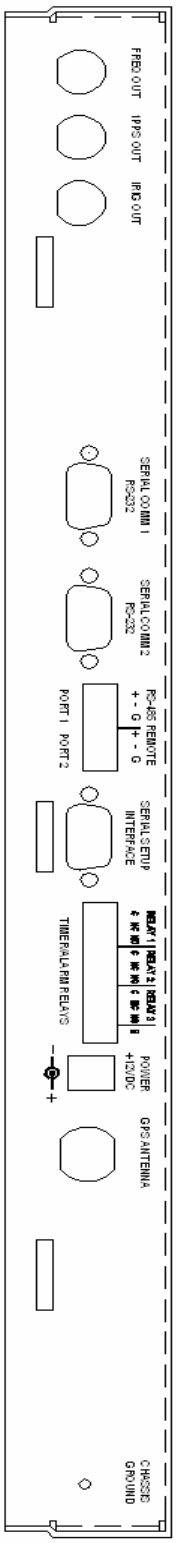


Figure 4-2: Rear panel illustration

4.3 Leap Second occurrence

4.3.1 Reasons for a Leap Second correction

A **Leap Second** is an intercalary, one-second adjustment that keeps broadcast standards for time of day close to mean solar time. Leap seconds are necessary to keep time standards synchronized with civil calendars, the basis of which is astronomical. They are used to keep the earth's rotation in sync with the UTC time.

If it has been determined by the International Earth Rotation and Reference Systems Service (IERS) that a Leap Second needs to applied, this time correction occurs only at the end of a UTC month, and has only ever been inserted at the end of June 30 or December 31. A Leap Second may be either added or removed, but in the past, the leap seconds have always been added because the earth's rotation is slowing down.

Historically, Leap seconds have been inserted about every 18 months. However, the Earth's rotation rate is unpredictable in the long term, so it is not possible to predict the need for them more than six months in advance.

The NetClock can be alerted of impending leap seconds by either of the following methods:

1. GPS Receiver – The GPS satellite system transmits information regarding a Leap second adjustment at a specific Time and Date an arbitrary number of months in advance.
2. Modem – (Applicable to only units with Option 3 Modem installed). During a modem dial-out call, the call service indicates that a Leap second adjustment at the end of this current calendar month will occur.

4.3.2 Leap Second alert notification

The NetClock will announce a pending Leap Second adjustment by the following methods:

1. Data Formats 2 and 7 on the Serial and Remote Ports contain a Leap Second indicator. During the entire calendar month preceding a Leap Second adjustment, these Formats indicate that at the end of the current month a Leap Second Adjustment will be made by having a 'L' rather than a ' ' (space) character in the data stream. Note that his does not indicate the direction of the adjustment as adding or removing seconds. These formats always assume that the Leap Second will be added, not removed.
2. NTP Packets contain a Leap Indicator Bit. In the 24 hours preceding a Leap Second Adjustment, the Leap Indicator Bits (2 bits) which normally are 00b for sync are 01b (1) for Add a Leap Second and 10b (2) for remove a Leap Second. The bit pattern 11b (3) indicates out of sync and in this condition NTP does NOT indicate Leap seconds. The Sync state indicates leap seconds by indicating sync can be 00b, 01b, or 02b.

Important Note: It is the responsibility of the client software utilizing either the Data Formats or NTP time stamps to correct for a Leap Second occurrence. The NetClock will make the correction at the right time. However, because computers and other systems may not utilize the time every second, the Leap second correction may be delayed until the next scheduled interval, unless the software properly handles the advance notice of a pending Leap Second and applies the correction at the right time.

3. The Dynamic System Information box in the "System Status" page located under the web page of "Status and Logs" will display a Leap Second Status box indicating +1 or -1 Leap second adjustment at the end of the month to users during the entire calendar month preceding the actual adjustment. Refer to Figure 4-3 and Figure 4-4.

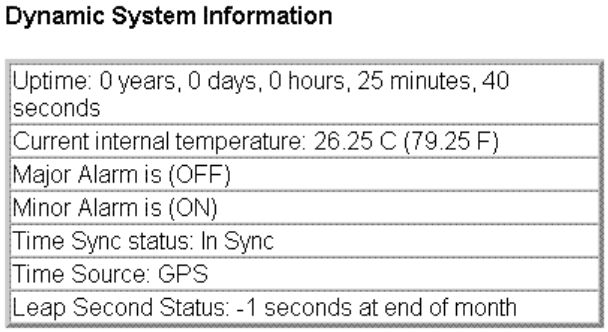


Figure 4-3: Negative Leap Second indication

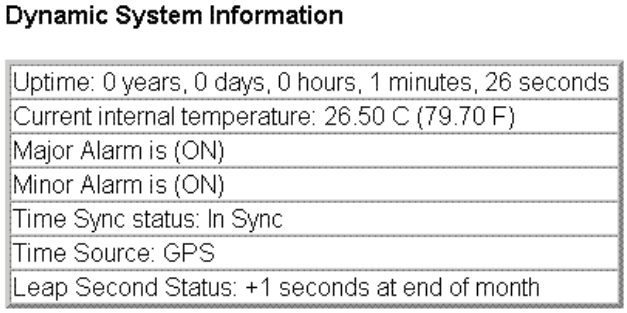


Figure 4-4: Positive Leap Second indication

4.3.3 Sequence of a Leap Second correction being applied

1. The following is the time output sequence that the Model 9183 will utilize to apply the Leap second at UTC midnight (Not local time midnight. The Local time at which the adjustment is made will depend on which Time Zone you are located in).

   A) Sequence of seconds output when adding a leap second:

   56, 57, 58, 59, 60, 0, 1, 2, 3, …

   B) Sequence of seconds output when removing Leap seconds:

   56, 57, 58, 0, 1, 2, 3, 4, …
2. An entry will be made in the Operational log that the time was adjusted for a Leap Second.

A) An example log entry for a Positive Leap Second is as follows:

```
TIME= 23:59:59 DATE= 2005-12-31
System Clock Service
Leap second inserted at end of month.
```

B) An example log entry for a Negative Leap Second is as follows:

```
TIME= 23:59:59 DATE= 2005-12-31
System Clock Service
Leap second removed at end of month.
```

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 5.3, GPS reception troubleshooting.
Flashing Green	(Known as holdover mode) Successfully synchronized with optional dial-out modem (Option 3). OR Recently stopped Tracking satellites (The unit has not timed-out of hold-over mode).	(Time is still valid. Other devices will still be synchronized). This is a normal indication when the unit is synchronized via the optional dial-out modem (Option 3). If not using the optional dial-out modem, refer to section 5.3, GPS 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 synchronized). Refer to section 5.3, GPS reception troubleshooting. Review the Alarm and Qualification logs. If the modem dial-out is enabled, also need to verify modem operation as well. The modem should have prevented this from occurring.
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 5.4, GPS 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

Table 5-1: Status of Front Panel Power and Sync lampsFront 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 NetClock but the Gold Link indicator on the HUB/Switch is not lit.	The NetClock and the HUB/Switch are not communicating at the correct port speed.	If the Hub/switch is set to auto, power cycle the NetClock 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 NetClock	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 NetClock 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.

Table 5-2: Status of Front Panel LAN connector

5.2 Verify operation of a Serial port

If you want to verify the operation of a Serial port output, you can use a straight thru standard serial cable and a terminal emulator such as HyperTerminal or Procomm to view the output data.

For RS-232 cable information as well as information to configure HyperTerminal, refer to http://www.spectracomcorp.com/support/applicationNotes.php.

To verify the operation of the Serial port, configure the terminal emulator program with the same baud rate as the port is configured for (such as 9600 baud). With the serial cable connected to the Serial port and with the port configured as "Request character" mode and the character set to a capital letter "T", each time a Capital letter "T" is pressed on the keyboard, the port will respond with a time stamp (any other character other than a "T" will respond with a "*").

If the port is configured as "multicast" mode, with the serial cable connected, the time stamp should be displayed on the PC every second.

If the time stamp is displayed on the PC, the Serial port is functioning. If the time stamp is not displayed, verify the serial cable, the port configuration for the correct baud rate and the configuration of the terminal emulation program. Refer to the Spectracom Application Note regarding HyperTerminal at:
http://www.spectracomcorp.com/support/pdf/using_hyperterminal.pdf.

5.3 Verify operation of a Spectracom TimeTap

If you want to verify the operation of a Spectracom TimeTap, follow the same process as Section 5.2, but instead of connecting a serial cable into the PC, connect the TimeTap directly to the Serial comm port on the PC (A DB9 to DB25 adapter is required to verify operation of a Model 8178T TimeTap).

The TimeTap outputs data every second without the need to type any characters. As long as the TimeTap, the Remote output and the RS-485 cabling are good, a once-per-second data stream will be present on the monitor. If no data is seen, check the cabling, the baud rate of the Remote port, the Remote port itself and the terminal emulator configuration.

5.4 GPS reception

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.

5.4.1 No GPS reception

Cable or connector problem: Antenna problem alarm and SNMP traps should be evident. 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 5-3 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 5-3: 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 2.4 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 2.4 for indoor antenna guidelines and Section 2.4 for outdoor antenna guidelines.

Window Type: Windows with metal film coatings, metal screens or blinds may impede GPS reception. If a window-mount antenna is being used, place the unit into the single satellite mode of operation. Refer to Section 3-22 for more information.

5.4.2 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 2.4.2 for GPS cable recommendations and Section 2.4.5 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. If a window-mount antenna is being used, place the unit into the single satellite mode of operation. Refer to Section 3-22 for more information.

5.5 Modem Dial-out (Option 3) troubleshooting

This section provides assistance with troubleshooting the operation of the modem dial-out feature for those units that have option 3 installed. There are two procedures to verify proper operation of the modem operation. The first test procedure (Test 1) is to determine if the modem will operate and connect to NIST without the Master Clock connected. The second procedure (Test 2) is to ensure the modem operates and connects to NIST when being controlled by the Master Clock. For assistance, please contact Spectracom Tech support at the contact information located at the end of this document.

5.5.1 Test 1: To verify modem is dialing and connecting to NIST in stand-alone mode:

This test will verify the operation of the modem with the Master Clock disconnected and not controlling the modem. If this test does not pass, the problem is with either the modem, the phone line or with NIST. If this test passes, next try dialing out with the modem connected to the Master Clock and follow the procedure below for testing with the unit connected to the modem. (Below these procedures are a sample response of the interaction of the PC, Master Clock and modem). The modem MUST be connected to an analog phone line to operate (It will not operate on a digital phone line).

1) Disconnect the modem from the Serial Setup Interface connector on the rear panel of the Master Clock.

2) Remove the null-modem adapter and plug the DB9 end of the cable into a PC's Comm port and the DB25 end of the cable into the modem.

3) Open HyperTerminal, Procomm or any other terminal emulator program on the PC. Direct the program to the PC's Comm port at 9600 baud.

4) The modem local echo is disabled by default. To see what you are typing, type ate1

5) Type **atz** <enter> to reset the modem settings.

6) Type **atm1** <enter> to turn the modem speaker on (When the modem is connected to the Spectracom clock, the unit will always disable the speaker if software is version 2.1.6 or below).

7) Type **atdt 9w1-303-494-4774** <enter> to dial NIST. 40 consecutive time messages will be displayed. NIST will then disconnect the call.

Note: If you receive the initial connection and "CD" lights on the modem but the 40 time messages are not received, the modem connected to NIST but NIST is having difficulties sending time data. This can happen if NIST is experiencing heavier than normal traffic.

Operation of the modem indicator lights located under the black window during a phone call to NIST:

OH (Off Hook) ***lights when call is started.***
CD (Carrier Detect) ***lights after successful negotiation of modem and NIST.***
DATA ***flashes as data is being received from NIST.***

Below is a sample interaction of the modem dialing NIST

ate1

OK

atz

OK

atm1

OK

atdt 9w1303-494-4774

CONNECT 9600

National Institute of Standards and Technology
Telephone Time Service, Generator 2b
Enter the question mark character for HELP

D L
MJD YR MO DA HH MM SS ST S UT1 msADV <OTM>
53215 04-07-29 12:45:53 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:45:54 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:45:55 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:45:56 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:45:57 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:45:58 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:45:59 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:00 50 0 -.5 045.0 UTC(NIST) *

53215 04-07-29 12:46:01 50 0 -.5 083.8 UTC(NIST) *
53215 04-07-29 12:46:02 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:03 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:04 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:05 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:06 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:07 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:08 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:09 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:10 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:11 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:12 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:13 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:14 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:15 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:16 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:17 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:18 50 0 -.5 205.0 UTC(NIST) *
53215 04-07-29 12:46:19 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:20 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:21 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:22 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:23 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:24 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:25 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:26 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:27 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:28 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:29 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:30 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:31 50 0 -.5 045.0 UTC(NIST) *
53215 04-07-29 12:46:32 50 0 -.5 045.0 UTC(NIST) *

5.5.1.1.1 NO CARRIER

5.5.2 Test 2: To verify operation of the modem while connected to the NetClock

Below is the verification that the modem is properly being controlled by the Spectracom Master Clock and the modem is successfully dialing and connecting to NIST.

For the modem to function with the NetClock, the modem mode needs to be selected in the Modem configuration page of the web browser user interface and the unit rebooted to accept the change from console mode.

If the unit is already powered-up and not synchronized, choosing dial-out now and hitting submit will cause the unit to connect to NIST. If the unit is already synchronized, this option is not

available (The dialout now function is not available for operation if the NetClock is in either holdover or sync mode). To operate the modem if it is in currently in sync, disconnect the antenna and wait until the variable holdover period expires or power cycle the unit to clear the sync condition. Then, the dial-out now function will be available.

Once the NetClock has dialed and synchronized to NIST, the unit will be in holdover mode until the variable holdover period expires (Devices syncing to the NetClock will still sync) indicated by the sync light flashing green. After the variable holdover expires, the unit will declare loss of sync (Sync lamp turns red) or when the scheduled Time Verification call occurs, the modem automatically dials NIST again. If connection is made, holdover is restored (Sync lamp flashes green again).

Verify proper operation of the modem by observing the status of the front panel sync lamp flashing green after connection to NIST and verifying the Model dial-out logs as shown below. If the sync lamp is also flashing red, this is because the GPS antenna is disconnected from the Master Clock. This is not directly related to the modem dial-out feature but if the antenna has been connected in the past, it is related to the reason why the modem is now dialing-out unexpectedly (Antenna problem causing loss of GPS time Sync).

Sample of successful Modem dial out log.

Log entry	Description of log entry
TIME= 12:36:59 DATE= 2004-07-29 Modem dial out to 9 1-303-494-4774.	(Beginning dial out process)
TIME= 12:37:33 DATE= 2004-07-29 on Time Marker. Front panel Synchronized clock to modem time.	(Connected to NIST and got a synchronized (date & time is Updated).
TIME= 12:38:10 DATE= 2004-07-29 correction) Dial out successful. Sync'ing system 1PPS.	(Modem disconnected from NIST, calculating 1PPS
TIME= 12:38:12 DATE= 2004-07-29 Synchronized 1PPS to modem time	(1PPS correction completed. Unit now in holdover**)**

If you are really in console mode but changed the setup to modem and did not reboot (Still in console mode) and try to force a dial-out now, this is the dial-out log result:

TIME= 12:52:47 DATE= 2004-07-29 Modem dial out to 9 1-303-494-4774.	(First response)
TIME= 12:52:47 DATE= 2004-07-29 Timeout occurs, operation is aborted.	

TIME= 12:52:49 DATE= 2004-07-29 (Second response)
Modem dial out to 9 1-303-494-4774.

TIME= 12:52:49 DATE= 2004-07-29
Timeout occurs, operation is aborted.

Note: There are two responses because the “retry call” default (In the modem dial-out configuration page) is set to twice.

5.6 Customer Service

Refer to Section 1.2, Warranty Information and Product Support for information on contacting

6 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 either Data Format 0 or Data Format 2.

6.1 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

6.2 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

Note: Data Format 1 has an available modification that may be made to the data stream structure. Most external systems utilizing Data Format 1 will look for a single digit day of the month for day 1 through day 9, with a space in front of each digit (^1, ^2, ^3 … 10,11…) whereas other systems need to see a two digit day of the month for all days 1 through 9 with a leading 0 instead of a space (01, 02, 03… 10, 11…). If your device requires the two digit day of the month for days 1 through 9, the following procedure will change the Data Format 1 structure to provide this.

Connect to the Serial Setup Interface port with a PC running HyperTerminal OR telnet into the NetClock using the IP address of the unit.

To change Data Format 1 output on a Serial port to a leading 0, type:
ser fmt [1/2] 1 zero <enter> (Where 1 or 2 is the desired Serial port number)

To change Data Format 1 output on a Remote RS-485 port to a leading 0, type:
rem fmt [1/2] 1 zero <enter> (Where 1 or 2 is the desired Remote port number).

To change Data Format 1 output on a Serial port back to a leading space, type:
ser fmt [1/2] 1 <enter> (Where 1 or 2 is the desired Remote port number).

To change Data Format 1 output on a Remote RS-485 back to a leading space, type:
rem fmt [1/2] 1 <enter> (Where 1 or 2 is the desired Remote port number).

6.3 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:

Note: Format 2 cannot be configured for a Time Zone Offset or with automatic Daylight Saving Time adjustment. Attempting to configure a Local clock using Data Format 2 with either a Time Zone Offset or automatic DST rule will result in an error message.

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.

Quality	Time (hours)	TCXO Error (Standard configuration) (milliseconds)	OCXO Error (Option 5) (milliseconds)	Rubidium Error (Option 4) (microseconds)
Space	Lock	<1	<0.01	<0.3
A	<10	<10	<0.72	<1.8
B	<100	<100	<7.2	<18
C	<500	<500	<36	<90
D	>500	>500	>36	>90

Table 6-1: 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.

6.4 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.

6.5 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.

6.6 Format 7:

This format provides a time data stream with millisecond resolution. The Format 7 data stream consists of indicators for time sync status, leap second and Daylight Saving Time. Time data reflects UTC time and is in the 24-hour format. Format 7 data structure is shown below:

CR LF i^YY^DDD^HH:MM:SS.FFFL^D CR LF

where:

CR =	Carriage Return
LF =	Line Feed
I =	Time Sync Status (space, ?, *)
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 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: ? 01 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status: The clock has lost GPS time sync.
Date: Day 271 of year 2001.
Time: 12:45:36 UTC time, Standard time is in effect.

6.7 Format 8:

Format 8 includes a time sync status character, the four digit year, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 8 also includes the DST/Standard Time indicator, and the Time Zone Offset value. Format 8 data structure is shown below:

CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D+XX CR LF or
CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D-XX CR LF

where

CR = Carriage Return
LF = Line Feed
I = Time Sync Status (space, ?, *)
YYYY = Four digit year indication
^ = 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,0)
XX = Time Zone Switch Setting (+/- 00 to 12)

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

Time sync status character I is described below:
I = (space) when the Master Clock is synchronized to UTC source.
= * when the Master Clock time is set manually.
= ? when the Master Clock has not achieved or has lost synchronization to UTC source.

The time and date can be set to either local time or UTC time, depending upon the configuration of the output port.

6.8 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

7 RS-232 SETUP PORT COMMANDS

From the rear panel RS-232 Serial Setup Interface Port, the user can manage files, configure network settings for the product and configure the front panel displays and rear panel outputs. Table 7-1 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	Section
fpd	Configures the Front panel display (Applicable only to units that have Option 2 installed- front panel displays and two Serial output ports).	7.1
frq	Configures the Signature Control for the frequency outputs (Applicable only with units that have Option 6 installed).	7.2
help	Help	7.3
IRIG	Configures the IRIG output (Applicable only to units with an IRIG output installed)	7.4
login	Log in at a specified security level	7.5
logout	Log out of the current security level	7.6
ltc	Configures up to five separate local clocks	7.7
mdo	Modem commands	7.8
mdo help	Display list of commands	7.9
mdo avg	Turn averaging algorithm on or off.	7.10
mdo log	Enable or disable debug logging.	7.11
mdo stat	View or reset the modem statistics.	7.12
net	Network configuration commands	7.13
net gateway	Enables/disables or set the default gateway	1.1
net help	Displays summaries of the network subcommands	1.1
net IP	Sets the IP address	1.1
Net mac	Displays the MAC address	1.1
net mask	Sets the subnet mask	1.1
net show	Shows network parameter	1.1
net http	Enable/disables http access to the unit	7.20
opt	Enables options	7.21
reboot	Reboots the unit	7.22
rem	Configures the Remote RS-485 output(s)	7.23
sec	Security Commands	7.24

sec help	Displays summaries of the security subcommands	1.1
sec level	Displays the current security level	7.26
sec password	Sets the password for the current security level	1.1
ser	Configures the Serial port(s)	7.28
update	Firmware Update Commands	7.29
App	Updates the Application software	1.1
boot	Updates the Boot Monitor	7.29.2
csl	Updates the CSL	7.29.3
kern	Updates the kernel	7.29.4
help	Displays summaries of the update subcommands	1.1

Table 7-1: Alphabetical List of Commands

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

7.1 fpd

The command, ***fpd***, displays the current configuration of the front panel LCD displays. The user may specify a particular command or set of commands to display more detailed help information. The ***fpd*** command is also used to change the configuration of the front panel displays.

The ***fpd*** command requires the user level to be in either config or admin mode.

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

Type: **fpd** <enter>

Type: **fpd help** <enter>
Displays this information.

Type: **fpd format [lcd] [format]** <enter>
Selects the Display format for a specified LCD.

Where: **lcd** : LCD Display Number (0|1) (LCD 1 is the left display and 2 is the right display)

format : Desired LCD Display Format Description from choices listed below.

- none - No format displayed
- product - Product powerup display
- revision - Revision version display
- timeview - Time View display
- time - Time only display
- doy - Day of Year display
- date - Date only display
- date_time - Date and Time display
- doy_time - Day of Year and Time display

fpd date [format]<enter>
Selects date format for LCD Displays

format : Date Format selected from available choices below.

- MM_DD_YY
- DD_MM_YY
- YY_MM_DD
- MM_DD_YYYY

DD_MM_YYYY
YYYY_MM_DD

Fpd time [0|1] [format] <enter>
Selects time format for LCD Displays.

Where: [0|1] : Desired LCD Number to configure
format : Date Format as a 12 or 24 hour display. Choices below.
12
24

fpd font [font]<enter>
Select time reference for LCD Displays
Where font : Font
led - Large Blocky LED Font
thin - Thinner Blocky LED Font
mark - Rounded large blocky LED Font
arial - Arial type font

fpd reset <enter>
Resets LCD Display state back to factory default.

fpd status <enter>
Displays LCD Display state and current selections.

fpd ltc [0|1] [index] <enter>
Sets selected LCD Display's Local Time Clock by index

fpd print lcd row col text <enter>
Prints text string on lcd at desired location
[0|1] : LCD Number
row : Y location
col : X location
text : string to print

7.2 frq

The command, ***frq***, displays the configuration of Signature Control for the frequency output(s). Signature Control is used to disable the frequency output if an alarm or an out–of-sync condition occurs. The ***frq*** command is also used to configure the desired Signature Control settings.

Type: **frq sig [interface] [mode|status] [none|major|sync]** <ent>

Where:	interface	10MHz
	mode	Set Signature Control Mode of operation
	status	View Signature Control status
	none	No Signature Control enabled
	major	Major Alarm will disable frequency output
	sync	Loss of time sync will disable frequency output

7.3 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

7.4 IRIG

irig help <enter>
Display this information

irig disp <enter>
Display the current IRIG port settings.

irig b <AM|TTL> <enter>
Sets the irig output to format B
AM = amplitude modulated output
TTL = TTL compatible output

irig brb <enter>
Sets the irig output to format B Rubidium.
This option is only available on Rubidium units only.

irig e <AM <100|1000>|TTL> <enter>
Sets the irig output to format E
AM = Amplitude modulated output. AM can have 100 or 1000Hz
TTL = TTL compatible output

irig amp <level> <enter>
Sets the amplitude level for AM signals.
level = amplitude of signal. 0 to 255.
Refer to the IRIG section of the instruction manual.

irig ltc <clock> <enter>
Sets the reference clock for the IRIG output.
clock = reference clock index. 0 - UTC, 1-5 local clock
Use 'ltc disp' to see the available clocks

irig sig <none|sync> <enter>
Sets the signature control of the IRIG port.
none = no signature control
sync = synchonized signature control

7.5 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 <enter>
Response:	Account:
Type:	LEVEL <enter>
Response:	Password:
Type:	PASSWORD <enter> (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 <enter>
Response:	Password:
Type	PASSWORD<enter> (the terminal will not show what you type)
Response:	Login Successful
Security Level is now:	Config Level

7.6 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 <enter>
Response:	Logout Successful
now at:	User Level

7.7 ltc

The ltc command is used to create up to five Local clocks. Local clocks allow many of the output ports to be able to provide time data as local time instead of just UTC time. This command requires admin level login.

Usage:

ltc help <enter>
Display this information

ltc disp (index) <enter>
If no arguments are given, displays summary information of all clocks.
If an index is given, displays detailed information for that clock.

ltc create <name> <enter>
Creates a new local clock. Multiple consecutive spaces in the name will be reduced to a single space.
Name = Desired name for the local clock.

ltc delete <index> <enter>
Deletes a local clock at the specified index.

ltc tz <index> <+/-XX:XX|auto> <enter>
Assigns a new Time Zone Offset for the local clock.
XX:XX = define the offset manually
auto = Use GPS to determine the offset.

ltc dst <index> <none|auto|region|bwd|bdm> <args> <enter>
Assigns a new Daylight Saving Time rule to the clock.

index = index of clock

none <enter> (no args) = No DST rule.

auto <enter> (no args) = Use GPS to determine the DST rule.

region <reg> <enter> = Set DST rule as defined by region.
1 - Europe
2 - North America
3 - Australia-1
4 - Australia-2

bwd IN <W> <DDD> <MMM> <HH:MM> <hh:mm> OUT <W> <DDD> <MMM> <HH:MM> <enter>
Defines DST rule by week of month and day of week.

W = Week of month; 1, 2, 3, 4, L (Last)
DDD = Day of week; MON, TUE, WED, THU, FRI, SAT, SUN
MMM = Month; JAN, FEB, MAR, APR, MAY, JUN,
JUL, AUG, SEP, OCT, NOV, DEC
HH:MM = Time change; hours:minutes 00:00-23:59 local time
hh:mm = Amount of change; hours:minute 00:00-23:59

bdm IN <MM> <DD> <HH:MM> <hh:mm> OUT <MM> <DD> <HH:MM> <enter>
Defines DST rule by date.
MM = Month; 01-12
DD = Day of month; 01-31
HH:MM = Time change; hours:minutes 00:00-23:59 local time
hh:mm = Amount of change; hours:minute 00:00-23:59

7.8 mdo

The mdo command is used to configure the dial-out modem option if it is installed. The ***mdo*** command consists of a set of subcommands that are used to control logs and configurations of the modem features.

7.9 mdo help <enter>

Display list of commands

7.10 mdo avg <on|off> <#|auto> <enter>

Turn averaging algorithm on or off.
If averaging is turned on then the number of points to average needs to be specified.
If the number of points is specified as auto then the unit will choose the best number.
If no parameter is specified then the current state will be printed. The system defaults to auto.

Example: mdo avg on auto

7.11 mdo log <normal|debug> <enter>

Enable or disable debug logging.
When debug logging is enabled, a log is created for each call in a set of call attempts. This log contains every message the modem received. The log is stored in the logs folder with the name "call#.log" where # is the number of the call in the set. The system defaults to normal.

The system defaults to normal upon reboot.

Example mdo log debug

7.12 mdo stat [reset] <enter>

View or reset the modem statistics.
If no argument is specified the statistics are printed to the console.
If the reset argument is used the statistics are reset

Example: mdo stat

The system resets all stats on boot

7.13 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:

7.14 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.

7.15 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

7.16 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.

7.17 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.

Note: The MAC address of the NetClock is configured at the factory and cannot be changed.

7.18 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.

7.19 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

7.20 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

7.21 opt

For admin and config levels, options can be shown or enabled by a hash.

```
help       option help - list of options commands
display    option display - used to display current options
enable     option enable [option] [Hash In] - enables options using MD5


>opt disp
Executable:   91XX        (0x00a5)
Product:      9189        (0x0002) EEPROM (0x0002)
Product Name: 9189
Options:      (0x180107ff)        EEPROM (0x180107ff)
Options State: INVALID

  Security:               ON
  Modem:                        ON
  Serial Port 1:          ON
  Remote Port 1:          ON
  Serial Port 2:          ON
  Remote Port 2:          ON
  IRIG Output:            ON
  Front Panel:            ON
  Relays:                       ON
  Oscillator Disciplining: ON
  10 MHz Frequency Output: ON
  Serial Time Code Input:  OFF
  SNTP Server:            ON
  Oscillator Type:        TCXO
  GPS Receiver:           Motorola M12T
  Board:                NONE
```

7.22 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 available ***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.

7.23 rem

The rem command allows the rear panel Remote output(s) to be configured from the console port. This command requires config level or higher login to modify.

Usage:

rem help <enter>
Display this information

rem disp <**X**> <enter>
Display the current remote serial port settings.
X = serial port number; 1, 2

rem baud <X> <baud> <enter>
Sets the baud rate of a remote serial port
X = serial port number; 1, 2
baud = baud rate; 1200, 2400, 4800, 9600

rem fmt **<X> <fmt**> <enter>
Sets the output format of a remote serial port
X = serial port number; 1, 2
fmt = format type; 01, 02, etc.

rem ltc <X> <ltc> <enter>
Sets the output format of a remote serial port
X = serial port number; 1, 2
ltc = clock setting; 0 - UTC, 1-5 local clock

rem all <port> <baud> <format> <clock> <enter>
Configure all settings of the remote serial port
port : The remote serial port to configure (1 or 2)
baud : Baud rate; 1200, 2400, 4800, 9600
format: Format of output
00, 01, 02, 03, 04, 06, 07, 08, 90
clock : Reference clock. 0 - UTC, 1-5 local clocks

7.24 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:

7.25 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

7.26 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

7.27 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

7.28 ser

The ser command allows the rear panel Serial ports to be configured from the console. They require config level or higher login.

Usage:

ser help <enter>
Display this information

ser disp <X> <enter>
Display the current serial port settings.
X = serial port number; 1, 2

ser baud <X> <baud> <enter>
Sets the baud rate of a serial port
X = serial port number; 1, 2
baud = baud rate; 1200, 2400, 4800, 9600

ser fmt <X> <fmt> <enter>
Sets the output format of a serial port
X = serial port number; 1, 2
fmt = format type; 01, 02, etc.

ser ltc <X> <ltc> <enter>
Sets the output format of a serial port
X = serial port number; 1, 2
ltc = clock setting; 0 - UTC, 1-5 local clock

ser req <X> <req> <enter>
Sets the output format of a serial port
X = serial port number; 1, 2
req = request character. Use 'none' for multicast

ser all <port> <baud> <format> <req> <clock> <enter>
Configure all settings of the serial port
port: The serial port to configure
baud: Baud rate; 1200, 2400, 4800, 9600
format: Format of output
00, 01, 02, 03, 04, 06, 07, 08, 90
req: Request character. Use none for multicast
clock: Reference clock. 0 - UTC, 1-5 local clocks

7.29 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:

7.29.1 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.

7.29.2 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.

7.29.3 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.

7.29.4 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.

7.29.5 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

8 Options

Spectracom offers several options for the Model 9183. The following section provides descriptions and details on configuration of these available options.

Some of the options listed below can be purchased and installed with the NetClock still in the field, while other options must be purchased with the unit at the time of the initial purchase. The following table provides the standard configurations for the Model 9183 and the options that may be purchased and installed in the field.

Available Model 9183 Option Combinations

Feature/Option	Model 9183	Capable of being purchased after the initial equipment purchase	Refer to manual Section
Security	Std.	N/A	Section 3.14
Front panel display + (2) additional serial ports	Std.	N/A	Sections 2.6 and 3.5
Dial-Out Modem	Opt 3	Yes	Section 8.1
Rb (Rubidium) Oscillator *	Opt 4	No	Section 8.2
OCXO Oscillator *	Opt 5	No	Section 8.3

Std. = Standard feature. Opt X = Option number X. NA = Not Available.
*Can choose one, cannot choose both oscillators.

Please contact our Sales department for information regarding any of the options that are not currently installed in your NetClock that you may be interested in obtaining.

8.1 Option 3: Modem

8.1.1 Option 3 basics

Option 3 provides the NetClock with the capability to use a modem to dial-out via an analog phone line for time retrieval if GPS reception is either lost or cannot be obtained due to site limitations. The modem can be configured in the software as either the primary external time reference or it can also be configured as a Secondary/Backup reference in case the primary reference is lost.

The modem interfaces to the NetClock via the Serial Setup Interface located on the rear of the NetClock. This dual-function port provides the capability to initially configure the network settings and is also the interface for the modem.

If not initially purchased with the unit, Option 3 can be enabled (turned on) in the field. Please contact our Sales department to purchase this option. You will be sent a Hash key that can be

entered in the NetClock to enable the security algorithms. The purchase of the option includes a Spectracom supplied compatible modem.

Note: The modem **MUST** be **Hayes AT** compatible and configured for this mode of operation to operate correctly with the unit. The Spectracom supplied modem is Hayes AT compatible.

8.1.2 Modem installation

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

1. Connect the null modem converter that comes with the serial cable to the DB9 end of the cable.

2. Connect the DB25 side of the null modem converter to the modem and the modified DB9 side to the Serial Setup port located on the rear of the NetClock.

3. Connect the CAT2 telephone cable from the analog phone line to the modem.

4. Connect the modem power adapter to a power outlet.

8.1.3 Modem Dial-Out Setup

Using the web browser user interface to configure dial-out modem feature:
The modem dial-out feature is used as either a Secondary/Backup time reference when all other external time references become unavailable or can also be used as a primary reference if an external reference is not available for use (Such as the inability to receive GPS at a particular location). The Modem dial-out Configure web page provides options to configure the operation of the dial-out modem feature. Login to either the configuration or administrator-level mode if changes are desired. All fields will display the current system settings. The Modem dial-out configuration screens are accessed from the "System Setup" page on the bottom frame, and then select the “Modem Dial Out” from the left frame.

There are four different types of modem dial-out calls that can be made. The call type is determined by the state of the system (after the call is finished) as well as user input. Calibration calls happen upon a user request. Time verification calls happen on a user specified interval if holdover is entered from time sync with another source. Time sync calls happen when time sync is lost and on a user specified interval until another time source is available. Modem test calls happen when no calls have been made for a user specified time, or upon a user request. Because the modem determines how to use a call after the call is finished it is possible to start a call as a certain call type and actually use it as another call type. Here is a description of each of the four possible call types.

8.1.4 Calibration Call

Calibration calls are done to characterize the call latency. A user specified number of calls will be made over the calibration period and the average latency will be used to adjust all future calls. The calibration will only be done at the user's request and may be started only while in sync from another time source. Calibration calls may be continued into holdover, but will be cut off if the unit goes out of sync at any point during the calibration period.

8.1.5 Time Verification Call

Time verification calls are made to verify the unit still has acceptable time and to correct for any leap seconds that may be asserted while the reference is not available. Calls will be made on a user specified time table. If the call interval is more than a month leap seconds may be missed. If a leap second is to be inserted at the end of the month then the clock will be scheduled to do so. If the time is off by more than half a second then the unit will be immediately put into unsynchronized mode (Time sync lamp will extinguish and time outputs will be ignored).

8.1.6 Time Sync Call

Time sync calls are done to set the second and sub second timers and to check for any leap seconds. If a call is successful the timer will be set and the unit will be put in holdover mode with the holdover timer reset. In addition if a leap second is to be inserted at the end of the month then the clock will be scheduled to do so. Time sync calls will be made once the unit has gone into unsynchronized mode until it obtains sync from another time source. During this period, calls will be made on a user specified timetable or any time the unit goes out of sync.

8.1.7 Modem Test Call

Test calls are calls that make sure the modem is working. The modem will call out and check for valid time messages. The unit will log "test passed" if it was able to get good time messages or failed if it was not. No changes will be made to the system time. Testing can be done only in sync from another time source and can either be on a specified interval or as requested.

8.1.8 Modem Dial-Out CONFIGURE page

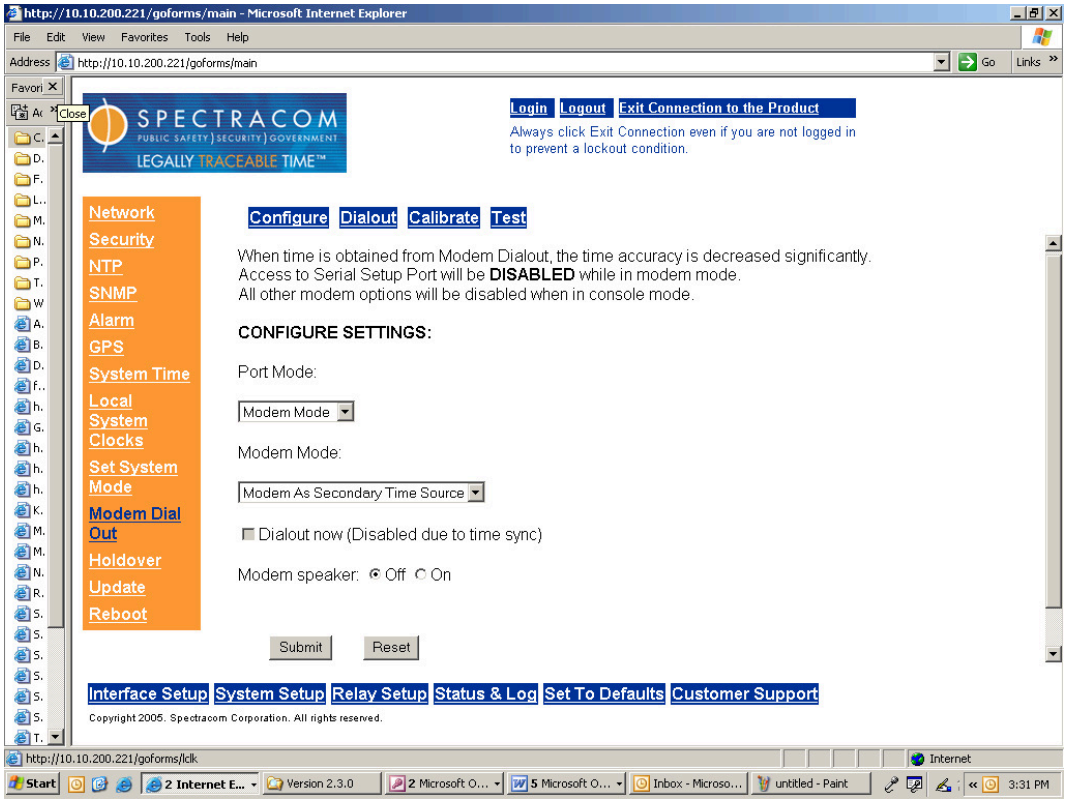


Figure 8-1: Modem Dial-Out CONFIGURE Screen

Serial Setup Port Mode:
The modem is connected to the Serial Setup port for normal operation. On the Modem Configure page is a pull-down menu to select the mode that the Serial Setup Port will operate in. Two options are available:

Console Mode: In this mode, Serial Setup port can be connected with a serial cable to a computer with a serial terminal program running. The serial setup software commands can then be used to interface with the unit. The modem operation will not be available while selected to this mode.

Modem Mode: In this mode, the Serial Setup port can be connected to a modem for dialing out. The Serial Setup port will be unavailable for network configuration while in this mode.

Important Note: The unit **must be rebooted** to apply the changes made to the serial setup port mode.

Modem as Primary/Secondary time source
The modem can be configured as either the primary reference or a secondary/back-up mode of operation. This selection is configured on the Modem dial-out Configure page. In the Secondary/Back-up mode of operation, all GPS antenna problem alarms (Indicating a short or open in the antenna cable) and SNMP traps associated with the GPS reference input will be fully enabled. When the modem Primary mode of operation is selected, the antenna problem alarm and associated SNMP traps for the antenna will not be generated. No indication of a problem with the GPS cable will be present or available. The Modem mode of operation does not affect the ability to receive GPS.

Note: If the unit initially operated without a GPS reference and primary mode of operation was selected, then at a later time a GPS antenna is connected, the mode of operation should be changed to secondary mode to enable the GPS antenna problem alarms to aide in troubleshooting.

Dialout now:
(Only available in Modem Mode and only when the unit is not in time sync).
Checking this box and clicking submit will prompt the dial out modem software to attempt an immediate dial out procedure with the current settings if the unit is currently out of sync. When a unit is configured in modem mode while it is in time sync, the "Dialout now" checkbox will be greyed-out (disabled).

Modem speaker: Toggles the modem speaker on or off during dial out.

8.1.9 Modem Dial-out DIALOUT page

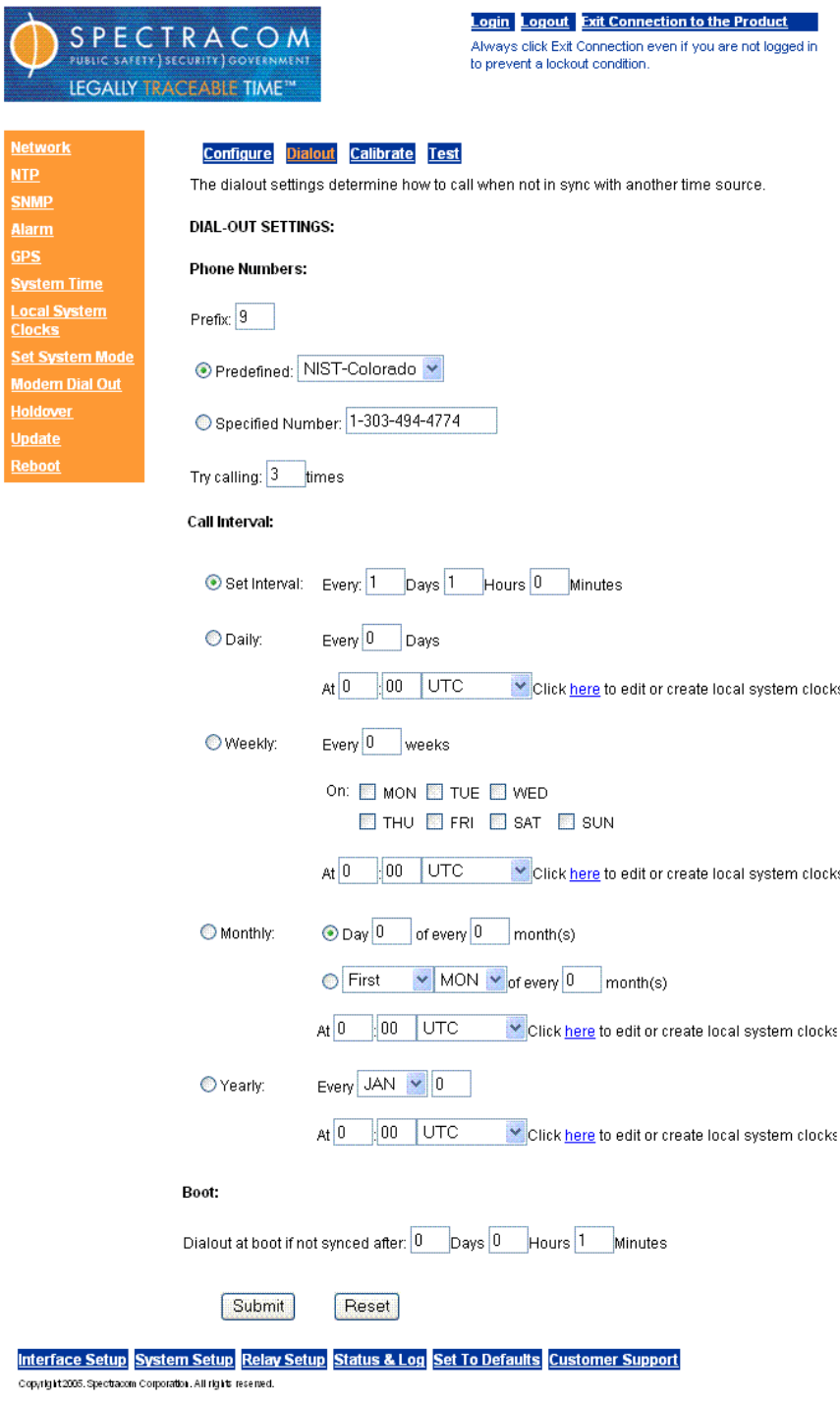


Figure 8-2: Modem Dial-Out DIALOUT Configure Screen

The model dial-out DIALOUT page is used to annotate the phone number used to obtain the time from and to determine how often the modem will be used to retrieve the current time.

Phone Numbers:
Prefix: The phone prefix is a number(s) that need to be dialed to reach an outside line.

Predefined: Stores two predefined number NIST-Colorado and NIST-Hawaii. These are the phone numbers to the National Institute of Standards and Technology modem time service.

Specified Number: This field will take any phone number that the user would like to use to dial out to obtain time.

Try Calling: This field specifies how many times the dial out modem software will try to connect to the selected phone number. Setting this field's value to 0 will generate a warning because it will prevent any dial out to be made in any condition, effectively disabling the modem dial out feature.

Call Interval:
The call interval is used to manually configure how often the modem should dial-out for Time verification calls when the unit is in the holdover mode and Time Sync is normally derived from GPS (Secondary/Backup mode of operation) or Time Sync calls when the modem is selected as the primary mode of operation.

To prevent a leap second occurrence from being missed and a one second error being inserted into the NetClock, we recommend the Time Verification calls be placed less than once-per-month. Setting the Time Verification call period to longer than once-per-month can result in a one second error from the time a leap second is asserted by NIST until the next Time Verification/Time Sync call is placed.

To help prevent a loss of Time Sync condition from occurring, the call interval should be configured for a value of less than the holdover period. This will prevent the holdover period from expiring (which will cause loss of Time Sync) because the modem was configured to dial-out after the holdover expired. For example, if the holdover period is set for two weeks, the call interval should be set to dial-out less than every two weeks. Otherwise, holdover will expire before the modem is scheduled for a dial-out and Time Sync will be lost.

Boot dial-out:
This field specifies how long the modem software will wait after being powered up to check the unit's time sync status. If this time expires and the unit has not achieved time sync yet, the modem software will automatically dial out with the current settings at that time. Note that changes to this timer's settings will not change the timeout of the current countdown if it has already begun (e.g. If the timer is set to 1 hour and then rebooted, the unit will countdown to 1 hour at power up. Changing the timer's settings to 30 minutes will not affect the current countdown. The new 30 minutes value will only be used if another power cycle occurred). If want to skip the initial countdown, you can always use the *Dialout Now* feature.

If the modem is the primary mode of operation for Time sync, the boot dial-out value should be set for a very short duration as the unit will not be able to achieve time sync without the modem placing a call. If the modem is strictly a backup to the external reference, this period can be lengthened to longer than the typical amount of time needed to synchronize to the external reference.

8.1.10 Modem Dial-out CALIBRATE page

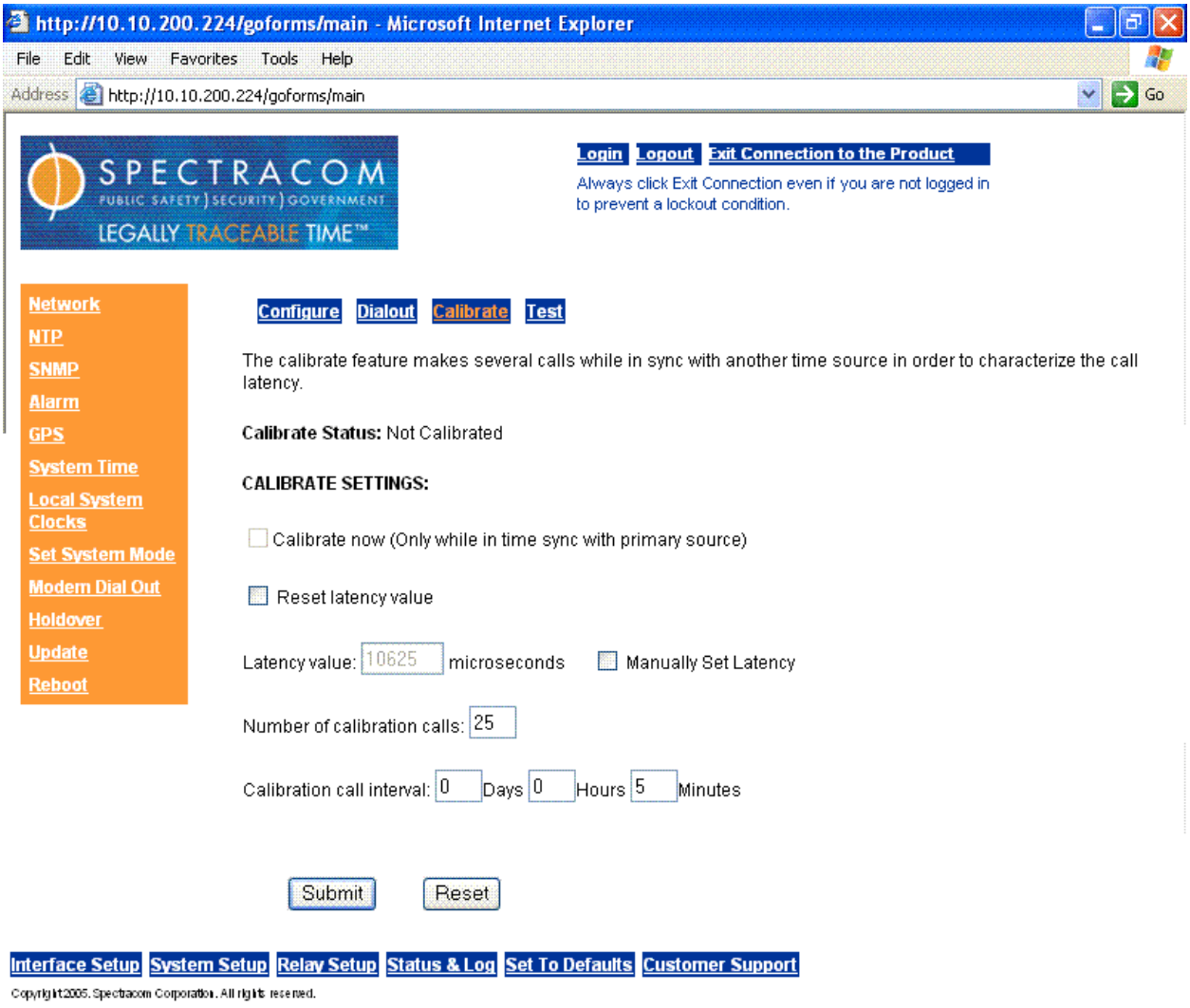


Figure 8-3: Modem Dial-Out CALIBRATE Screen

The Modem dial-out calibrate screen is used to calibrate the modem for increased accuracy of the dial-out calls. The calibration procedure is not required but may be used to provide greater accuracy of future modem calls. The calibration process, using several dial-out helps compensate for inherit internal software processing lags as well as phone network delays as well. Different locations may experience different latencies as well as time of day latencies may also vary.

The calibrate mode allows the user to define the typical latency for the geographic location as well as the time of day the modem is most likely to be used for time sync (such as for primary mode of operation).

Calibrate Status:
The status of calibration is displayed at the top of the screen. If the calibration has been made then the unit will say "calibrated". If the latency has not been set or has been manually set, then the unit will say "not calibrated". If the unit is currently calibrating then the number of successful calls will be displayed here.

Calibrate Now:
Calibrate now is based on the current settings. This will calculate the call latency and adjust all future calls based on this value. The call latency is based primarily on the phone system. Therefore, this should be done when the unit is first set up and does not need to be done again unless it is connected to a different phone system.

Reset Latency Value:
This resets the latency value to the factory default. This can be done if the unit was accidentally set.

Latency Value/Manually Set Latency:
This box displays the current latency value. If the "manually set latency" box is checked then this can be edited to set the current latency.

Number of Calibration calls:
This is the number of calibration calls to be made before the modem is declared as calibrated. The accuracy of the latency calculation depends directly on this number. The more calls that are made, the more accurate the calculation will be. This should not be lowered from the default, but it may be safely raised.

Calibration Call Interval:
This is the interval between calibration calls. This value, along with the number of calibration calls, will determine how long the calibration process will take.

8.1.11 Modem Dial-out TEST page

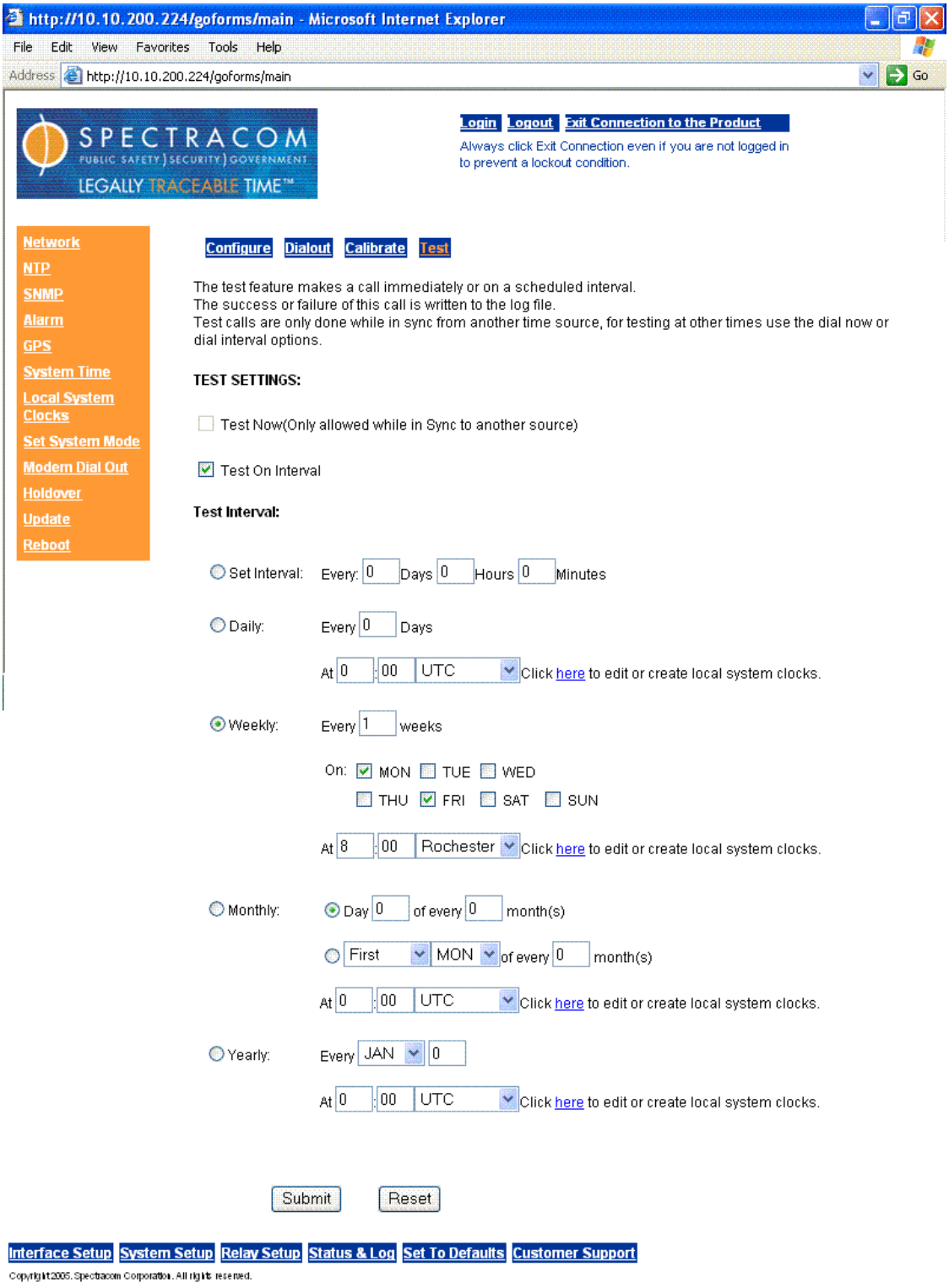


Figure 8-4: Modem Dial-Out TEST Screen

Test Now:
Tests the modem to make sure it can correctly dial-out. This may only be done while in time sync from another source such as GPS. To test in other states, use the dial now button. The result of this test will be written to the log file.

Test On Interval:
Enables the modem test interval. If the unit has not made another type of call during this interval then a test call will be made.

Test Interval:
Sets the modem test interval. In order to set these values, the "Test On Interval" box must be checked. If the interval expires before another type of call is made then a modem test call will be made. To schedule a call when not in sync from another time source, use the "Call Interval" setting in the Dialout Settings page.

Example 1: To configure the modem dial out to:
Wait 30 minutes before checking time sync status at power up
Dial to NIST-Hawaii
With a phone prefix of 9
Retry the connection 5 times before giving up
Checking the system sync status every 15 days
Dialout with the modem speakers on

Connect to the web browser user interface of the unit.

Login to configuration- or administrator-level mode and browse to the Modem Dial Out page.

Select 'Modem Mode' from the Serial Setup Port Mode pull down menu.

In the *"Dialout if not synchronized after"* fields, type '30' in the Minutes field and type '0' in the other fields.

Type '9' in the Prefix text field.

1. *Select the Predefined radio button.*

Select 'NIST-Hawaii' from the Predefined pull down menu.

In the *"try calling"* fields, type '5' to try the connection 5 times.

In the *"redial after"* fields, type '15' in the Days field and type '0' in the other fields.

Change the modem speaker radio button settings to on.

Review the changes made and click Submit. The browser will ask for the unit to be rebooted to apply the changes to the setup serial port mode.

Reboot the unit.

After the reboot, the unit will function in modem mode. If you need to dial out immediately, connect a modem to the setup serial port and then check the 'Dialout now' box and click Submit. Recall that this option will only be available if the unit is not in time sync. If you have set the "*Dialout if now sync after"* timer, the timer will begin counting down as soon as the software is started.

To observe the result of the dial out, monitor the Dialout Log.

Once a dialout procedure is finished successfully, the unit's state will be in sync. The unit's internal oscillator maintains this sync state for a duration of time called the holdover period. During this time, there is no need to dialout again hence the dialout option is disabled.

There will be time periods when NIST's ACTS telephone lines are used up. If you are unable to connect, please try again at another time. Also, verify that your phone line is **analog**.

If you forgot you network settings while in modem mode:

While in modem mode, the setup serial port will still respond to the '***net show***' command. Disconnect the modem from the setup serial port and attach a serial cable to a PC with a terminal software running as if you are connecting in console mode. Type '***net show***' and the current network settings will be displayed. Use this information to connect to the unit through telnet or the web browser user interface to communicate with the unit.

Note: For additional assistance with troubleshooting the modem functionality, please refer to Section 5.5.

8.2 Option 4: Rubidium oscillator

Option 4 provides the NetClock with a self-calibrating ovenized rubidium oscillator. The purpose of this oscillator is to provide a very accurate time base when GPS is either lost or cannot be obtained due to site limitations. It is also used to provide a very stabile and accurate 10 MHz output with a high degree of holdover if GPS is lost. Because of its high degree of stability, this oscillator provides the ability to greatly extend the hold-over period when GPS is not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

Note: The NetClock must be ordered with Option 4 installed at the time of the initial purchase. This option cannot be added after the NetClock has been shipped from the factory.

The Rubidium oscillator is atomic in nature but requires no MSDS.

8.2.1 Comparison of the Rubidium oscillator to the OCXO and standard TCXO oscillators:

10 MHZ frequency output:

Rubidium oscillator (Option 4): $1x10^{-12}$ typical 24-hour average locked to GPS, $1x10^{-11}$ per month typical aging unlocked.

OCXO oscillator (Option 5): $1x10^{-11}$ typical 24-hour average locked to GPS, $2x10^{-9}$ per week typical aging unlocked.

TCXO oscillator (Standard): $1x10^{-10}$ typical 24-hour average locked to GPS

Time drift while the NetClock is in Holdover mode (Loss of primary/backup reference):

Oscillator	Option	Estimated Error Rates	Time to reach 2 ms
Rb	Option 4	0.18 microseconds / hour (nominal)	463 days
OCXO	Option 5	72 microseconds / hour (nominal)	28 hours
TCXO	Standard	1.0 milliseconds / hour (nominal)	2 hours (typical)
TCXO	Standard	7.2 milliseconds / hour (worst case)	17 minutes*

8.3 Option 5: OCXO oscillator

Option 5 provides the NetClock with a self-calibrating ovenized quartz oscillator. The purpose of this oscillator is to provide a very accurate time base when GPS is either lost or cannot be obtained due to site limitations and a very precise 10 MHz output. Because of its high degree of stability, this oscillator provides the ability to greatly extend the hold-over period when GPS is not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

The OCXO characteristics are not quite the same as the Option 04 Rubidium oscillator, but are still much greater than the standard TCXO that is used in the product when option 4 and 5 are not installed.

Note: The NetClock must be ordered with Option 5 installed at the time of the initial purchase. This option cannot be added after the NetClock has been shipped from the factory

---

8.3.1 Comparison of the OCXO to the Rubidium and standard TCXO oscillators:

10 MHZ frequency output:

OCXO oscillator (Option 5): $1x10^{-11}$ typical 24-hour average locked to GPS, $2x10^{-9}$ per week typical aging unlocked.

Rubidium oscillator (Option 4): $1x10^{-12}$ typical 24-hour average locked to GPS, $1x10^{-11}$ per month typical aging unlocked.

TCXO oscillator (Standard): $1x10^{-10}$ typical 24-hour average locked to GPS.

Time Drift while the NetClock is in Holdover mode (Loss of primary/backup reference):

Oscillator	Option	Estimated Error Rates	Time to reach 2 ms
OCXO	**Option 5**	**72 microseconds / hour (nominal)**	**28 hours**
Rubidium	Option 4	0.18 microseconds / hour (nominal)	463 days
TCXO	Standard	1.0 milliseconds / hour (nominal)	2 hours (typical)
TCXO	Standard	7.2 milliseconds / hour (worst case)	17 minutes*

9 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
    permissions and restrictions.  Use only at your own responsibility.
    You will be responsible for any legal consequences yourself; I am
not
    making any claims whether possessing or using this is legal or not
in
    your country, and I am not taking any responsibility on your
behalf.


                                NO WARRANTY

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

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

2)
    The 32-bit CRC implementation in crc32.c is due to Gary S. Brown.
    Comments in the file indicate it may be used for any purpose
without
    restrictions:

     * COPYRIGHT (C) 1986 Gary S. Brown.  You may use this program, or
     * code or tables extracted from it, as desired without
restriction.

3)
    The 32-bit CRC compensation attack detector in deattack.c was
    contributed by CORE SDI S.A. under a BSD-style license.

     * Cryptographic attack detector for ssh - source code
     *
     * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
     *
     * All rights reserved. Redistribution and use in source and binary
     * forms, with or without modification, are permitted provided that
     * this copyright notice is retained.
     *
     * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
     * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
     * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY
OR
     * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
     * SOFTWARE.
     *
     * Ariel Futoransky <futo@core-sdi.com>
     * <http://www.core-sdi.com>

4)
    ssh-keygen was contributed by David Mazieres under a BSD-style
    license.

     * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
     *
     * Modification and redistribution in source and binary forms is
     * permitted provided that due credit is given to the author and
the
     * OpenBSD project by leaving this copyright notice intact.

5)
    The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers
    and Paulo Barreto is in the public domain and distributed
    with the following license:

     * @version 3.0 (December 2000)
     *
     * Optimised ANSI C code for the Rijndael cipher (now AES)
     *
     * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
     * @author Antoon Bosselaers
<antoon.bosselaers@esat.kuleuven.ac.be>
     * @author Paulo Barreto <paulo.barreto@terra.com.br>
     *
     * This code is hereby placed in the public domain.
     *
     * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY
EXPRESS
     * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
     * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
     * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
     * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
     * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
     * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
     * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
     * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
     * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
     * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)
    One component of the ssh source code is under a 4-clause BSD license,
    held by the University of California, since we pulled these parts from
    original Berkeley code.  The Regents of the University of California
    have declared that term 3 is no longer enforceable on their source code,
    but we retain that license as is.

     * Copyright (c) 1983, 1990, 1992, 1993, 1995
     *      The Regents of the University of California.  All rights
reserved.
     *
     * Redistribution and use in source and binary forms, with or without
     * modification, are permitted provided that the following conditions
     * are met:
     * 1. Redistributions of source code must retain the above copyright
     *    notice, this list of conditions and the following disclaimer.
     * 2. Redistributions in binary form must reproduce the above copyright
     *    notice, this list of conditions and the following disclaimer in
the
     *    documentation and/or other materials provided with the
distribution.
     * 3. All advertising materials mentioning features or use of this
software
     *    must display the following acknowledgement:
     *      This product includes software developed by the University of
     *      California, Berkeley and its contributors.
     * 4. Neither the name of the University nor the names of its
contributors
     *    may be used to endorse or promote products derived from this
software
     *    without specific prior written permission.
     *
     * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS''
AND
     * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
     * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
     * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE
LIABLE
     * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
     * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS
     * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
     * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
     * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY
     * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF
     * SUCH DAMAGE.

7)
    Remaining components of the software are provided under a standard
    2-term BSD licence with the following names as copyright holders:

            Markus Friedl
            Theo de Raadt
            Niels Provos
            Dug Song
            Aaron Campbell
            Damien Miller
            Kevin Steves
            Daniel Kouril
            Per Allansson

     * Redistribution and use in source and binary forms, with or without
     * modification, are permitted provided that the following conditions
     * are met:
     * 1. Redistributions of source code must retain the above copyright
     *    notice, this list of conditions and the following disclaimer.
     * 2. Redistributions in binary form must reproduce the above copyright
     *    notice, this list of conditions and the following disclaimer in
the
     *    documentation and/or other materials provided with the
distribution.
     *
     * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
     * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES
     * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED.
     * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
     * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT
     * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE,
     * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
     * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
     * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF
     * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



  LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a dual license, i.e. both the conditions
of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
```

```
  See below for the actual license texts. Actually both licenses are
BSD-style
  Open Source licenses. In case of any license issues related to
OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2003 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be
used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long
as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL
documentation
 * included with this distribution is covered by the same copyright
terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given
attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
the
 *    documentation and/or other materials provided with the
distribution.
 * 3. All advertising materials mentioning features or use of this
software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the
library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative
thereof) from
 *    the apps directory (application code) you must include an
acknowledgement:
 *    "This product includes software written by Tim Hudson
(tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version
or
 * derivative of this code cannot be changed.  i.e. this code cannot simply
be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */

---- Part 1: CMU/UCD copyright notice: (BSD like) -----
       Copyright 1989, 1991, 1992 by Carnegie Mellon University
                          Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California
                                All Rights Reserved
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 that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.
CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS.  IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----
-
Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
*  Redistributions of source code must retain the above copyright notice,
   this list of conditions and the following disclaimer.
*  Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
*  Neither the name of the Networks Associates Technology, Inc nor the
   names of its contributors may be used to endorse or promote
   products derived from this software without specific prior written
   permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----
Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
*  Redistributions of source code must retain the above copyright notice,
   this list of conditions and the following disclaimer.
*  Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
*  The name of Cambridge Broadband Ltd. may not be used to endorse or
   promote products derived from this software without specific prior
   written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----
Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.
Use is subject to license terms below.
This distribution may include materials developed by third parties.
Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered
trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
*  Redistributions of source code must retain the above copyright notice,
    this list of conditions and the following disclaimer.
*  Redistributions in binary form must reproduce the above copyright
    notice, this list of conditions and the following disclaimer in the
    documentation and/or other materials provided with the distribution.
```

```
*  Neither the name of the Sun Microsystems, Inc. nor the
    names of its contributors may be used to endorse or promote
    products derived from this software without specific prior written
    permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----
Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:
*  Redistributions of source code must retain the above copyright
notice,
   this list of conditions and the following disclaimer.
*  Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
*  Neither the name of the Networks Associates Technology, Inc nor the
   names of its contributors may be used to endorse or promote
   products derived from this software without specific prior written
   permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE


This open software is available for at least three
   years, to give any third party, for a charge no more than your
   cost of physically performing source distribution, a complete
   machine-readable copy of the corresponding source code, to be
   distributed under the terms of Sections 1 and 2 above on a medium
   customarily used for software interchange
```

NETCLOCK
MODEL 9183
MANUAL ADDENDUM
SOFTWARE v2.3.0 TO v2.3.1

95 Methodist Hill Drive
Rochester, NY 14623
Phone: 585.321.5800
Fax: 585.321.5219

www.spectracomcorp.com
Part Number 9183-5001-0050
Manual Addendum
22 December 2005

SPECTRACOM LIMITED 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.

SPECTRACOM 95 Methodist Hill Drive Rochester, NY 14623

+1.585.321.5800 FAX: +1.585.321.5218 www.spectracomcorp.com sales@spectracomcorp.com

Table of Contents

List of Figures

1 Changes for v2.3.0 to v2.3.1

This addendum to the operations and maintenance manuals for the Spectracom NetClock® Model 9183 (current to software version 2.3.0) describes the changes made to software features for version 2.3.1. These changes include additions and enhancements to the Web User Interface (Web UI), to the command line, and in SNMP.

2 Network and Web User Interface Changes

The user may now enable and disable all network interfaces. The HTTPS port has been added to the Web UI and may be controlled on the System Setup web page on the Network tab.

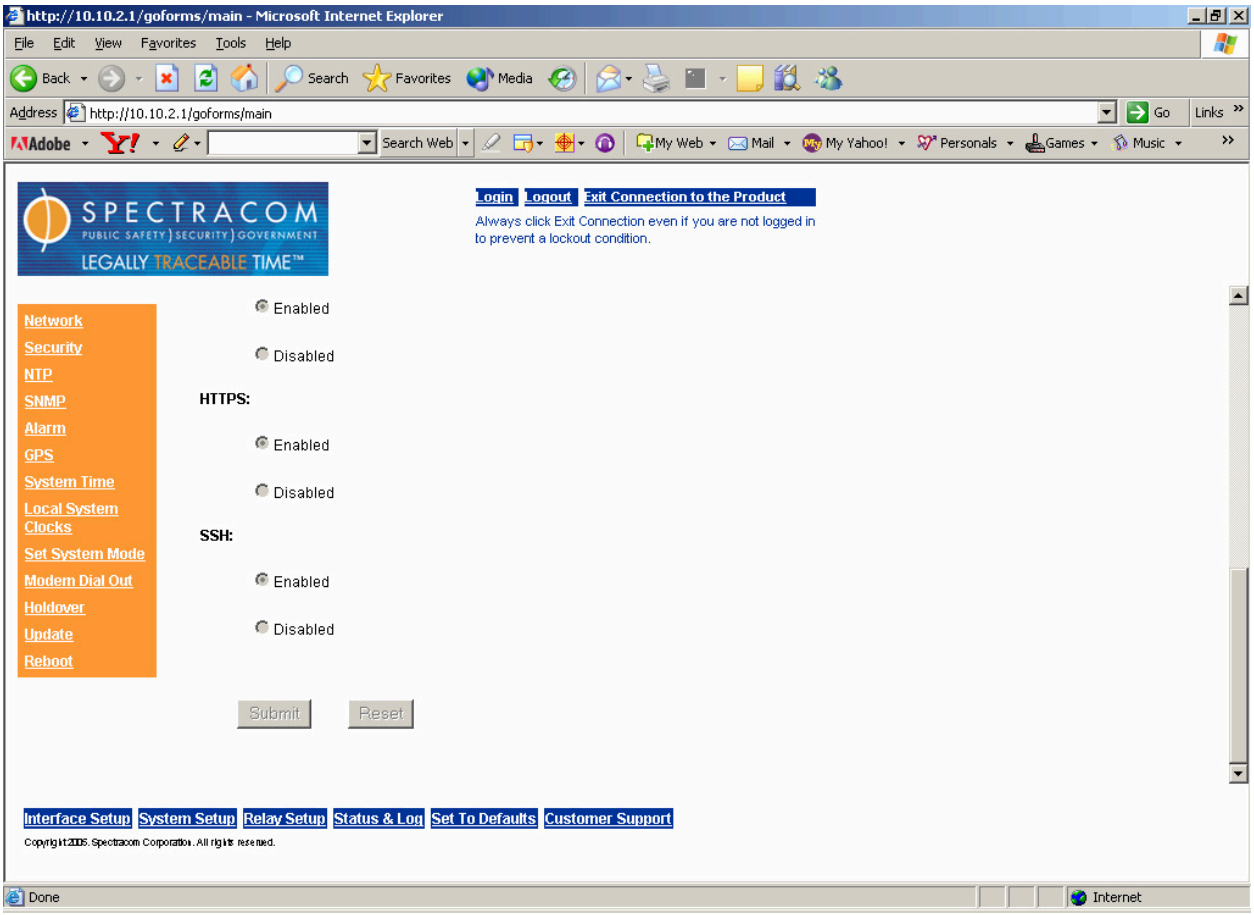


Figure 2-1: Enabling and Disabling Network Interfaces

Allowing the user to enable and disable at will all network interfaces provides greater security and stability of the NetClock in hostile network environments. It also allows users to comply with corporate security policies regarding network access.

2.1 Command Line Changes

The network interface command line now allows the user to enable and disable all ports for Telnet, FTP, HTTP, HTTPS and SSH.

The new commands for the network interface are:

telnet net telnet [yes,no] – Enable or disable telnet on port 23
ftp net ftp [yes,no] – Enable or disable ftp on port 21
https net https [yes,no] – Enable or disable https on port 443
sshd net sshd [yes,no] – Enable or disable ssh on port 22

2.1.1 net telnet

This command allows user to enable or disable the telnet port. Input yes to enable no to disable. Input **net telnet yes** to enable and **net telnet no** to disable.

2.1.2 net ftp

This command allows user to enable or disable FTP the port. Input **net ftp yes** to enable and **net ftp no** to disable.

2.1.3 net https

This command allows the user to enable or disable the HTTPS port controlling access to the secure web server. Enter **net https yes** to enable and **net https no** to disable.

2.1.4 net sshd (Includes SSH, SCP, and SFTP)

This command allows the user to enable or disable the SSH port controlling access to secure SSH protocols SSH secure shell, SCP secure copy, and SFTP secure file transfer. Input **net sshd yes** to enable and **net sshd no** to disable.

2.2 Web Server Timeout

The manner in which the GoAhead Web Server functions requires users to terminate Web UI sessions by clicking “Exit Connection to the Product”. Clicking the “X” button on the browser does not end the session, but closes the window – which means the user cannot log in again until the session expires. In some versions of the software, this is 15 to 30 minutes, which some users find inconvenient.

Version 2.3.1 software includes new console commands that allow administrator-level to users to exit the current locked Web UI session using telnet or ssh. Also added is a command to set the timeout to a user-defined value, which means users may now dictate the length of time it takes for the session to expire.

Use the 'web help' command to see a list of net commands. These include **web exit** and **web timeout minutes** (to set the connection timeout).

2.2.1 web exit

This command allows the user to exit the current web session from telnet or ssh connections.

2.2.2 web timeout

This command allows the user to set the web session timeout to any value between 1 and 60 minutes (inclusive). Spectracom recommends selecting a timeout interval of 10 to 15 minutes.

2.3 HTTPS Certificate 20-Year Life

The HTTPS Certificate Creation Web UI page has been changed to indicate required parameters (with a red asterisk). Refer to the Security tab on the System Setup page.

The default Spectracom HTTPS Web Server Certificate is now 20 years. The new default Certificate life is therefore 7300 days (20 years, in days) and appears on the page as:

* Self Signed Certificate Expiration (Days): 7300

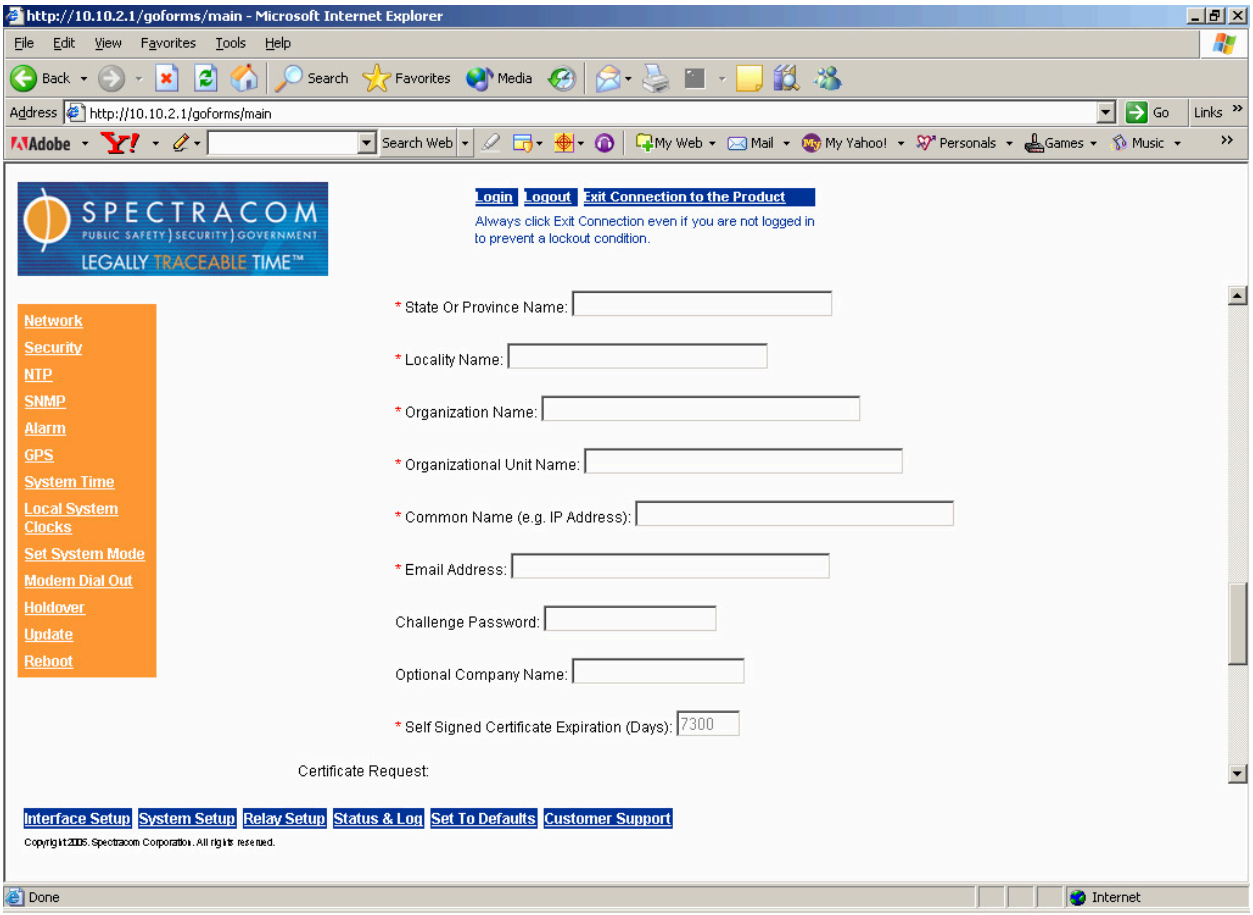


Figure 2-2: HTTPS Certificate Creation Web UI Page

2.4 Modem

Modem functionality has been improved in software version 2.3.1. ITU-R TF583.4 format is now supported. Support has also been added for the two most commonly used baud rates (1200 and 9600 baud) for ITU-R and ACTS formats. NetClocks running software version 2.3.0 require the user to reboot the unit when switching from Console to Modem mode. In software version 2.3.1, it is no longer necessary to reboot when switching from one mode to the other.

The user may select the Baud Rate or the Setup Port mode as shown in the following sections.

2.4.1 Baud Rate

The baud rates 1200 and 9600 are supported because they are the most commonly used baud rates for ITU-R and ACTS formats worldwide. ITU-R format typically uses 1200 baud, while ACTS format typically uses 9600 baud.

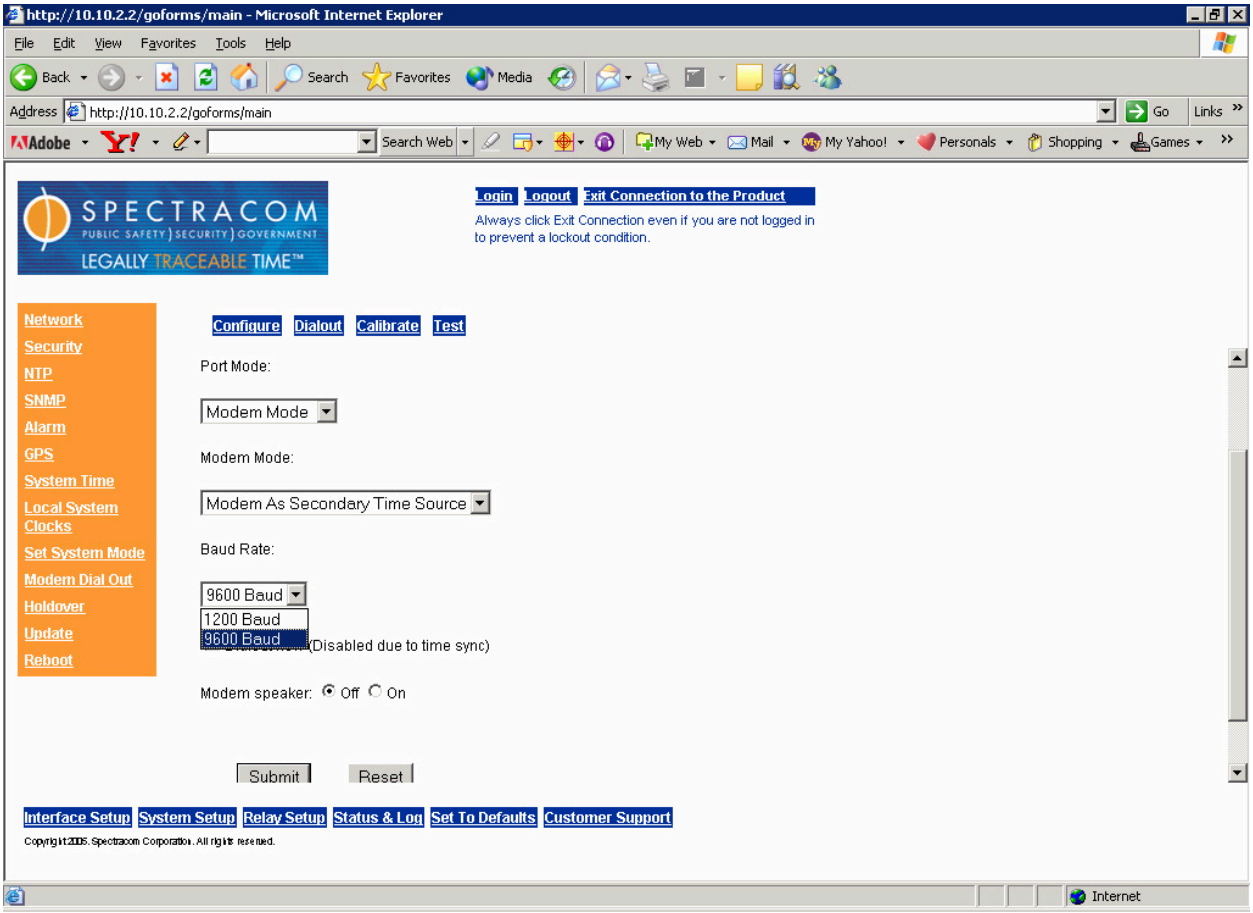


Figure 2-3: Baud Rate Support

2.4.2 Setup Serial Port Mode

To switch from Serial Console Port mode, select Modem mode (Figure 2-4). Once the Modem mode is selected, click Modem Dial Out (Figure 2-5). This displays all the modem tabs.

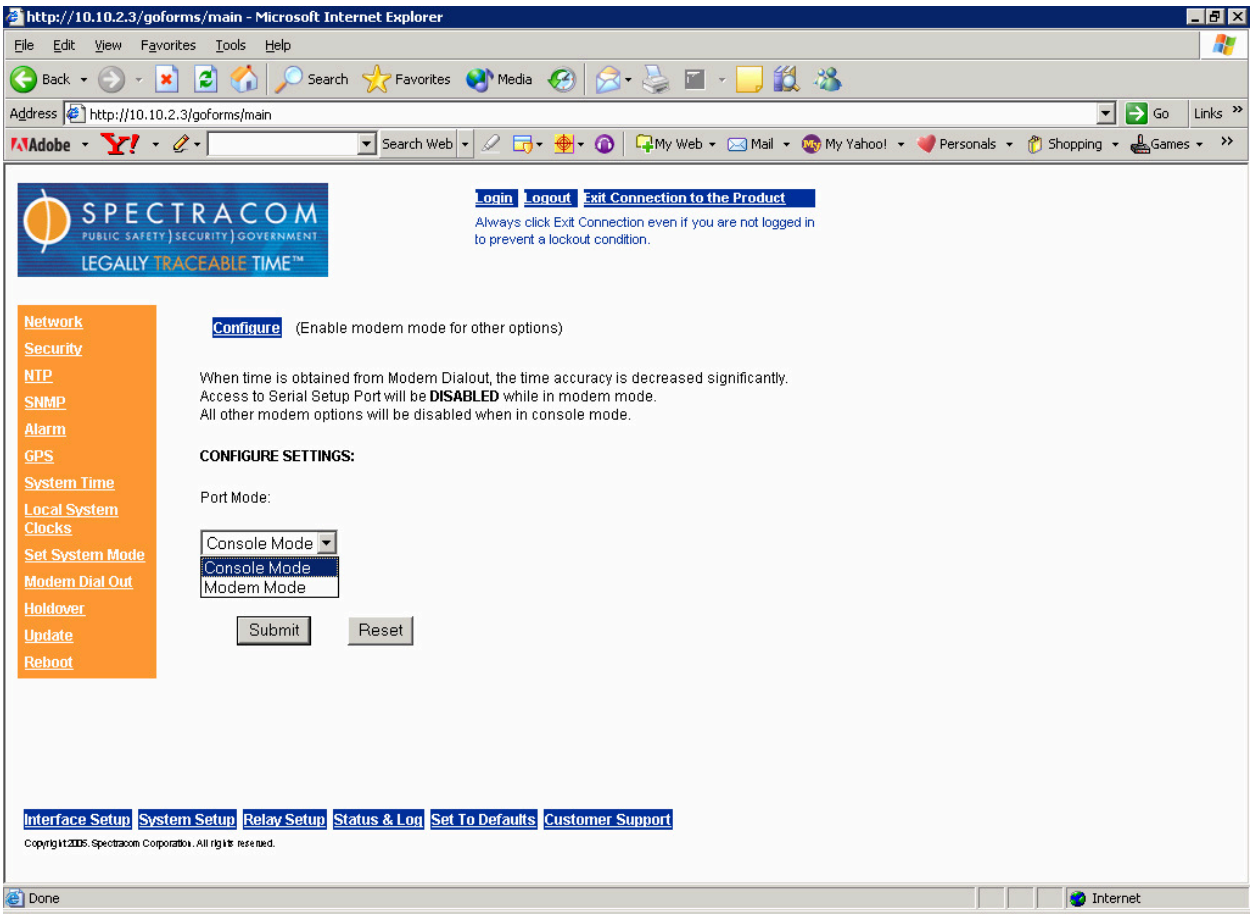


Figure 2-4: Switching from Console Mode to Modem Mode

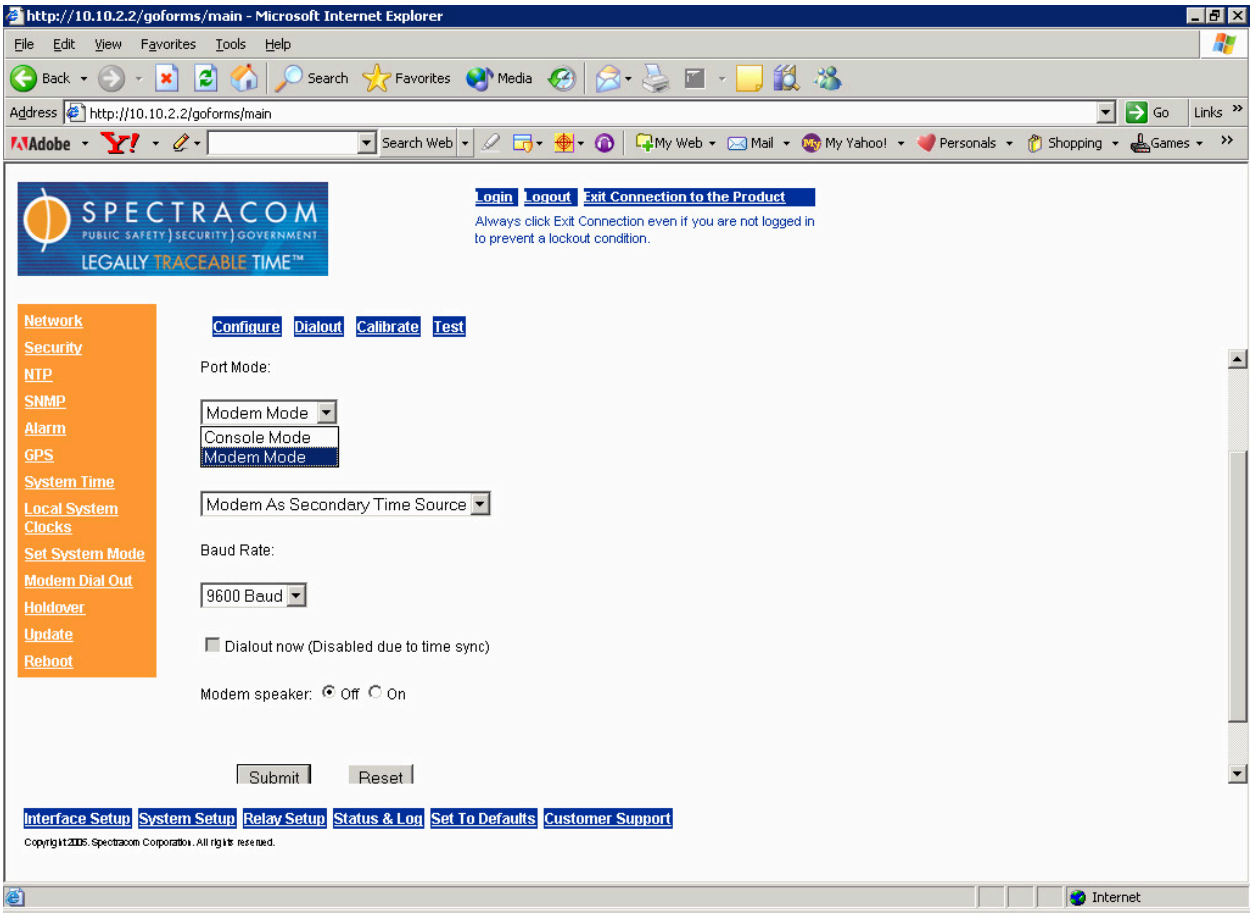


Figure 2-5: Modem Dial Out

2.4.3 Modem Command Line Commands

New modem line commands have been added to facilitate user operation and debugging of modem features. This supports customers in the field should there be issues concerning other dial-up time references.

The provided modem commands are:

mdo help	mdo help – Used to get detailed information for modem commands
mdo avg	mdo avg [on|off] [#|auto] – Set the averaging behavior of the modem
mdo log	mdo log [debug|normal] – Set logging mode
mdo stat	mdo stat [reset] – View or reset the modem statistics
mdo delaycomp	mdo delaycomp [spring|itur] [on|off] – Enable/disable delay compensation
mdo mode	mdo mode [console|modem] [1200|9600] – Set port mode and optionally change baud rate
mdo dialnow	mdo dialnow [test] – Dial out immediately
mdo baud	mdo baud [1200|9600] – Set baud rate
mdo speaker	mdo speaker [on|off] – Set modem speaker enable

2.4.3.1 mdo avg

Usage: mdo avg [on|off] [#|auto]
This command switches the averaging algorithm on and off. If averaging is turned on (**mdo avg on**), the number of points to average must be specified. If the number of points is specified as auto, the unit will choose the appropriate number. If no parameter is specified, the current state will be printed.

NOTE: By default, averaging is NOT used. Averaging is recommended only after a few successful dial-outs have been performed.

2.4.3.2 mdo log

This command allows the user to turn on logging of call data and state to debug files for use in providing feedback to Spectracom when testing with unsupported ACTS or ITU-R time references. The call data files are named call#.log and are found in the logs directory.

NOTE: Do not leave this mode switched on, as the number of log files increases with each call. Switch it on as directed by Spectracom if you are testing a new dial-up time service.

Enter **mdo log debug** to switch the log on. Enter **mdo log normal** to switch the log off. When detailed logging is enabled, every message from the modem is printed to a file. Remember that this mode should be used only for debugging, as files will accumulate.

2.4.3.3 mdo stat

This command allows the user to view or reset modem statistics. Enter **mdo stat** to print the statistics to the console. Enter **mdo stat reset** to reset the statistics.

2.4.3.4 mdo delaycomp

This command skips the delay compensation step in ACTS and ITU-R protocols. This is required in the UK when using the free ITU-R NPL format (only the pay-for-use format supports delay compensation). Skipping the delay compensation may be useful in debugging or synchronizing to untested ACTS or ITU-R protocols. If the modem indicates a No Sync error when calling and connecting, try disabling delay compensation.

NOTE: Disabling delay compensation reduces the accuracy of the time synchronization.

Enter **mdo delaycomp spring on** or **mdo delaycomp itur on** to enable delay compensation. Enter **mdo delaycomp spring off** or **mdo delaycomp itur off** to disable delay compensation.

2.4.3.5 mdo mode

This command sets the console mode and, optionally, changes the baud rate. Enter **mdo mode console** or **mdo mode modem** to switch between console and modem modes. Enter **mdo mode modem 1200** or **mdo mode modem 9600** to set the baud rate.

2.4.3.6 mdo dialnow

This command dials out the modem. Enter **mdo dialnow** to dial out immediately.

2.4.3.7 mdo baud

This command sets the baud rate.

NOTE: ITU-R protocols typically use 1200 baud, while ACTS protocols typically use 9600 baud. NIST ACTS may support either, but 9600 baud is recommended.

2.4.3.8 mdo speaker

Entering this command switches the modem speaker on and off. Enter **mdo speaker on** to enable the speaker and **mdo speaker off** to disable it.

2.5 NTP

The NTP Daemon has been extended to allow the user to define the Reference Identifier string. A Reference Identifier is a 4-byte field in the NTP packets indicating, in either numerical or ASCII format, the time source used by the NetClock. This field contains the Time Identifier, such as GPS, STCI (Serial Time Code Input), or Modem Format (ITUR, PTB, SP [SPRING], NPL etc.).

The user can set the Reference Identifier to indicate the actual time source, such as WWVB for a 9188 NetClock using the Serial Time Code Interface (STCI) to connect to a NetClock/2 or some other WWVB receiver. The user may also use the 4-byte field as an abbreviation for the location of the NetClock, such as NYC, CHI, BOS, etc. Refer to Figure 2-6.

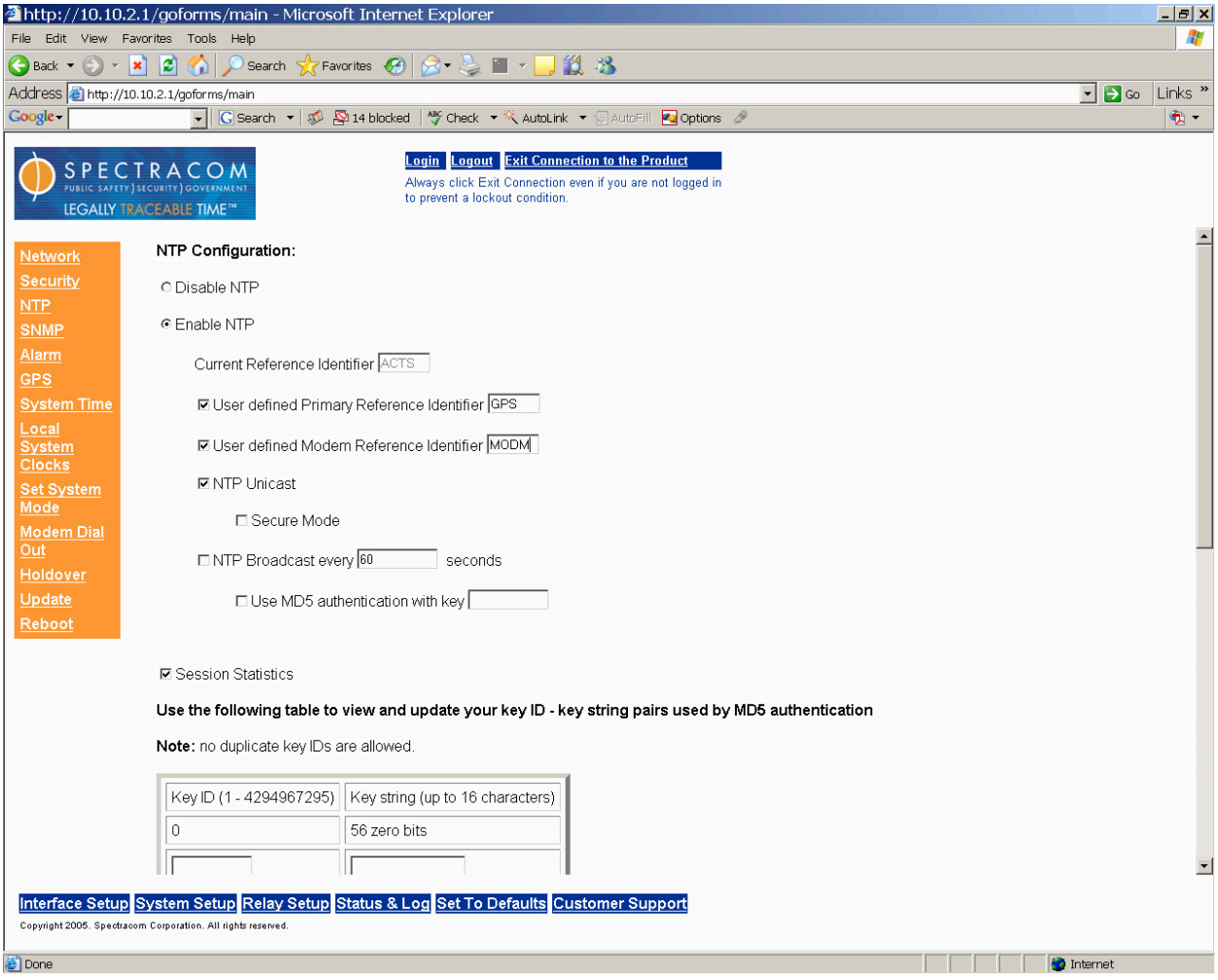


Figure 2-6: Reference Identifier Field

Spectracom provides a means to set a Reference Identifier for the primary time sources, such as GPS, Serial Time Code Input, or User Defined. A means to define the

Modem Reference Identifier separately is also provided for NetClocks that include a Modem as a backup time source (Figure 2-6).

2.5.1 NTP Command Line

The NTP Daemon also supports new commands for software version 2.3.1:

ntp refsrc ntp refsrc [primary|modem] [on|off] [‘4-character-string] – Sets NTP reference source

ntp timeout ntp timeout [seconds] – Used to set timeout for remote access tool

2.5.1.1 ntp refsrc

This command allows the user to set the primary and modem user-defined reference identifiers. Input this as **ntp refsrc [primary|modem] [on|off] ['4-character-string]** with the appropriate entries.

2.5.1.2 ntp timeout

This command allows the user to set the time difference allowed between the remote Network Access Tool and the NetClock. This is a security feature avoiding replay attacks. Enter **ntp timeout [seconds]** to set the value.

2.6 System Time

The System Time Tab found on the System Setup web page allows the user to view the current time on the unit using UTC or a Local Clock defined by the user. This page also allows the user to set (manually) the system time. The page has been modified for version 2.3.1 software to include two additional check boxes. The “Allow user to set time using SNMP or Web UI” checkbox allows user inputs from SNMP or this Web UI to set the system time manually. If the checkbox is NOT checked, users may not manually input time. Refer to Figure 2-7.

NOTE: When a user sets the time manually, the serial time code messages from the unit and the NTP packets will indicate that the NetClock is NOT synchronized. Setting the time manually means the unit is NOT traceable to UTC. When entering time manually, you MUST use UTC time. If you enter local time (or a time from any other time zone), the time will be misinterpreted as UTC.

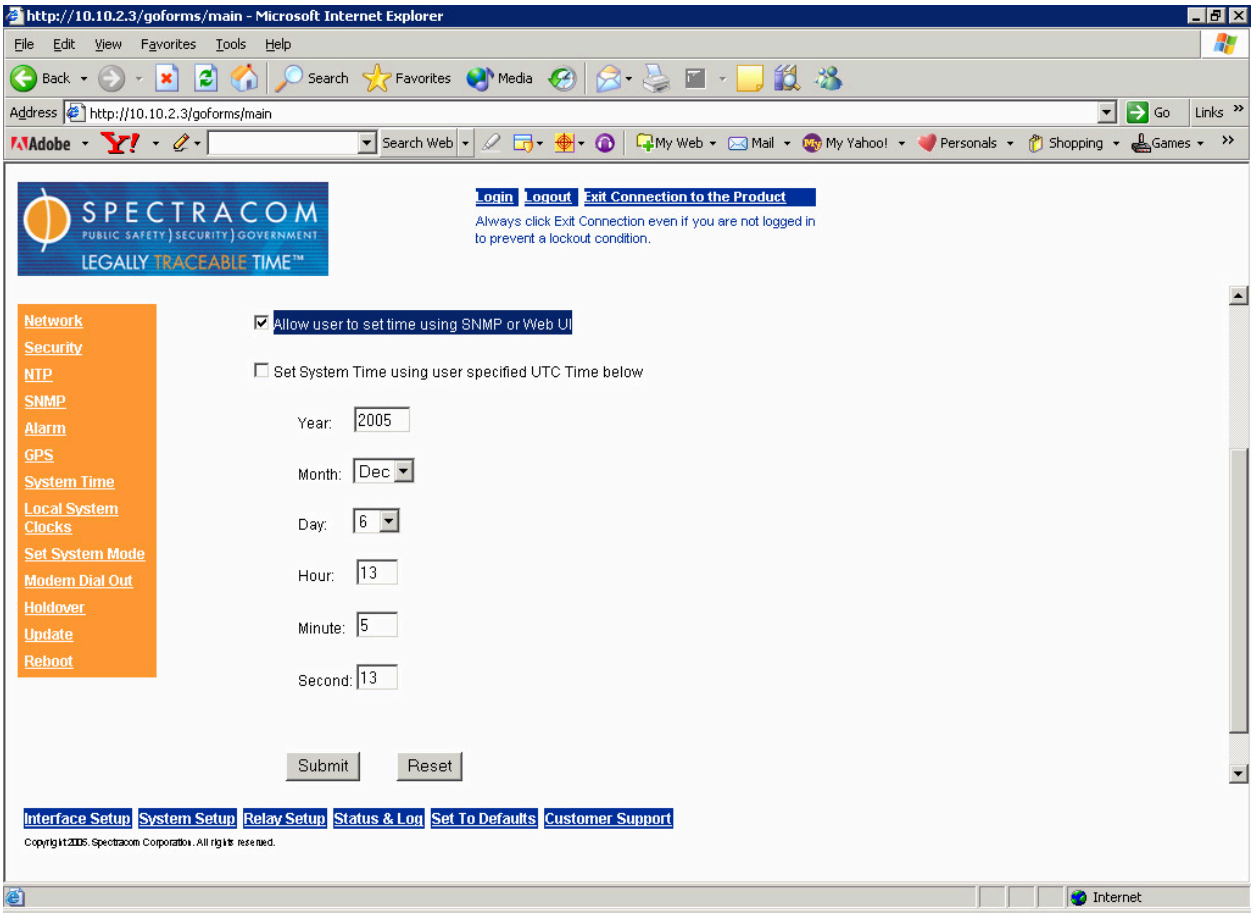


Figure 2-7: Setting System Time Options

2.7 Further Assistance

If you require additional assistance integrating this addendum with your operations and maintenance manual(s), please contact Spectracom Customer Service at 585.321.5800. Spectracom may also be reached through our website at www.spectracomcorp.com.

Spectracom Corporation
95 Methodist Hill Drive
Rochester, NY 14623
www.spectracomcorp.com
Phone: 585.321.5800
Fax: 585.321.5219