



SPECTRACOM
PUBLIC SAFETY) SECURITY) GOVERNMENT

MODEL 9188
NTP Ethernet Time Server
INSTRUCTION MANUAL

95 Methodist Hill Drive
Suite 500
Rochester, NY 14623

Phone: 585.321.5800
Fax: 585.321.5219

www.spectracomcorp.com

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

Part number 9188-5002-0050
Manual Revision H
October 2006

Current to software version 2.3.0 (refer to 2.3.1 Addendum)



Copyright © 2005 Spectracom Corporation. Contents of this publication may not be reproduced in any form without the written permission of Spectracom Corporation. Specifications subject to change or improvement without notice. Printed in USA.

Spectracom, NetClock, TimeView and Legally Traceable Time are Spectracom registered trademarks. All other products are identified by trademarks of their respective companies or organizations. All rights reserved.

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

1	GENERAL INFORMATION	1-1
1.1	Introduction.....	1-1
1.2	Warranty Information and Product Support	1-2
1.3	Unpacking.....	1-3
1.3.1	Package Contents	1-3
1.4	Model 9188 Specifications	1-4
1.4.1	RS-232 Serial Setup Interface Port	1-4
1.4.2	10/100 Ethernet Port	1-4
1.4.3	Protocols supported.....	1-4
1.4.4	RS-232 Communication Port (1)	1-5
1.4.5	RS-485 Connectors (2)	1-5
1.4.6	Front Panel LED Indicators	1-5
1.4.7	Relay Outputs.....	1-6
1.4.8	Input Power	1-6
1.4.9	Mechanical and Environmental	1-6
1.4.10	Agency Approvals	1-6
2	INSTALLATION.....	2-1
2.1	Installation Summary	2-1
2.2	Tools and cables required	2-2
2.3	Power and Ground Connection	2-2
2.4	Ethernet Network Cabling.....	2-3
2.5	CNC3000 cable kit	2-3
2.6	RS-485 Wiring and Set up.....	2-3
2.6.1	Remote Connections	2-4
2.6.2	Remote Output Usage	2-5
2.6.3	RS-485 Guidelines	2-5
2.6.4	Connection Method.....	2-6
2.6.5	Termination.....	2-10
3	PRODUCT CONFIGURATION	3-1
3.1	Network Configuration	3-1
3.1.1	To configure the product to work on a network via the Setup port	3-2
3.1.2	To configure the product to work on a network via the web browser user interface	3-4
3.1.3	Default and Recommended Configurations.....	3-6

3.2	Login.....	3-7
3.2.1	To Change the Default Login Password Values	3-9
3.2.2	To reset the current Login Password Values back to the factory default values ...	3-10
3.3	Configure the RS-485 Reference Input.....	3-11
3.4	Alarms.....	3-13
3.4.1	Alarm Outputs.....	3-13
3.4.2	Alarm log	3-13
3.5	Event Timer	3-14
3.5.1	Configuring the Event Timer	3-14
3.6	Interface Setup	3-18
3.6.1	Using the web browser user interface to configure any Interface	3-19
3.6.2	To configure a product's Interface via interface	3-19
3.7	“Set To Defaults” web browser user interface	3-21
3.8	Local System Clocks Setup	3-22
3.8.1	Time Zone and DST.....	3-25
3.9	Logs	3-28
3.9.1	Display Alarm Log	3-29
3.9.2	Display Event Relay Log	3-29
3.9.3	Display Operational Log.....	3-30
3.10	NTP/SNTP	3-31
3.10.1	Configure NTP.....	3-31
3.10.2	NTP Support	3-33
3.10.3	Application Note: MD5 Authentication using a Cisco Router	3-33
3.11	NTP Statistics	3-34
3.12	Relays	3-36
3.12.1	Configuring the relays.....	3-36
3.13	SNMP	3-38
3.13.1	SNMP Configuration	3-38
3.13.2	Spectracom MIB	3-42
3.13.3	SNMP Support.....	3-43
3.14	System Status.....	3-43
3.14.1	Dynamic System Information	3-43
3.14.2	Static System Information.....	3-45
3.14.3	System Test Results	3-45
3.14.4	System Features and Options.....	3-45
3.15	System Time	3-46
3.16	Variable Holdover.....	3-48
3.16.1	Setting the variable holdover value for the oscillator	3-49

4	OPERATION.....	4-1
4.1	Front Panel	4-1
4.1.1	Status Indicator	4-3
4.2	Rear Panel.....	4-4
4.3	Leap Second occurrence.....	4-6
4.3.1	Reasons for a Leap Second correction.....	4-6
4.3.2	Leap Second alert notification	4-6
4.3.3	Sequence of a Leap Second correction being applied	4-7
5	TROUBLESHOOTING.....	5-1
5.1	Front Panel Power and Sync Lamps.....	5-1
5.2	Front Panel LAN Connector.....	5-2
5.3	Verify operation of a Serial port.....	5-3
5.4	Verify operation of a Spectracom TimeTap.....	5-3
5.5	Customer Service	5-3
6	SERIAL DATA FORMATS	6-1
6.1	Format 0:	6-1
6.2	Format 1:	6-2
6.3	Format 2:	6-4
6.4	Format 3:	6-6
6.5	Format 4:	6-8
6.6	Format 7:	6-9
6.7	Format 8:	6-11
6.8	Format 90:	6-12
7	RS-232 SETUP PORT COMMANDS.....	7-1
7.1	help	7-2
7.2	login	7-3
7.3	logout.....	7-3
7.4	lrc	7-4
7.5	net	7-6

7.6	net gateway	7-6
7.7	net help.....	7-8
7.8	net ip.....	7-8
7.9	net mac	7-9
7.10	net mask.....	7-9
7.11	net show.....	7-10
7.12	net http	7-11
7.13	opt.....	7-12
7.14	reboot [bootloader]	7-13
7.15	rem.....	7-14
7.16	sec	7-15
7.17	sec help.....	7-15
7.18	sec level.....	7-17
7.19	sec password	7-17
7.20	ser	7-18
7.21	update.....	7-19
7.22	update app	7-19
7.23	update boot	7-20
7.24	update csl	7-20
7.25	update kern.....	7-21
7.26	update help	7-21
8	OPTIONS.....	8-1
8.1	Option 1: Security	8-2
8.1.1	Option 1 basics.....	8-2
8.1.2	Security overview	8-2
8.2	Configuring SSH.....	8-2
8.2.1	Overview.....	8-2
8.2.2	Managing Host Keys.....	8-3
8.3	Configuring HTTPS	8-11

8.3.1	Overview	8-11
8.3.2	Deleting Certificates, Private Keys, and Certificate Requests.....	8-11
8.3.3	Restoring Self Signed Certificates and Private Keys.....	8-12
8.3.4	Creating Self Signed Certificates, a Private Key, and a Certificate Request.....	8-12
8.3.5	Requesting Certificate Authority Certificates.....	8-14
8.3.6	Installing Certificates	8-15
8.3.7	Using Externally generated Certificates	8-15
8.3.8	What to do if you cannot get into a secure Spectracom Product	8-16

9 SW LICENSE NOTICES.....9-1

List of Figures

Figure 2-1: Remote Outputs.....	2-5
Figure 2-2: RS-485 Output.....	2-5
Figure 2-3: One-Way Bus Installation.....	2-7
Figure 2-4: Split Bus Configuration.....	2-7
Figure 2-5: Wire Strain Relief.....	2-8
Figure 2-6: TimeView RS-485 Interface.....	2-9
Figure 2-7: Model 8179T TimeTap RS-485 Interface.....	2-9
Figure 2-8: Model 9188 RS-485 Interface.....	2-10
Figure 2-9: TimeBurst RS-485 Interface.....	2-10
Figure 3-1: Serial Setup Interface port connector.....	3-2
Figure 3-2: Log-in Permissions.....	3-7
Figure 3-3: Configuration mode Log-in.....	3-8
Figure 3-4: Administrator mode Log-in.....	3-8
Figure 3-5: Set Serial Time Code Screen.....	3-12
Figure 3-6: Event Timer Relay Screen.....	3-14
Figure 3-7: Event Timer Relay Screen.....	3-15
Figure 3-8: Serial port connector.....	3-18
Figure 3-9: Interface Screen.....	3-20
Figure 3-10: Restore Interface setup back to factory defaults.....	3-21
Figure 3-11: Local System Clocks Setup Screen.....	3-22
Figure 3-12: Time Zone and DST Setup Screen.....	3-23
Figure 3-13: NTP Screen.....	3-31
Figure 3-14: NTP Statistics.....	3-34
Figure 3-15: Relay Output Screen.....	3-36
Figure 3-16: SNMPv1 Setup Screen.....	3-38
Figure 3-17: System Time.....	3-46
Figure 3-18: Oscillator variable holdover configuration.....	3-49
Figure 4-1: Front panel display.....	4-2
Figure 4-2: Rear panel illustration.....	4-5
Figure 4-3: Leap Second indication.....	4-7
Figure 8-1: SSH configuration Screen.....	8-3
Figure 8-2: Creating SSH host key files.....	8-4
Figure 8-3: Selecting SSH authentication modes.....	8-6
Figure 8-4: Adding SSH public key to authorized keys.....	8-7
Figure 8-5: Adding a new SSH public key file.....	8-8
Figure 8-6: Deleting SSL Certificate, Certificate Request and Private Key Files.....	8-11
Figure 8-7: Restoring user's Self Signed Certificate and Private Key Files.....	8-12
Figure 8-8: Creating a new Certificate Request and Self Signed Certificate.....	8-13
Figure 8-9: A new Certificate Request and Self Signed Certificate.....	8-14
Figure 8-10: Installing a new Certificate.....	8-15
Figure 8-11: Using External Certificate.....	8-16

List of Tables

Table 2-1: Time Zone Offsets available for Data Outputs	2-2
Table 2-2: Port 2 to Master Clock pin-out information	2-4
Table 2-3: Cable Sources for RS-485 Lines Over 1500 Feet	2-6
Table 2-4: Cable Sources for RS-485 Lines Under 1500 Feet	2-6
Table 3-1: Serial Setup port pin-outs	3-2
Table 3-2: Default and Recommended Configurations	3-6
Table 3-3: Serial Port Pin Assignments	3-18
Table 3-4: Descriptions of logs	3-28
Table 3-5: Estimated oscillator error rates	3-48
Table 3-6: Minimum and Maximum allowable holdover values	3-48
Table 4-1: Status Indicator	4-3
Table 5-1: Status of Front Panel Power and Sync lamps	5-1
Table 5-2: Status of Front Panel LAN connection	5-2
Table 6-1: Table of Quality Indicators	6-5
Table 7-1: Alphabetical List of Commands	7-1

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 Ethernet Time Server is a direct response to customer needs for cutting-edge synchronization technology at an affordable price.

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

The Spectracom Model 9188 is called an Ethernet Time Server as it provides disciplined timing using NTP (Network Time Protocol). Model 9188 Ethernet Time Servers utilize the NetClock Master Clock's capabilities to be able to provide NTP synchronization to isolated networks or to provide NTP synchronization from an existing NetClock that doesn't have an Ethernet output.

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

Set-up and reporting are web-enabled and 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 port, RS-485 data bus ports. Alarm outputs and programmable timer outputs are also provided.

The Ethernet Time Server system includes a CE/UL-approved power supply for international use 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 any 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 damage 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

- ☐ Model 9188 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 Resistor, 120Ω

1.4 Model 9188 Specifications

1.4.1 RS-232 Serial Setup Interface Port

Function:	Accepts commands to locally configure the IP network parameters for initial connectivity.
Connector:	DB9 female, pin assignments conform to EIA/TIA-574 standard, data communication equipment.
Character structure:	ASCII, 9600 baud, 1 start, 8 data, 1 stop, no parity.

1.4.2 10/100 Ethernet Port

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

1.4.3 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 Server:	For browser-based configuration and monitoring using Internet Explorer 5 or Netscape 6 per RFC 1945 and 2068.
HTTPS Server:	(Applicable to units with Option 1 Security enabled). For secure 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:	Standard configuration-Up to 16-character Telnet password, Telnet Disable, FTP Disable, MD5 Authentication. With Option 1 Security enabled- SSH utilities, HTTPS, HTTP Disable.
Connector:	RJ-45, Network IEEE 802.3.

1.4.4 RS-232 Communication Port (1)

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 user interface. Bit rate selections are 1200, 2400, 4800 and 9600 baud. There are eight Data Format selections available.

1.4.5 RS-485 Connectors (2)

Signal:	Selected time Data Format in RS-485 levels. Port 2 receives input once-per-second and Port 1 sends 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 user interface. Input and output Bit rate selections are 1200, 2400, 4800, and 9600 baud.

For Port 1 (Output port): There are eight output Data Format selections available.

For Port 2 (Input port): Data Formats 00, 02 and 08 as configured in the NetClock Master Clock are available as inputs.

Note: Data Format 8 is not available as an output from all Spectracom NetClock Master Clocks. Contact Tech Support for more information on Data Format 8.

1.4.6 Front Panel LED Indicators

Power:	Green, always on
Sync:	Tri-color LED indicates the time data accuracy and equipment fault
LAN:	Green: Good Link indicator Yellow: Activity

1.4.7 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.
---------------------	--

1.4.8 Input Power

Power source:	90 to 240 VAC, 47 to 63 Hz through an IEC 320 universal connector. North American AC power cord supplied. AC cables for other countries available locally.
DC input:	9.5 to 30 VDC, 10 watts, through a CE/UL/CSA-approved power adapter (supplied). The Spectracom P/N for the power adapter is PS06-0E0J-DT01.
Connector:	Barrel, 5.5mm O.D., 2.5 mm I. D.
Polarity:	Negative shell, positive center.

1.4.9 Mechanical and Environmental

Dimensions:	EIA 19" rack mount W x 1.75" H [1U] x 11.00" D (483 mm W x 44 mm H x 305 mm D).
Weight:	4.8 lbs. (2.2 kg).
Temperature:	32° to 122°F (0° to 50°C) operating range. -40° to 185°F (-40° to 85°C) storage range
Humidity:	10% - 95% relative humidity, non-condensing

1.4.10 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 Model 9188 Ethernet Time Server consists of the following steps:

- 1) Optional- install the rack-mount ears on the 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) Assign a static network IP address for the Ethernet Time Server using the Serial Setup Interface connector connected to a PC with the provided serial cable. (Refer to Section 3.1).
 - 4) Connect the Ethernet Time Server to a hub/switch on the network with a standard network cable. Verify the green Good Link lamp next to the Ethernet connector illuminates. (Refer to section 2.4).
 - 5) Connect the RS-485 data from the NetClock Master Clock's Remote RS-485 output to Port 2 on the rear panel of the Ethernet Time Server using a twisted-pair cable. (Refer to section 2.6.1). Terminate the RS-485 if necessary. (Refer to Section 2.6.5).
 - 6) Match the NetClock RS-485 output configuration and the Ethernet Time Server's RS-485 input by performing either of the following (Refer to section 2.6.1 and Section 3.3):
 - A) (Recommended method- but may affect other systems on the same RS-485 output port. Not available if the Master Clock is a NetClock/2). Configure the NetClock Master Clock's RS-485 Remote output that is connected to the Model 9188 with the Model 9188's factory default configuration of Data Format 2, 9600 baud. (Refer to Section 2.6.1 and the corresponding NetClock Master Clock instruction manual).
- OR
- B) Configure the Ethernet Time Server's RS-485 input as the same settings as the NetClock Remote output is currently configured as, using the "Set Serial Time Code" page in the web browser user interface. (Refer to the NetClock Master Clock instruction manual to determine the current configuration and to Section 3.3 to change the Model 9188's RS-485 input configuration).
 - 7) Verify the NetClock Master Clock front panel Time Sync lamp is solid green (The Model 9188 Ethernet Time Server won't synchronize to a NetClock Master Clock that isn't synchronized and won't synchronize the network if it isn't green).
 - 8) Verify the front panel Sync lamp turns from blank to green moments after it is connected to the Master Clock and the RS-485 configuration of the NetClock Master Clock and the Model 9188 are the same.
 - 9) Synchronize the network PC's via 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).
 - 10) 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 always reflects UTC (Even if the RS-485 input is configured as local time). 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.

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

2.2 Tools and cables required

- 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 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 (The Spectracom P/N for the power adapter is PS06-0E0J-DT01).

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 Ethernet Time Server 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 Ethernet Time Server 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 Ethernet Network Cabling

Spectracom Model 9188 Ethernet Time Servers provide a 10/100 Ethernet port for full NTP functionality as well as full web enabled configuration, monitoring and diagnostic support.

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

- Use standard CAT 5 cable with RJ45 connectors.
- When connecting to a hub, switch or router use a straight-through wired cable.
- When connecting directly to a PC, use a crossover wired cable.

2.5 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 RS-485 Wiring and Set up

2.6.1 Remote Connections

The NetClock has two rear-panel Remote RS-485 connections labeled **RS-485 1** and **RS-485 2**. **Port 2** is the RS-485 input from the Master Clock. **Port 1** is used as a time output port only to other devices. Refer to Figure 2-1: Remote Outputs.

Port 2 (Input port) needs to be connected to the Master Clock's RS-485 output port using a twisted-pair cable. Connect the "+", "-", and "G" pins of the supplied RS-485 terminal block connector to the corresponding pins on the selected Master Clock's Remote output connector. Refer to the Master Clock instruction manual and Table 2-2 for pin-out information.

For proper termination - If the Model 9188 is either the last device or the only device on the RS-485 bus from the NetClock, place the included 120 ohm resistor (Located in the ancillary kit) across the + Data and - Data pins (Insert resistor leads in the terminal block with the RS-485 bus wires). Refer to Section 2.6.5 for more information regarding termination.

Time Server	NetClock Master Clock	
Model 9188 Port 2 (Terminal block connector)	WWVB based NetClock/2 or Model 8182 <u>Remote output</u> (DB9F connector)	GPS based Model 8183 and 918x <u>Remote port</u> (Terminal block connector)
"+"	Pin 8 (+)	Pin 1 (+)
" - "	Pin 3 (-)	Pin 2 (-)
" G"	Pin 9 (G)	Pin 3 (G)

Table 2-2: Port 2 to Master Clock pin-out information

Note: The configuration of the RS-485 output data from the NetClock Master Clock and the RS-485 input of the Ethernet Time Server must be configured identically. Refer to Section 3.3.

Port 1 (Output port) provides a continuous once-per-second time data stream in the selected Data Format. There are seven-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, the baud rate and UTC time difference of each output is selectable. Refer to the Interface Set-up Section 3.6 for configuring these outputs.

A 3-position terminal block is supplied in the ancillary kit for each Remote Connections. Connector pin assignments are shown in Figure 2-1.

RS-485 REMOTE

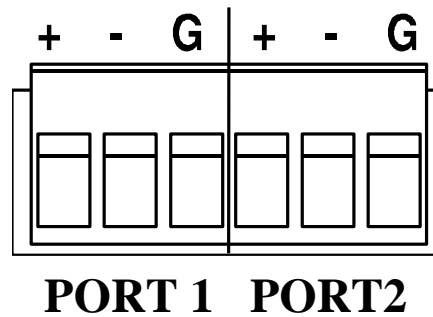


Figure 2-1: Remote Outputs

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

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

Error! Objects cannot be created from editing field codes.

Figure 2-2: RS-485 Output

2.6.2 Remote Output Usage

The Remote Output (Port1) provides 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 2-5 and Figure 2.6 illustrate typical RS-485 time data bus interconnections. Follow the guidelines listed below when constructing the RS-485 data bus.

2.6.3 RS-485 Guidelines

Cable selection: Low capacitance, shielded twisted pair cable is recommended for installations where the RS-485 cable length is expected to exceed 1500 feet. Table 2-3 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

2.6.4 Connection Method

The RS-485 transmission line must be connected in a daisy chain configuration as shown in Figure 2-3: One-Way Bus Installation. In a daisy chain configuration, the transmission line connects from one RS-485 receiver to the next. The transmission line appears as one continuous line to the RS-485 driver.

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

the insulating jacket as shown in Figure 2-5. Wrapping the wires in this manner prevents smaller gauge wires from breaking off when exposed to handling or movement.

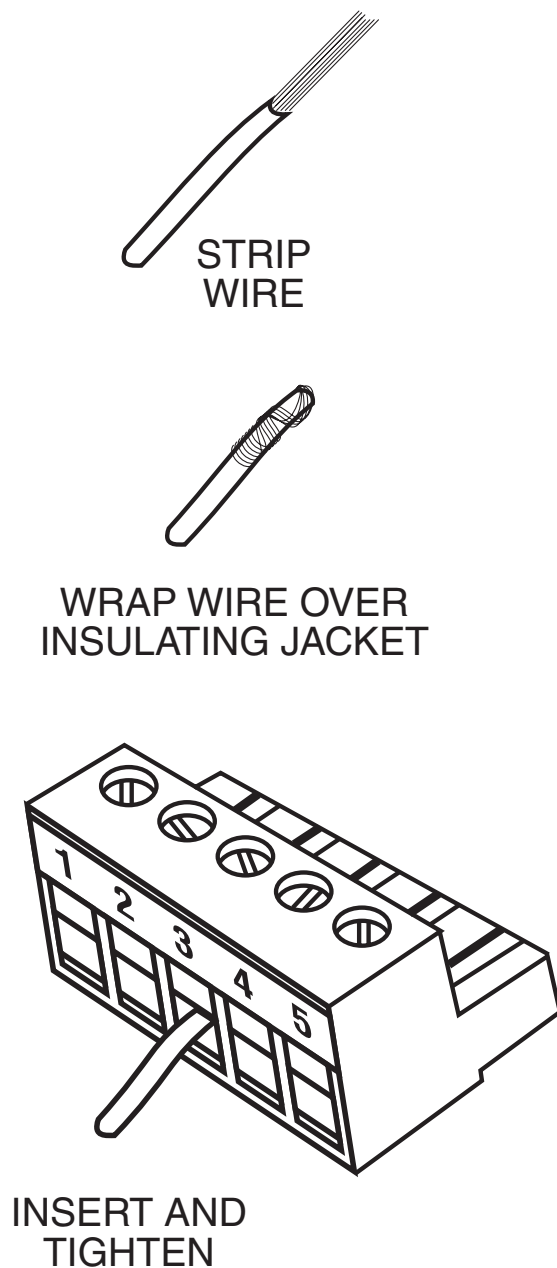


Figure 2-5: Wire Strain Relief

TimeView display clocks use a 6-position terminal block to connect to the RS-485 data bus. Connect the TimeView to the Ethernet Time Server's RS-485 Output as shown in Figure 2-6. The TimeView display clocks accept only Data Formats 0 or 1.

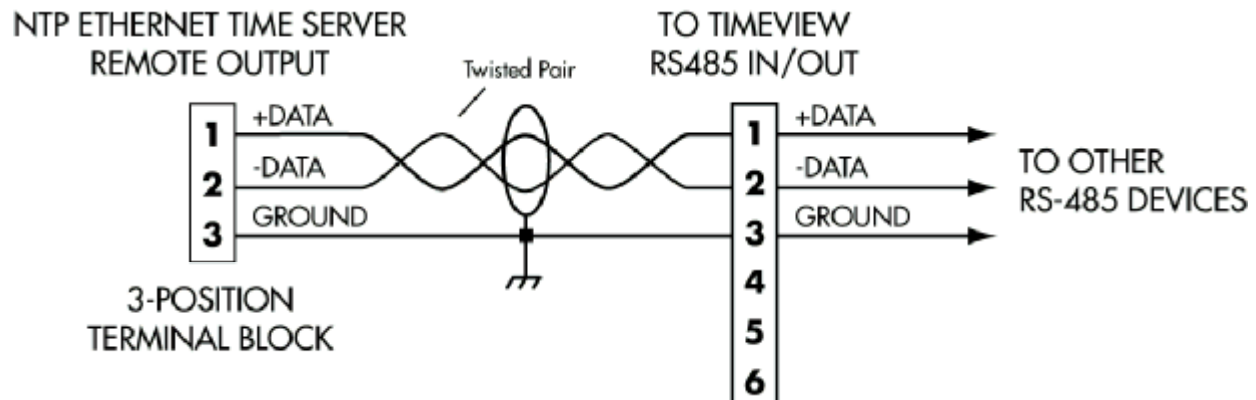


Figure 2-6: TimeView RS-485 Interface

The Model 8179T TimeTap is an RS-485 to RS-232 converter. The Model 8179T has a DB9 RS-232 interface that receives operational power from the RS-232 flow control pins RTS or DTR. Connect the TimeTap to the RS-485 data bus as shown in Figure 2-7.

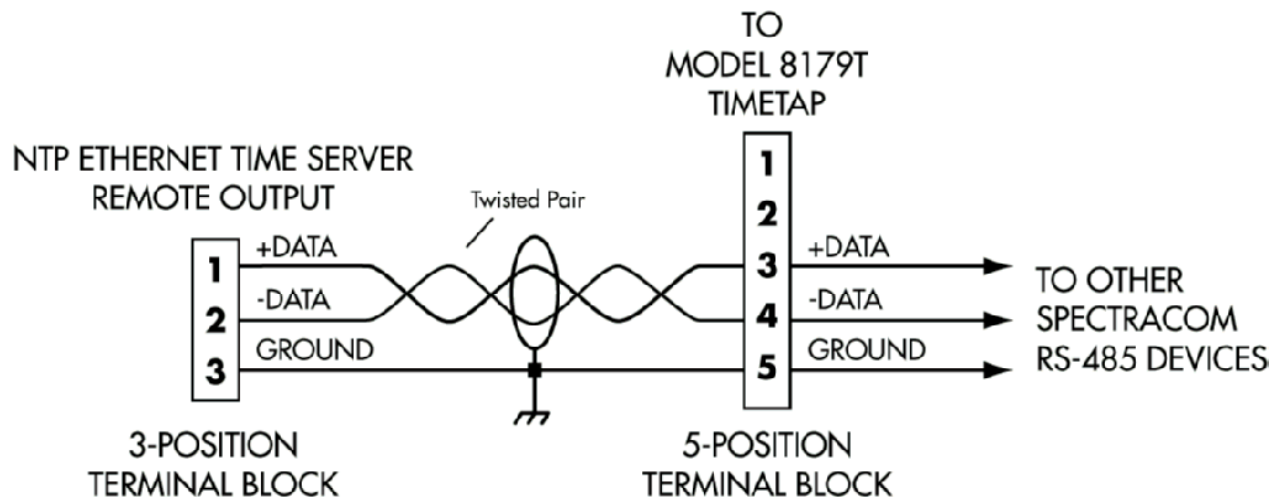


Figure 2-7: Model 8179T TimeTap RS-485 Interface

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 2-8.

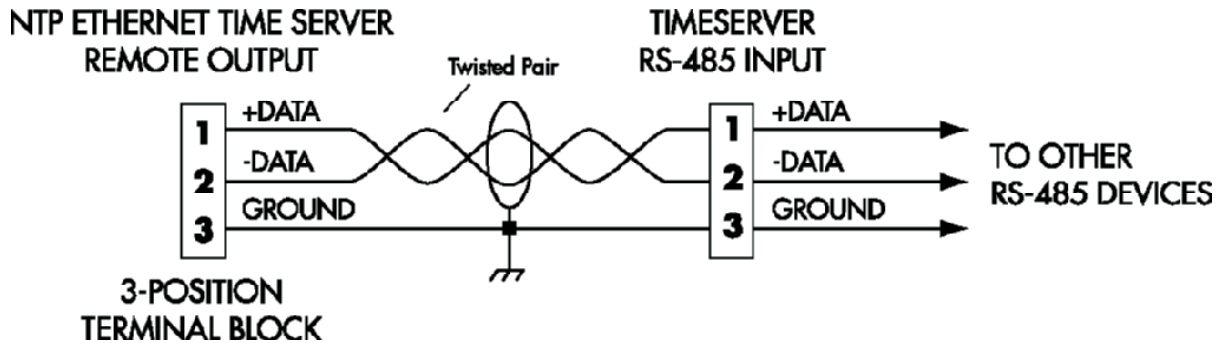


Figure 2-8: Model 9188 RS-485 Interface

The Model 8185, TimeBurst™, provides a digital time-of-day data burst to a radio transmitter. The TimeBurst accepts either Format 0 or Format 1. Connect the TimeBurst to the RS-485 data bus using a 3-position terminal block as shown in Figure 2-9.

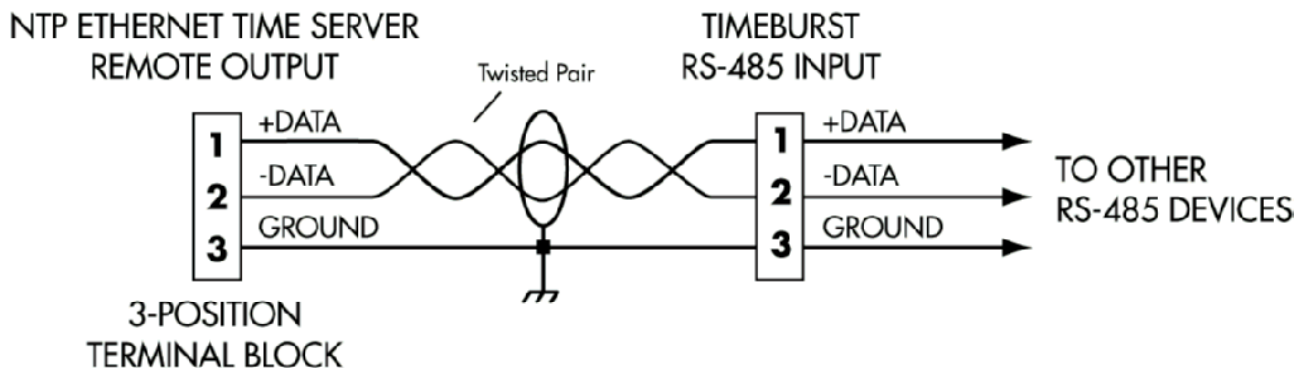


Figure 2-9: TimeBurst RS-485 Interface

2.6.5 Termination

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

For a one-way bus installation (Figure 2-5), terminate the last device on the bus. The RS-485 data bus can be split in two directions as shown in Figure 2-6. In a split bus configuration, terminate the devices installed on each end of the bus. Most Spectracom products include a built in termination switch to terminate the RS-485 bus when required.

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 Time Server'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 on Spectracom Time Servers with Option 1: Security enabled.

Note: 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 (Applicable when Option 1 Security is enabled).

Before the Ethernet Time Server can provide NTP time stamps to the network and access to the web browser user interface for configuration and logs can be obtained, the IP address of the Ethernet Time Server 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 RS-232 serial cable and a terminal emulator program (recommended method) OR they can be changed using a PC's network interface card connected directly to the front panel Ethernet port with a network cross-over cable. The PC will need to be configured with the IP address of 10.10.200.x (Where x is any number from 2 to 254).

3.1.1 To configure the product to work on a network via the 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 Ethernet Time Server. Port settings should be 9600 Baud, No parity, 8 data bits, 1 stop bit, No flow control. Power on the Ethernet Time Server.

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>

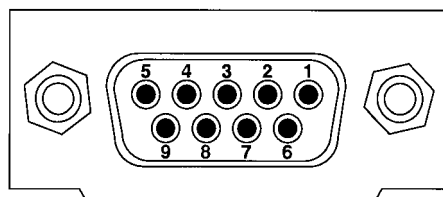


Figure 3-1: Serial Setup Interface port connector

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

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 configuration- or 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) For admin mode, type: **admin** <enter>. (**Note:** User logins and passwords are case sensitive).
 - * For config mode, type **config** <enter>
- 4) The unit will respond with “**Password:**”
- 5) For admin mode, Type **admin123** <enter> (For security reasons, the unit will not show what you type).
 - * For config mode, type: **config12** <enter> (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 “>” (Command prompt).

Note: Admin and config login lasts for 15 minutes or until the Ethernet Time Server is rebooted (Whichever occurs first). For security reasons, you will be exited out of the login after 15 minutes as the connections reset every 15 minutes.

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

To display or configure the IP address:

To display the current IP address, type **net ip** <enter>

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

To display or configure the Net Mask:

To display the current subnet mask, type **net mask** <enter>

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).

To display or configure the Gateway settings:

To display the current gateway configuration, type **net gateway** <enter>

To enable the gateway, type **net gateway yes xxx.xxx.xxx.xxx** <enter> (where x is the immediate network gateway’s IP address).

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

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.

1. Connect to the serial port of the unit.
2. Login with configuration- or administrator-level permissions with the 'login' command.
3. Type **net ip 10.10.200.5 <enter>** to set the IP address.
4. Type **net mask 255.255.255.128 <enter>** to set the subnet mask.
5. 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.

3.1.2 To configure the product to work on a network via the 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 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 [3.1.3](#) for instructions on web browser user interface login.

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

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

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

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

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

The Telnet and FTP settings are displayed as radio buttons.

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

1. Connect to the web browser user interface of the product.

2. Login to configuration- or administrator-level mode and browse to the Network configuration page.
3. Enter '10', '10', '200', and '5' in the corresponding IP Address fields.
4. Select '255.255.254.0' from the Subnet Mask pull down menu.
5. Choose the Gateway Enabled radio button.
6. Enter '10', '10', '200', and '10' in the corresponding Gateway Address fields.
7. Choose the Telnet Disabled radio button.
8. Choose the FTP Enabled radio button.
9. Review the changes made and click Submit. The browser will display the status of the change.

Note: If changing the IP address of the Ethernet Time Server to a different subnet, when you hit submit, the Ethernet Time Server will immediately start using the new IP address. This will cause the web browser user interface to stop responding. Move the Ethernet Time Server 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.

**Applicable when option 1 is enabled.

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:

1. *Configuration Mode* allows non-critical system changes.
2. *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.

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying `http://10.10.200.226/goforms/main`. The page header includes the Spectracom logo and the text "PUBLIC SAFETY | SECURITY | GOVERNMENT" and "LEGALLY TRACEABLE TIME™". Navigation links include "Login", "Logout", and "Exit Connection to the Product". A note states: "Always click Exit Connection even if you are not logged in to prevent a lockout condition."

On the left side, there is a vertical menu with the following items: "Alarm Log", "Event Relay Log", "Operational Log", "NTP Statistics", and "System Status".

The main content area displays two login modes: "Configuration Mode Login" and "Administrator Mode Login". Below these, a table lists the permissions for each mode.

Functionality	Config	Admin
Interface Setup	Y	Y
* Serial Port 1	Y	Y
* Remote Port 1	Y	Y
System Setup		
* Network	N	Y
* NTP	N	Y
* SNMP	N	Y
* Alarm	Y	Y
* System Time	N	Y
* Local System Clocks	N	Y
* Setup Serial Time Code	N	Y
* Holdover	N	Y
* Update	N	Y
* Reboot	N	Y
Relay Setup	Y	Y
Status & Log	Y	Y
Set To Defaults	Y	Y
Customer Support	Y	Y

At the bottom of the page, there is a row of buttons: "Interface Setup", "System Setup", "Relay Setup", "Status & Log", "Set To Defaults", and "Customer Support". Below this row, the copyright notice reads: "Copyright © 2005, Spectracom Corporation. All rights reserved."

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.

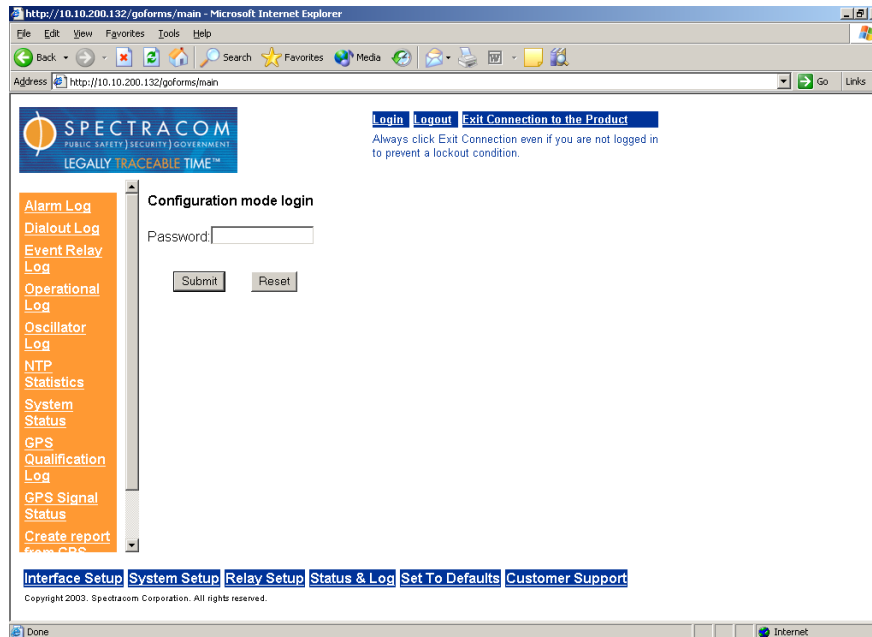


Figure 3-3: Configuration mode Log-in

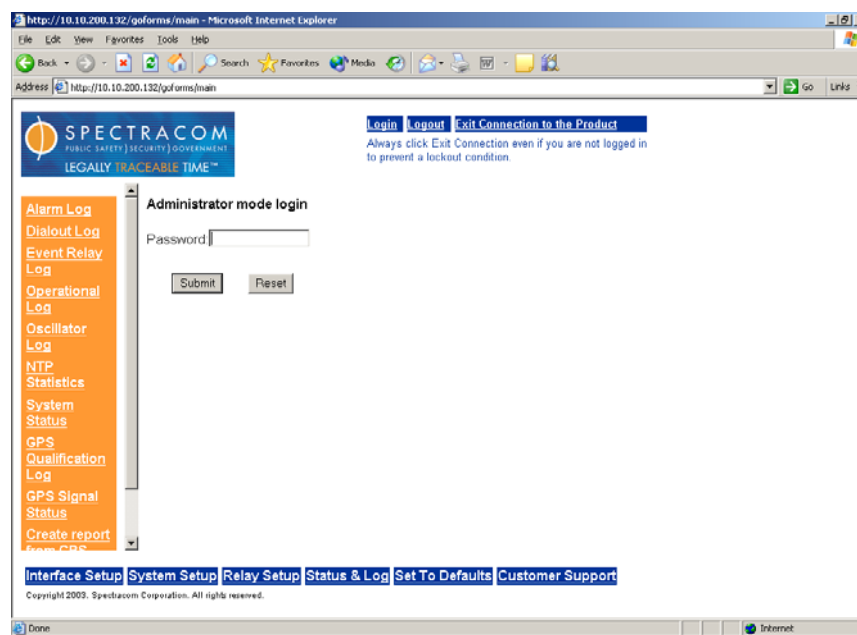


Figure 3-4: Administrator mode Log-in

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 browser user interface 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 the 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 Ethernet Time Server settings. For security reasons, only one connection session is supported at any one time, so this ensures that a new session can be activated immediately. If you don't log out or exit the connection, you will have to wait a time-out period or reset the unit to begin a new session.

3.2.2 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 desired 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.

- 1) 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).
- 2) With “**Spectracom Login:**” displayed, type **defaults** <enter> (If the login prompt is not displayed, hit the enter key).
- 3) When the Ethernet Time Server prompts for “**Password:**” just hit the enter key (Don’t enter a password).
- 4) 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**.
- 5) Using these current password values, follow the procedure in 3.2.1 to change these passwords to the desired values.

3.3 Configure the RS-485 Reference Input

The Ethernet Time Server accepts RS-485 data from the NetClock Master Clock. RS-485 Port 2 on the rear panel of the Ethernet Time Server is the input from the Master Clock's Remote output (Port 1 is an RS-485 output port only).

There are three RS-485 input time Data Format selections available on the Model 9188. These are Data Formats 0, 2 or 8 (Note that Data Format 8 is not available from any NetClock/2 or Model 8183 NetClock Master Clock and only certain Model 9183 and Model 9189 NetClock Master Clocks). By factory default, the Model 9188 is configured to accept the RS-485 data as Data Format 2, 9600 baud. The default factory configuration of all Spectracom Master Clock Remote RS-485 outputs is Data Format 0, 9600 baud. One of the following will need to be performed:

- 1) (This method is recommended if one or more Model 9188(s) is/are the only device(s) on that particular NetClock Remote output). The NetClock Master Clock Remote RS-485 output settings will need to be configured as Data Format 2, 9600 to match the Model 9188's input configuration. Refer to the appropriate NetClock Master Clock instruction manual for the procedure to change the Remote port configuration of the Master Clock.

OR

- 2) (This method is recommended if any devices other than the Model 9188, such as wall display clocks or other peripheral devices also need to be connected to the same Remote output along with the Model 9188). The Ethernet Time Server's port 2 (RS-485 input port) configuration will need to be changed to match the NetClock Master Clock's Remote RS-485 output configuration (Data Formats 0 or 8 with baud rates of 1200 to 9600).

The "Set Serial Time Code" page provides the RS-485 input configuration. Follow the simple steps below to quickly configure the RS-485 input to the Time Server.

Connect to your 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.

Click on the on "Set Serial Time Code" on the left side of the screen to enter the RS-485 input configuration page. Note: you must be logged in as an administrator to modify the NTP settings.

Note: Data Format 00 does not contain year information so the present year needs to be entered. The year only needs to be set during initial install if it is different than the year already entered in the "Set Serial Time Code" page. The year will automatically update every Dec 31st.

[Network](#)

[NTP](#)

[SNMP](#)

[Alarm](#)

[Set System](#)

[Time](#)

[Local](#)

[System](#)

[Clocks](#)

[Set Serial](#)

[Time Code](#)

[Update](#)

[Reboot](#)

The Serial Time Code Setup configures the expected input that this unit will receive from an external source. You must know what the source output settings are before proceeding.

BAUD RATE:

DATA FORMAT:

For data format 00, please enter year of the current UTC time.

If you select any other data format, the input from the year field will be ignored.

Valid year must be later than the year 1980 and earlier than year 2098.

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 3-5: Set Serial Time Code Screen

3.4 Alarms

3.4.1 Alarm Outputs

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

Timer/Alarm Relays output connector

For detailed information about the rear panel connectors, see the “Rear Panel Functions” section. For detailed information about configuring the relays to signal alarms, see Section [5.3.1](#).

System Status displayed on a web browser 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”.

3.4.2 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: Either the period of time allotted for operation without the NetClock Master Clock being time synchronized (Master Clock Time sync lamp is not solid green) or the RS-485 data from the NetClock is either not present or incorrectly configured has expired. This is known as the holdover mode of operation. Factory default period is 2 hours. This is a **Major** alarm.

Refer to section 3.16 for information on configuring the length of the holdover mode of operation.

Power Failure: The Ethernet Time Server has lost power. This is both a **Major** and **Minor** alarm.

3.5 Event Timer

3.5.1 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 [3.5.1](#) 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.



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

[Relay Output](#)
[Event Timer Relay](#)
[Current Event Schedule](#)
[Reset ALL Event Timers](#)
[Set Event Clock](#)
[Test Relays](#)

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

Event Scheduler ID (1 - 128)

[Edit/View](#)

Currently Scheduled Events

* Relay not configured as 'Event Timer'

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

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 3-6: 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 Offset

On the left side pane, select “Set Event Clock”. Choose an already defined Clock (Time Zone) or define a new one. See Section 3.8 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.



[Login](#) [Logout](#) [Exit Connection to the Product](#)

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

[Relay Output](#)

[Event Timer](#)
[Relay](#)

[Current](#)
[Event](#)
[Schedule](#)

[Reset ALL](#)
[Event Timers](#)

[Set Event](#)
[Clock](#)

[Test Relays](#)

Note: The time on this page should be UTC time.

Time accuracy is within 100 milliseconds.

Event Scheduler ID is 1

☒ Relay #1 ☐ Relay #2 ☐ Relay #3

☒ Enabled ☐ Disabled ☐ Delete

☒ ON ☐ OFF

Frequency:

☒ Hourly:

Minute Second Millisecond

☐ Daily:

Hour Minute Second Millisecond

☐ Weekly:

Day Hour Minute Second Millisecond

☐ Monthly:

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

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 1 st 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.

3.6 Interface Setup

The rear panel of the Ethernet Time Server has one RS-232 SERIAL COMM port. This port 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 available are listed in Section 6 Serial Data Formats.

The Serial port 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, Interface setup for more information. The SERIAL COMM port has a standard RS-232 pin configuration as shown in Figure 3-8 and Table 3-3.

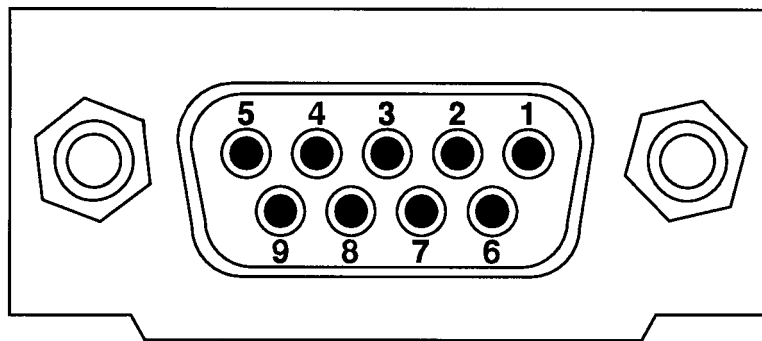


Figure 3-8: Serial port connector

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 3-3: Serial Port Pin Assignments

3.6.1 Using the web browser user interface to configure any Interface

The product has one RS-232 port (also called Serial Port) and one RS-485 output port (also called Remote Port) 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 above. 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 rules 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'.

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

3.6.2 To configure a product's Interface via 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.

[Serial Port 1](#)
[Serial Port 2](#)
[Remote Output 1](#)
[Remote Output 2](#)
[Front Panel Display](#)

BAUD RATE:
DATA FORMAT:
REQUEST CHAR: ☐ Multicast ☒ User defined
SYSTEM CLOCK: Click [here](#) to edit or create local system clocks.

Figure 3-9: 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 “Set To Defaults” web browser user interface

The “Set To Defaults” web browser user interface screen is used to return Serial Port 1 and Remote Port 1 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 then press the “Restore to factory defaults” button.

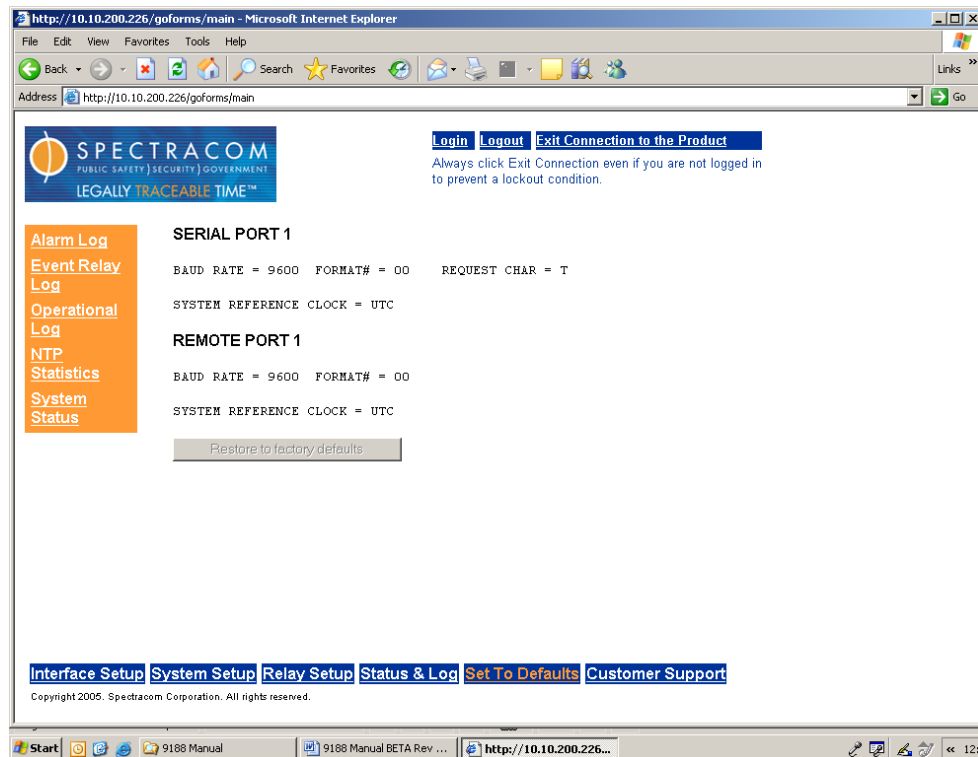


Figure 3-10: Restore Interface setup back to factory defaults

3.8 Local System Clocks Setup

You can define up to 5 Local Clocks or Time Zones to be used with any of the Remote, Serial, and event timers (The Local clock is not available for the Ethernet NTP output per the NTP specifications. When using NTP, each client on the network will handle corrections for local times). 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:

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:

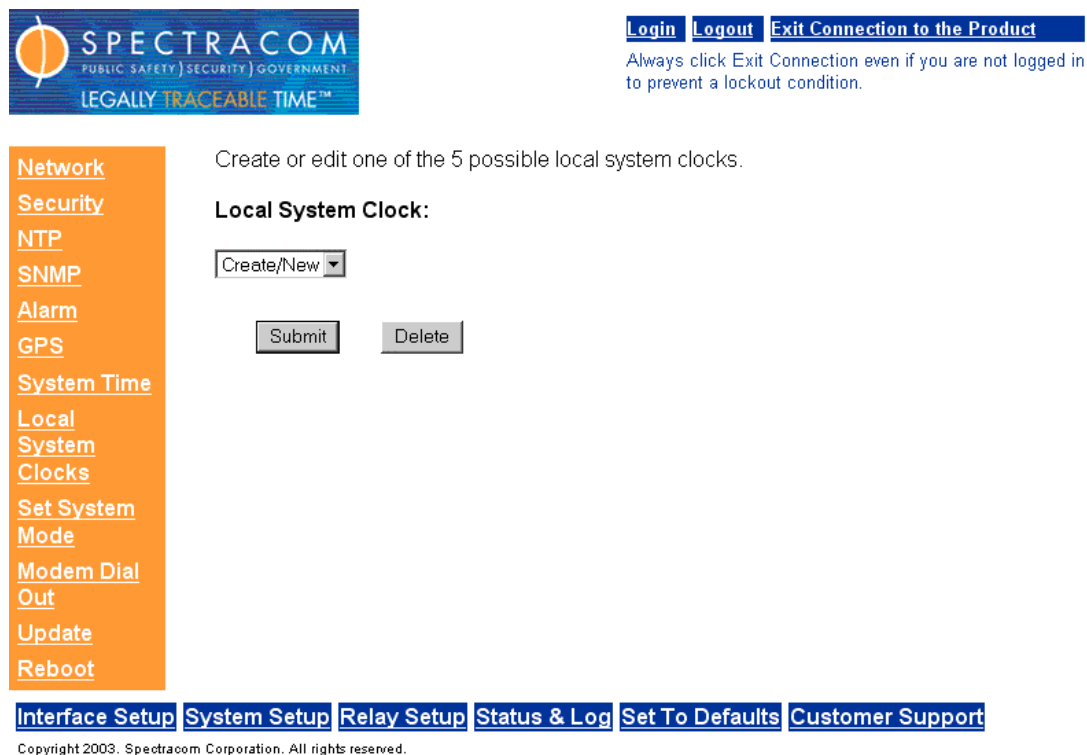


Figure 3-11: Local System Clocks Setup Screen

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

New Local Clock Name:

TIME ZONE SETUP:

- ☐ Automatically configure to unit's physical locality
- ☒ Manually defined UTC offset

DST SETUP:

- ☒ No DST rule, always standard time
- ☐ Automatically configure to unit's physical locality
- ☐ Manually defined by region
- ☐ Manually defined by week and day

DST In Date:

Week: Day: Month:

Hours: Minutes:

DST Out Date:

Week: Day: Month:

Figure 3-12: Time Zone and DST Setup Screen

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

Time Zone Setup:

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

DST Setup:

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

Manually specify a pre-defined DST rule.

- Europe

- North America
- Australia-1
- Australia-2

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

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

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

1. Connect to the web browser user interface of the unit.
2. Login to administrator-level mode and browse to the System Setup, Local System Clocks page.
3. Select Create/New and assign the clock a meaningful name.
4. Click on the “Manually Defined UTC Offset” button.
5. Select 'UTC+1:00' from the Time Zone pull down menu.
6. Select the 'No DST rule' radio button.
7. Review the changes made and click Submit. The browser will display the status of the change.

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

1. Connect to the web browser user interface of the unit.
2. Login to administrator-level mode and browse to the System Setup, Local System Clocks page.
3. Select Create/New and assign the clock a meaningful name.
4. Under “DST Setup”, select the 'Manually defined by week and day' radio button.
5. Enter/select '3rd', 'Friday', 'Apr', '2', and '0' in the DST In Date section.
6. Enter/select '1st', 'Sunday', 'Oct', '1', and '0' in the DST Out Date section.
7. Enter '1' and '0' in the corresponding fields of the Change Amount section.
8. Review the changes made and click Submit. The browser will display the status of the change.
9. Browse to the “Interface Setup, Remote Port” page and Select the proper System Clock.

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

1. Connect to the web browser user interface of the unit.
2. Login to administrator-level mode and browse to the System Setup, Local System Clocks page.
3. Select the desired Clock Name.
4. Select the 'Manually defined by month and day' radio button.
5. Enter/select '2', 'Oct', '1', and '1' in the DST In Date section.
6. Enter/select '17', 'Apr', '2', and '0' in the DST Out Date section.
7. Enter '0' and '30' in the corresponding fields of the Change Amount section.
8. Review the changes made and click Submit. The browser will display the status of the change.

3.8.1 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 browser user interface 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 user browser are configured as UTC plus or minus a set number of hours. For **Eastern**, chose UTC-5, for **Central**, chose UTC-6, for **Mountain**, chose UTC-7 and for **Pacific**, chose UTC-8.

DST rule

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

No DST Rule, always standard time

This option should only be used when you do not want to apply any DST rule to this Interface output.

Auto DST

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

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

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

Note: 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.

3.9 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	Event Relay Log	Operational Log
Purpose	Reports any status change of Major or Minor alarms (On/Off).	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 any boot of the unit, time source changes, and sync acquisition or loss. All system time adjustments are also shown here.
Where	Top of left menu under Status & Log tab in web browser user interface	Next on menu	Next on menu
Update frequency	Per alarm state change	Per alarm or scheduled event.	Per boot up or system time change
Maximum log size	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
Log rollover typical	Months	Months	Months

Table 3-4: Descriptions of logs

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

3.9.1 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= 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 UNIT LOST Time Sync on May 5th at 18:23:39 UTC. Then, the unit regained Time sync moments later at 18:24:44 UTC. This cleared the Major alarm occurrence.

3.9.2 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](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.

3.9.3 Display Operational Log

To Display the Operational log do the following:

Use a PC with a web browser and connect to the product by typing in the IP address into the address window of the browser as follows: [http:// 10.10.200.1](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 9188

Software Version 2.3.0 Date: 07/12/2005

Unit Started 15:15:27 2005-07-18

Serial Port 1 Version 2.03

Remote Port 1 Version 2.03

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 the NetClock Master Clock 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.

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 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.

3.10.1 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.

The screenshot shows the Spectracom web interface for NTP configuration. At the top left is the Spectracom logo with the tagline 'LEGALLY TRACEABLE TIME™'. To the right are links for 'Login', 'Logout', and 'Exit Connection to the Product', with a note: 'Always click Exit Connection even if you are not logged in to prevent a logout condition.' On the left is a vertical navigation menu with links: Network, Security, NTP (highlighted), SNMP, Alarm, GPS, System Time, Local System Clocks, Set System Mode, Modem Dial Out, Update, and Reboot. The main content area is titled 'NTP' and contains the following options: 'Disable NTP' (radio button), 'Enable NTP' (radio button, selected), 'NTP Unicast' (checked checkbox), 'Secure Mode' (unchecked checkbox), 'NTP Broadcast every 60 seconds' (checkbox and text input), 'Use MD5 authentication with key' (checkbox and text input), and 'Session Statistics' (checked checkbox). Below these is a section titled 'Use the following table to view and update your key ID - key string pairs used by MD5 authentication' with a note: 'Note: no duplicate key IDs are allowed.' The table has two columns: 'Key ID (1 - 4294967295)' and 'Key string (up to 16 characters)'. The first row shows '0' and '56 zero bits'. The second row has empty text input fields. At the bottom are links for 'Interface Setup', 'System Setup' (highlighted), 'Relay Setup', 'Status & Log', 'Set To Defaults', and 'Customer Support'. A copyright notice at the very bottom reads: 'Copyright 2003. Spectracom Corporation. All rights reserved.'

Key ID (1 - 4294967295)	Key string (up to 16 characters)
0	56 zero bits
<input type="text"/>	<input type="text"/>

Figure 3-13: 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: multicast mode is only used with select NTP based client software programs. Multicast mode is seldom 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.

3.10.2 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>.

3.10.3 Application Note: MD5 Authentication using a Cisco Router

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

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

where:

public_keynum is a number from 1 to 4,292,945,295 and is a key ID number

“trusted” is used to activate the key, “untrusted” to disable the key

md5 means the keyword (the type of key, Cisco only uses md5)

“secret_keystring” is the key value, it is from 1 to 32 printable characters.

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

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

```
set ntp key 3 trusted md5 TICKTOCK
```

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

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


3.11 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](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:



[Login](#) [Logout](#) [Exit Connection to the Product](#)

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

[Alarm Log](#)
[Dialout Log](#)
[Event Relay Log](#)
[Operational Log](#)
[Oscillator Log](#)
[NTP Statistics](#)
[System Status](#)
[GPS Qualification Log](#)
[GPS Signal Status](#)
[Create report from GPS Qualification Log](#)

Overall Statistics

Total clients	4
Total requests received	4492
Total requests processed	4492
Total authenticated requests	55
Total invalid requests	34
Total requests dropped	7
Total requests responded to	4475
Total response errors	0

Client Statistics

IP Address	Requests	Processed Reqs	Authenticated Reqs	Invalid Reqs	Dropped Reqs	Request Responses	Response Errors	Time of Last Req	Last Request Invalid?
192.168.0.94	3191	3191	0	17	0	3174	0	09/09/04 12:57:39	YES
10.10.200.195	1283	1283	55	17	0	1283	0	09/09/04 12:57:35	NO
10.10.200.200	11	11	0	0	0	11	0	09/08/04 21:12:24	NO
10.10.200.129	7	7	0	0	7	7	0	09/09/04 12:50:45	NO

[Refresh](#) [Reset](#)

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 3-14: 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 Ethernet Time Server has received NTP packets from, up to a maximum of 200.

Requests: Number of NTP packets received by the Ethernet Time Server from a client or clients.

Processed Requests: Number of NTP packets received that were processed by the Ethernet Time Server. The Ethernet Time Server 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 Ethernet Time Server that were processed, included authenticator fields, and authenticated successfully.

Invalid Requests: Number of NTP packets received by the Ethernet Time Server 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 Ethernet Time Server 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 Ethernet Time Server 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. Ethernet Time Server supports requests using versions 1, 2, 3, or 4.

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

Response Errors: Number of NTP request packets received by the Ethernet Time Server 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.

3.12 Relays

3.12.1 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.

SPECTRACOM
PUBLIC SAFETY | SECURITY | GOVERNMENT
LEGALLY TRACEABLE TIME™

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

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

	Major Alarm	Minor Alarm	Event Timer
Relay 1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Relay 2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Relay 3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 3-15: 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.”

3.13 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).

3.13.1 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.

http://10.10.200.110/goforms/main - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Media

Address http://10.10.200.110/goforms/main Go Links

SPECTRACOM
PUBLIC SAFETY SECURITY GOVERNMENT
LEGALLY TRACEABLE TIME™

[Login](#) [Logout](#) [Exit Connection to the Product](#)

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

Network
[Security](#)
[NTP](#)
[SNMP](#)
[Alarm](#)
[GPS](#)
[System Time](#)
[Local System Clocks](#)
[Set System Mode](#)
[Holdover](#)

SNMP Configuration:

☐ Disabled

☒ Enabled

☒ SNMPv1

SNMPv1 Access		
Permission	Community Name	Network Access
Read	public	0.0.0.0/0
Read/Write	private	0.0.0.0/0

Figure 3-16: 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”.

Holdover

Update

Reboot

☒ SNMPv2c

SNMPv2 Access		
Permission	Community Name	Network Access
Read	public	0.0.0.0/0
Read/Write	private	0.0.0.0/0

Figure 3.13-2: 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”.

http://10.10.200.110/goforms/main - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Mail Print

Address http://10.10.200.110/goforms/main Go Links >>

SPECTRACOM
PUBLIC SAFETY SECURITY GOVERNMENT
LEGALLY TRACEABLE TIME™

[Login](#) [Logout](#) [Exit Connection to the Product](#)

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

SNMPv1/SNMPv2c Traps

Trap Community

Trap Destination/Version	
Destination	Version
<input type="text" value="192.168.0.1"/>	<input type="text" value="v1"/>
<input type="text" value="192.168.0.2"/>	<input type="text" value="v2"/>
<input type="text"/>	<input type="text" value="none"/>
<input type="text"/>	<input type="text" value="none"/>
<input type="text"/>	<input type="text" value="none"/>

Network
Security
NTP
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Holdover

Figure 3.13-3: 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.

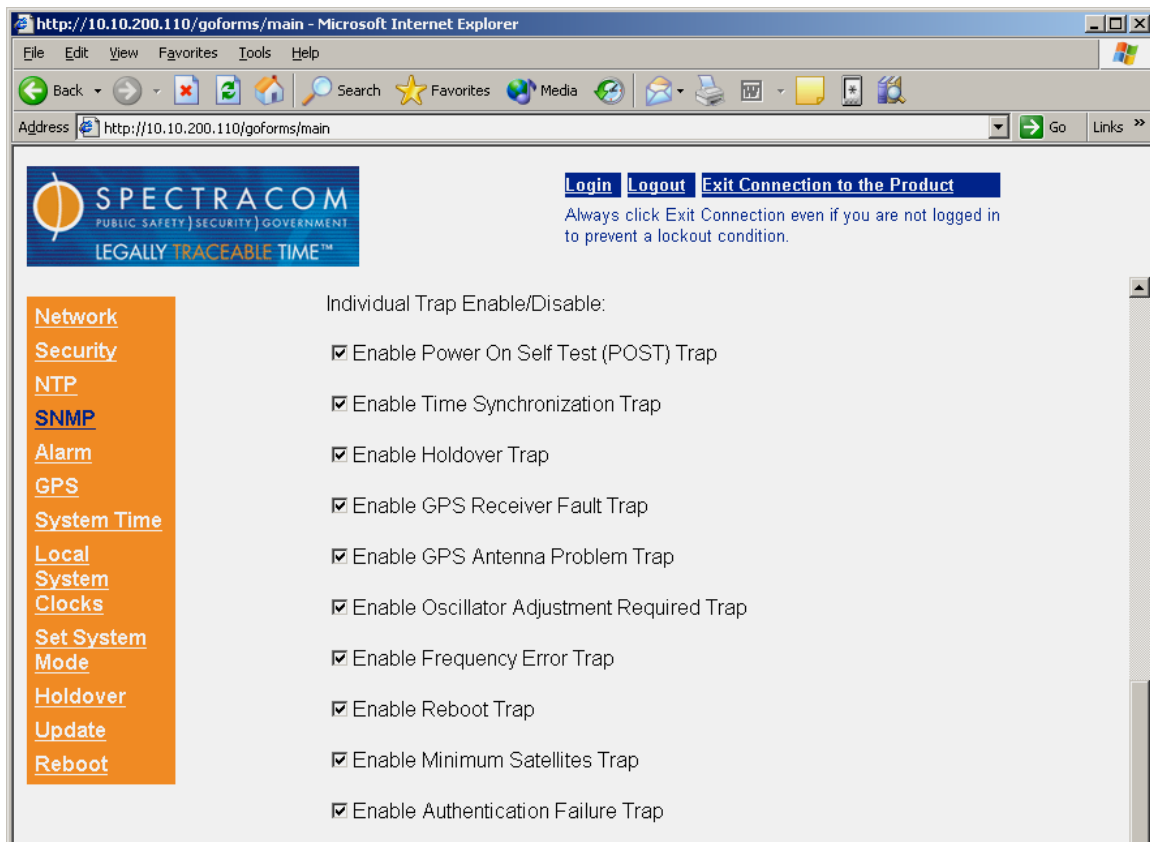


Figure 3.13-4: Trap selection Setup Screen

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 Time Server. Unchecking the box in front of each trap will prevent that particular trap from being sent.

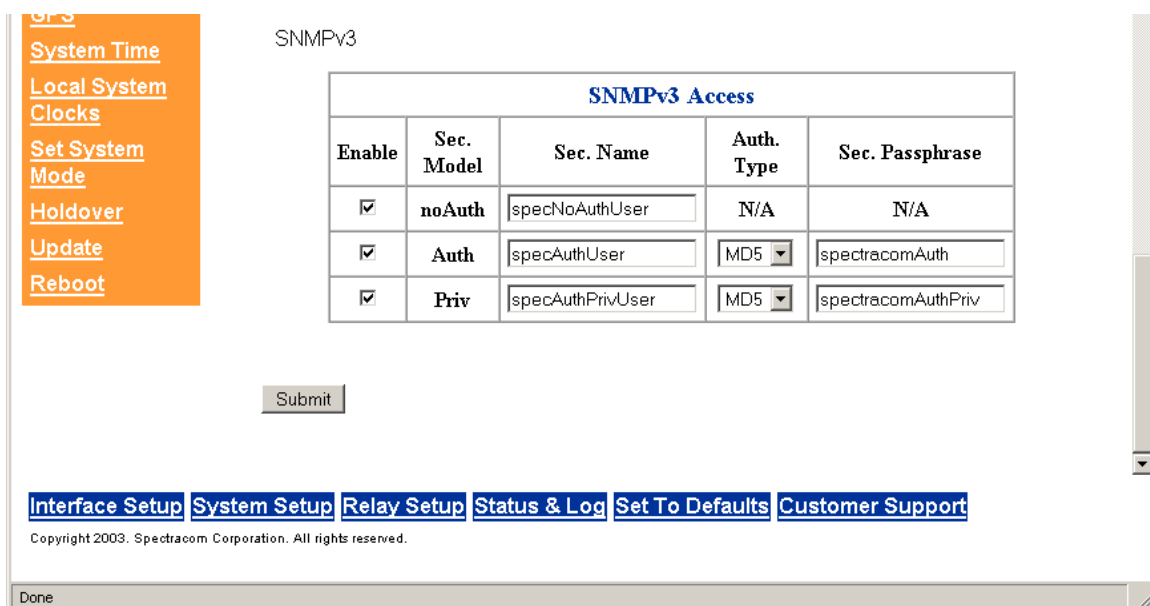


Figure 3.13-5: SNMPv3 Setup Screen

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.

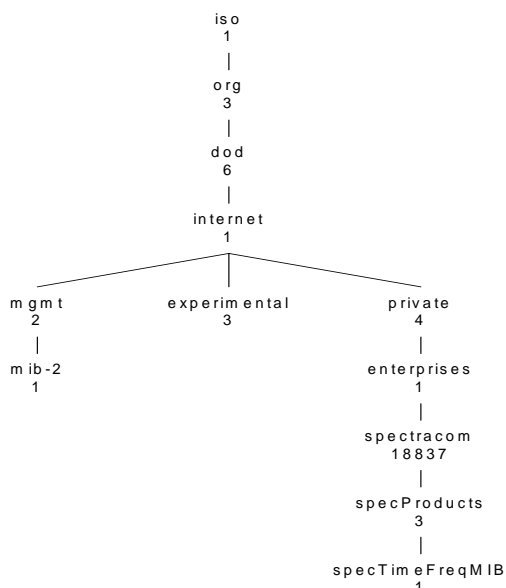
SNMPv3 (auth) – By enabling this access scheme, SNMP network managers may use SNMP version 3 protocol to manage the device. This level of SNMPv3 has you select a form of PDU authentication (MD5 or SHA) but does not use DES encryption. You may specify your own user name and pass phrase for this level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

3.13.2 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.



3.13.3 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 Ethernet Time Server 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 an Ethernet Time Server 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.

3.14 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 in 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"

3.14.1 Dynamic System Information

Uptime: 0 years, 6 days, 23 hours, 19 minutes, 6 seconds
Current internal temperature: 0.00 C (32.00 F)
Major Alarm is (OFF)
Minor Alarm is (OFF)

Time Sync status: In Sync
Time Source: Serial Time Code Input

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.
- **Serial Time Code Input** – The Model 9188 uses the RS-485 Serial Time Code Input from the NetClock Master Clock as a Primary Time Source since it does not have a GPS Receiver.
- **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. Note that User mode does not allow synchronization of the PC's or other devices connected to the Ethernet Time Server. Other systems will normally ignore the Time Stamp in this mode.

3.14.2 Static System Information

Product Name is Spectracom Corp. Model 9188
Application Name is 91XX
Application Rev is 2.3.0
Application Date is 07/28/2005
Boot Monitor Rev is 2.3.0
Unit's Serial Number: 595
MAC Address: 00:0c:ec:00:02:53

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

3.14.3 System Test Results

PCB Test	PASSED (PCB rev: 3)
PCC Test	PASSED (PCC rev: 3)
CSL Test	PASSED (CSL rev: 14)
RTC Test	PASSED
Serial Time Code Input	PASSED
Temp Sensor	PASSED
Serial Port 1	PASSED (2.03)
Remote Port 1	PASSED (2.03)

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

3.14.4 System Features and Options

Serial Port 1	ENABLED
Remote Port 1	ENABLED
Relays	ENABLED
Serial Time Code Input	ENABLED
NTP Server	ENABLED
TCXO Oscillator	ENABLED

The **System Features and Options** section provides the current status of all the features and options that are available for the Ethernet Time Server. Features that are currently turned on will indicate "ENABLED". Features that indicate "DISABLED" are not enabled. Option 1, Security 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**.

3.15 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 Ethernet Time Server currently is set to. This feature reads the information that the Ethernet Time Server is providing to the external equipment that is syncing to this device.

Note: Manually setting the time or date removes the Time Sync status. Most external devices, including network PC's will ignore the information from the Ethernet Time Server in this state.

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 3-17: System Time for more details. Note: You must be logged into the administrator mode to make any changes to this page.

The screenshot shows a web browser window with the address bar displaying `http://10.10.200.94/goforms/main - Microsoft Internet Explorer`. The page header includes the Spectracom logo with the tagline "PUBLIC SAFETY | SECURITY | GOVERNMENT" and "LEGALLY TRACEABLE TIME™". Navigation links for "Login", "Logout", and "Exit Connection to the Product" are present, along with a note: "Always click Exit Connection even if you are not logged in to prevent a lockout condition."

The left sidebar contains a menu with the following items: Network, Security, NTP, SNMP, Alarm, GPS, System Time (highlighted), Local System Clocks, Set System Mode, Modem Dial Out, Holdover, Update, and Reboot.

The main content area is titled "Local System Clock:" and features a dropdown menu set to "UTC" and a "Submit" button. Below this, it displays the "Current UTC Time: 21:37:28" with a note: "(Elapsed time based on browser clock. Click 'System Time' to update.)".

Two notes are provided: "Note: The date and time cannot be set on clocks tracking GPS satellites. They are overwritten with the received date and time information. Valid year must be later than year 1980 and earlier than year 2038." and "Note: The date and time must be set as UTC time."

Form fields for setting the time are provided: Year (2005), Month (Jun), Day (29), Hour (21), Minute (37), and Second (23). "Submit" and "Reset" buttons are located below these fields.

The bottom of the page features a blue navigation bar with links: Interface Setup, System Setup, Relay Setup, Status & Log, Set To Defaults, and Customer Support. A copyright notice at the bottom reads: "Copyright 2005. Spectracom Corporation. All rights reserved."

The Windows taskbar at the bottom shows the Start button, several open applications including Windows Explorer, Secure CustService, CUSTOMER SERVICE, and the current browser window, along with a system clock showing 5:38 PM.

Figure 3-17: 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 Ethernet Time Server is providing to the other devices it is syncing to.

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 Ethernet Time Server will not be synchronized and indicators in all of the outputs will be flagged as unsynchronized. Most software programs including NTP will ignore the Ethernet Time Server when these status messages indicate that the Ethernet Time Server is not synchronized.

When manually setting the time of the Ethernet Time Server, 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 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 Ethernet Time Server 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 the external reference.

3.16 Variable Holdover

The time interval between the loss of the primary external reference and the moment that the Ethernet Time Server declares loss of Time Sync is known as holdover mode. 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 stable 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 Ethernet Time Server 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.

The estimated error rates for the oscillator are listed below.

Estimated Error Rates	Time to reach 2 ms
1.0 milliseconds / hour (nominal)	2 hours (typical)
7.2 milliseconds / hour (worst case)	17 minutes*

Table 3-5: Estimated oscillator error rates

Note: The oscillator 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.

Limits on the minimum and maximum length of allowable holdover have been placed on the oscillator as shown below in Table 3-6.

Minimum Length	Maximum Length
15 minutes	24 hours

Table 3-6: 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.

3.16.1 Setting the variable holdover value for the oscillator

The user interface for the oscillator looks like:

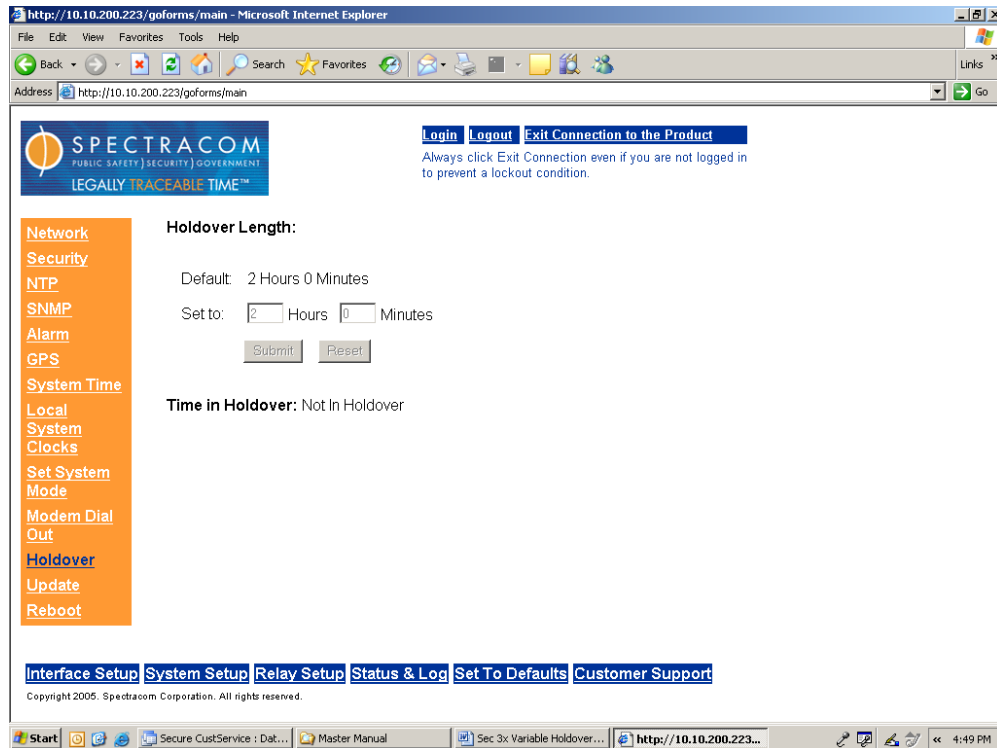


Figure 3-18: Oscillator variable holdover configuration

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 Ethernet Time Server 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.”**

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 Time Server.

Time in Holdover

Time in Holdover displays either the amount of time that the Ethernet Time Server 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 Ethernet Time Server consists of one Ethernet connector which has two small indicator lamps and two main status LED's. The two status lights are "Sync" and "Power".

The Spectracom Ethernet Time Server 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 Ethernet Time Server 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 user interface. 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 LED's.

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

- **Blink** is defined as 1/2 second on, 1/2 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 Ethernet Time Server. Power is disconnected.
SYNC	Multi	Off	No fault but not synchronized to the NetClock Master Clock. Holdover spec has not been met.
		Green On	Synchronized to the NetClock. Time is valid and within the Locked to Master Clock accuracy specs.
		Blinking Green	Holdover mode. Not synchronized to NetClock but time is still within Holdover accuracy specs.
		Yellow On	No longer synchronized to the NetClock 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 synchronize to the NetClock.
		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 Ethernet Time Server 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 **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.

RS-485 port 1 provides an RS-485 data output for synchronizing devices that accept an RS-485 input, such as wall display clocks and other Time Servers.

RS-485 port 2 provides an RS-485 data input from the NetClock Master Clock to allow the Ethernet Time Server to synchronize to the NetClock Master Clock.

Serial Comm 1 is a "DB9 female" connectors that provide RS-232 data output to devices that can accept an RS-232 input for synchronization.

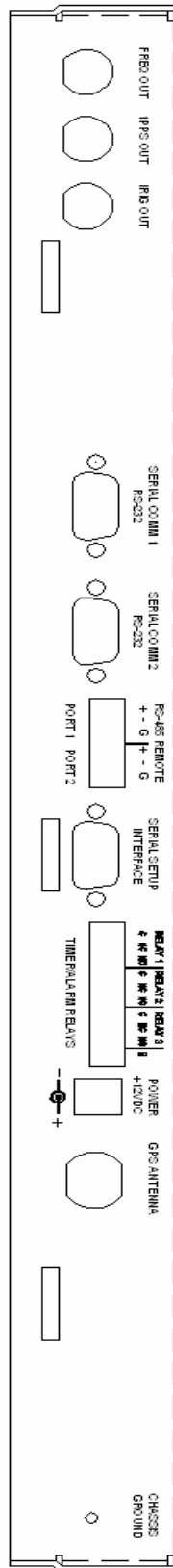


Figure 4-2: Rear panel illustration

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 be 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 Ethernet Time Server can be alerted of impending leap seconds by either of the following methods:

1. **Serial Time Code Input** – Once the NetClock Master Clock has ascertained a Leap Second correction is to occur (Via GPS or an optional modem dial-out available on certain NetClock Master Clocks), it will inform the Ethernet Time Server via the RS-485 input data stream that a Leap Second adjustment at the end of this calendar month will occur.

Notice: The Model 9188 can accept RS-485 Data Formats 0, 2 and 8 from the NetClock Master Clock. Data Format 2 has a Leap Second indicator in the data stream so the NetClock can warn the Ethernet Time Server of a pending leap second. Data Formats 0 and 8 do not have this indicator present in the data stream so they will NOT be able to warn the Ethernet Time Server of a pending leap second.

When using Data Format 2 as the selected input, the Ethernet Time Server will know ahead of time that the leap second will be occurring. When using Data Formats 0 or 8, the Time Server will adjust for a Leap Second at the correct time because of the discontinuity of time. But, it will not be able to set the indicator bits in the NTP or rear panel outputs ahead of time. So PC's and other peripheral devices will not know ahead of time that a leap second is pending.

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 Ethernet Time Server 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 calendar month a Leap Second Adjustment will be made by having a 'L' rather than a ' ' (space) character near the end of the data stream.

Note that this 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 browser user interface page of “Status and Logs” will display a Leap Second Status box indicating +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.

Dynamic System Information

Uptime: 0 years, 0 days, 0 hours, 2 minutes, 1 seconds
Current internal temperature: 26.25 C (79.25 F)
Major Alarm is (OFF)
Minor Alarm is (OFF)
Time Sync status: In Sync
Time Source: Serial Time Code Input
Leap Second Status: +1 seconds at end of month

Figure 4-3: Leap Second indication

4.3.3 Sequence of a Leap Second correction being applied

1. The following is the time output sequence that the Ethernet Time Server 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). The sequence used is based upon which RS-485 Data Format is being received from the NetClock as shown below:

A) Data Format 0 or 8 selected in the “Set Serial Time Code” page:

1. Sequence of the seconds output during a positive leap second:
56, 57, 58, 59, 00, 01, 02, 03, 04,...
2. Sequence of the seconds output during a negative leap second:

56, 57, 58, 59, 00, 02, 02, 03, 04,...

B) Data Format 2 selected in the “Set Serial Time Code” page:

1. Sequence of the seconds output during a positive leap second:
56, 57, 58, 59, 00, 01, 02, 02, 03, 04,...
2. Sequence of the seconds output during a negative leap second:
56, 57, 58, 59, 60, 02, 02, 03, 04,...

2. An entry will be made in the Operational log that the time was adjusted for a Leap Second.

Example log entry:

TIME= 23:59:59 DATE= 2005-12-31
System Clock Service
Leap second inserted 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	<ul style="list-style-type: none"> • 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		
<i>New install and Sync LED is not lit</i>	Not receiving correctly formatted RS-485 data from the NetClock or the NetClock is not time synchronized.	<ul style="list-style-type: none"> • Verify the cabling between NetClock Remote RS-485 output port and Port 2 on the Ethernet Time Server (+ to +, - to - and G to G). • Verify NetClock Remote output configuration and Ethernet Time Server Set Serial Time Code page configuration is identical (1200-9600 baud, Data Formats 0, 2 or 8). • Verify the NetClock front panel Time Sync lamp is green.
<i>Flashing Green</i>	Recently stopped Receiving RS-485 data from the NetClock or the NetClock has lost Time Sync (The unit has not timed-out of hold-over mode).	<p>(Time is still valid. Other devices will still be synchronized).</p> <ul style="list-style-type: none"> • Review the Alarm and Operation logs. • Verify NetClock Master Clock still has a green Time Sync lamp on the front panel. • Check the cabling between NetClock Remote RS-485 output port and Port 2 on the rear of the Time Server.
<i>Yellow</i>	Lost synchronization to the NetClock Master (No longer in hold-over mode).	<p>(Time is no longer valid). Other devices will not be synchronized). Review the Alarm and Qualification logs.</p>
<i>Red stays On</i>	Unit fault. Time may not be valid. Overrides all other indicators.	Contact Customer Service
<i>Blinking Red</i>	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 lamps

5.2 Front Panel LAN Connector

Symptom	Cause	Corrective Action
LAN Green LED is off (This LED also known as Good Link indicator).	Unit is not connected to the network	<ul style="list-style-type: none"> 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 Ethernet Time Server but the Gold Link indicator on the HUB/Switch is not lit.	The Ethernet Time Server and the HUB/Switch are not communicating at the correct port speed.	<ul style="list-style-type: none"> If the Hub/switch is set to auto, power cycle the Ethernet Time Server with the network cable connected. This will cause Auto-Negotiate to determine the settings of the HUB/Switch (Auto-Negotiate only occurs at power-on). Try setting the HUB/Switch to 100mbps and 10mpps
Can “Ping” the unit but can’t open web browser user interface	<ul style="list-style-type: none"> Gateway not configured correctly Web Browser proxy settings not correct 	<ul style="list-style-type: none"> 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 open web browser user interface to configure the unit but can’t synchronize any PC’s with the Time Server	PC software not installed or configured correctly.	<ul style="list-style-type: none"> Install YATS32 shareware program from www.dillobits.com. This program will allow you to view the raw NTP data to verify that the Ethernet Time Server is outputting time data. Refer to the Spectracom website Support page for additional information on YATS32. Refer to Spectracom website Support page for additional information on syncing PC’s. Verify the Sync lamp is solid green.
Unable to communicate with the unit on the network	Improper IP addressing	<ul style="list-style-type: none"> Make sure your IP address and subnet mask are set correctly. Make sure the unit is within the same Class and/or subnet range as the computers with which you are trying to communicate Check that the hub/switch/router device port is active and set to the correct port speed. Be sure to use a straight-through cable when connecting to a hub, a cross-over cable when connecting directly to a PC. Consult your Network System Administrator.

Table 5-2: Status of Front Panel LAN connection

5.3 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, 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.

5.4 Verify operation of a Spectracom TimeTap

If you want to verify the operation of a Spectracom TimeTap, follow the same process as Section 5.3 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.

5.5 Customer Service

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

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 ^ DDMMYY ^ 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 a possible 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.

- 1) Connect to the Serial Setup Interface port with a PC running HyperTerminal OR telnet into the Ethernet Time Server using the IP address of the Time Server.
 - A. 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)
 - B. 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).
 - C. 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).
 - D. 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 and the local clock not being created.

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)	Oscillator Error (milliseconds)
Space	Lock	<1
A	<10	<10
B	<100	<100
C	<500	<500
D	>500	>500

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 =	degrees, 00...90
mm.mmmm =	minutes, 00.0000....59.9999
n =	direction, N = North, S = South
dddmm.mmmm,e =	Longitude
ddd =	degrees, 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 are used to configure individual attributes for that subsystem.

Command	Description	Section
help	Help	7.1
login	Log in at a specified security level	7.2
logout	Log out of the current security level	7.3
ltc	Configures up to five separate local clocks	7.4
net	Network configuration commands	7.5
net gateway	Enables/disables or set the default gateway	7.6
net help	Displays summaries of the network subcommands	7.7
net IP	Sets the IP address	7.8
Net mac	Displays the MAC address	7.9
net mask	Sets the subnet mask	7.10
net show	Shows network parameter	7.11
net http	Enable/disables http access to the unit	7.12
opt	Enables options	7.13
reboot	Reboots the unit	7.14
rem	Configures the Remote RS-485 output (port 1)	7.15
sec	Security Commands	7.16
sec help	Displays summaries of the security subcommands	7.17
sec level	Displays the current security level	7.18
sec password	Sets the password for the current security level	7.19
ser	Configures the Serial port	7.20
update	Firmware Update Commands	7.21
App	Updates the Application software	7.22
boot	Updates the Boot Monitor	7.23
csl	Updates the CSL	7.24
kern	Updates the kernel	7.25
help	Displays summaries of the update subcommands	7.26

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 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

7.2 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

7.3 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

7.4 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

7.5 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:

7.6 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.

* * This feature is only available for the Model 9188 with Option 1 Security enabled.

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.

7.7 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

7.8 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.

7.9 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 Ethernet Time Server is configured at the factory and cannot be changed.

7.10 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

Where: New netmask Has been set
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.

7.11 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

7.12 net http^{*}

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

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

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

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

To disable HTTP issue the following command:

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

To enable HTTP issue the following command:

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

^{*} This feature is only available for the Model 9188 with Option 1 Security enabled.

7.13 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:    9188      (0x0002) EEPROM (0x0002)
Product Name: 9188
Options:    (0x180107ff)    EEPROM (0x180107ff)
Options State: INVALID
```

```
Security:      ON
Serial Port 1:  ON
Remote Port 1:  ON
Remote Port 2:  ON
Relays:         ON
Serial Time Code Input: OFF
SNTP Server:    ON
Oscillator Type: TCXO
```

7.14 reboot [bootloader]

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

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

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

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

<p>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.</p>

7.15 rem

The rem command allows the rear panel Remote RS-485 port (port1) 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 1 <enter>

Display the current remote serial port settings.

rem baud 1 <baud> <enter>

Sets the baud rate of a remote serial port

baud = baud rate; 1200, 2400, 4800, 9600

rem fmt 1 <fmt> <enter>

Sets the output format of a remote serial port

fmt = format type; 01, 02, etc.

rem ltc 1 <ltc> <enter>

Sets the output format of a remote serial port

ltc = clock setting; 0 - UTC, 1-5 local clock

rem all 1 <baud> <format> <clock> <enter>

Configure all settings of the remote port

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

7.16 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:

7.17 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

7.18 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

7.19 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

7.20 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

7.21 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:

7.22 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.

7.23 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.

7.24 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.

7.25 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.

7.26 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 an available option for the Model 9188. The following section provides descriptions and details on configuration of this available option.

Option 1 can be purchased and enabled with the unit still in the field as shown in the following table.

Available Model & Option Combinations

Feature/Option	Option number	Capable of being purchased after the initial equipment purchase	Refer to manual Section
Security	Opt 1	Yes	Section 8.1

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

8.1 Option 1: Security

8.1.1 Option 1 basics

Option 1 provides the Ethernet Time Server with the ability to make a secure network connection with the network. When this option is enabled, secure algorithms may then be used to protect the passwords and traffic that are sent over the network when communicating with the unit.

If not initially purchased with the unit, Option 1 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 into the Ethernet Time Server to enable the security algorithms.

8.1.2 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 browser user interface pages and secure file transfers.

A convenient and simple web browser user interface is provided on secure Spectracom products 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 secure products 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.

8.2 Configuring SSH

8.2.1 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 by the secure Spectracom products are SSH – secure shell, SCP – secure copy, and SFTP – secure file transfer protocol. The secure Spectracom products implement the server components of SSH, SCP and SFTP.

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

8.2.2 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.

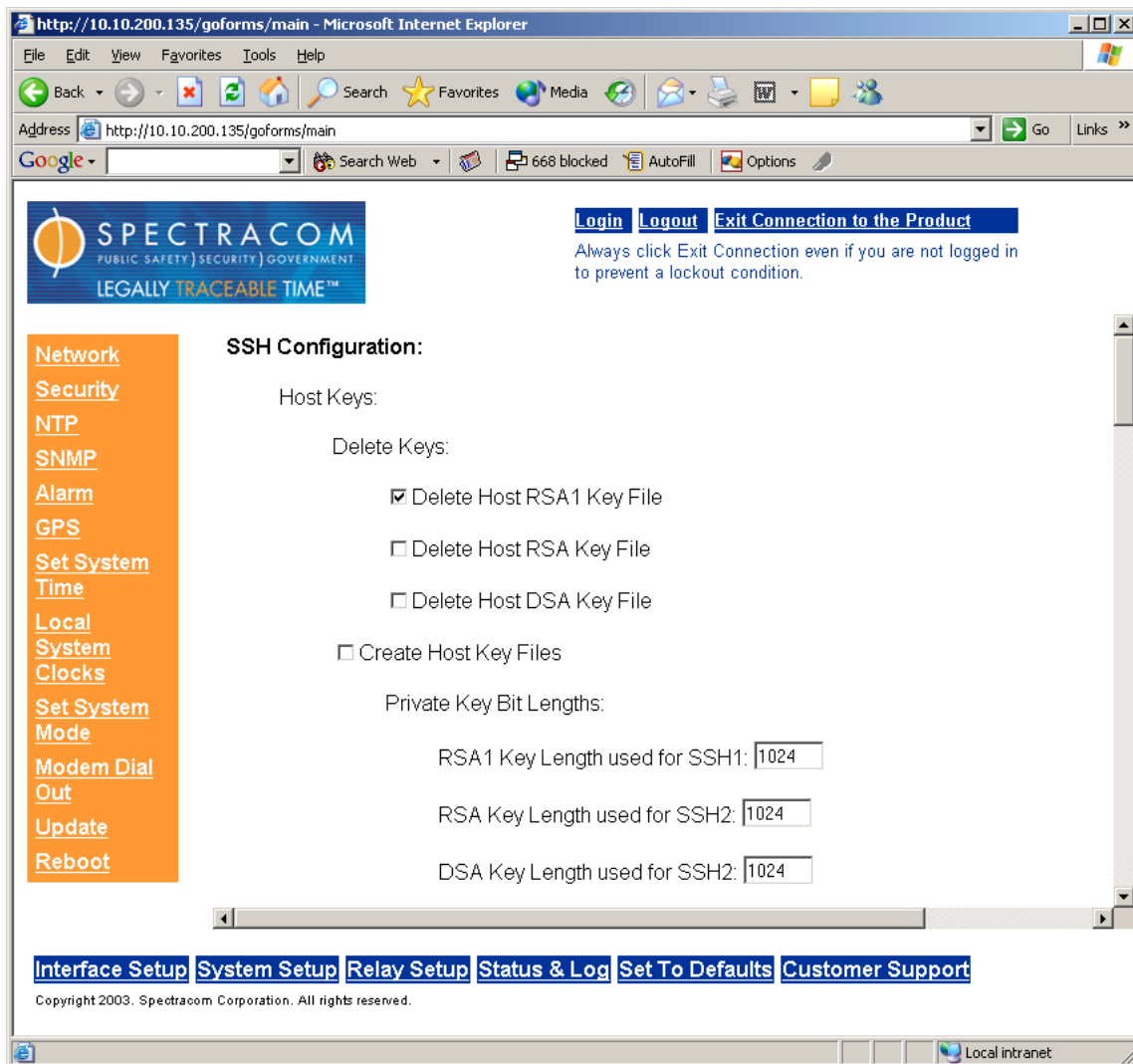


Figure 8-1: SSH configuration Screen

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.

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.

The screenshot shows a web browser window with the address <http://10.10.200.135/goforms/main>. The page features the Spectracom logo and a navigation menu on the left with links like Network, Security, NTP, SNMP, Alarm, GPS, Set System Time, Local System Clocks, Set System Mode, Modem Dial Out, Update, and Reboot. The main content area is titled 'SSH Configuration:' and includes a 'Host Keys:' section. Under 'Host Keys:', there is a 'Delete Keys:' section with three checkboxes: 'Delete Host RSA1 Key File', 'Delete Host RSA Key File', and 'Delete Host DSA Key File'. Below these is a checked checkbox for 'Create Host Key Files'. The 'Private Key Bit Lengths:' section contains three input fields: 'RSA1 Key Length used for SSH1:' with the value '1024', 'RSA Key Length used for SSH2:' with the value '768', and 'DSA Key Length used for SSH2:' with the value '768'. At the bottom of the page, there are links for 'Interface Setup', 'System Setup', 'Relay Setup', 'Status & Log', 'Set To Defaults', and 'Customer Support'. The footer text reads 'Copyright 2003. Spectracom Corporation. All rights reserved.'

Figure 8-2: Creating SSH host key files

Ethernet Time Servers with Option 1 enabled at the factory typically have their initial Host Keys already created. 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.

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.

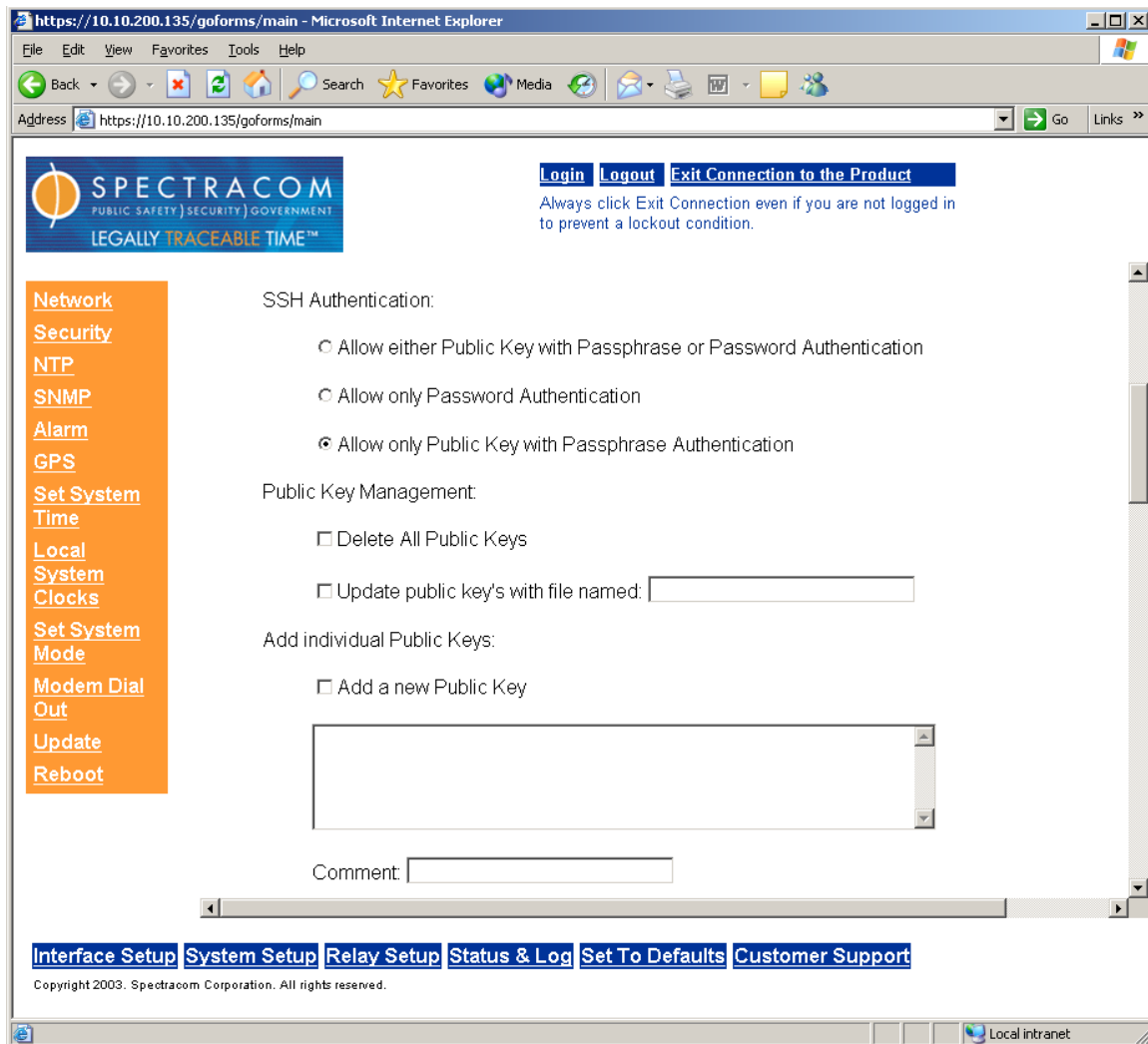


Figure 8-3: Selecting SSH authentication modes

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.

8.3.2.1 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.

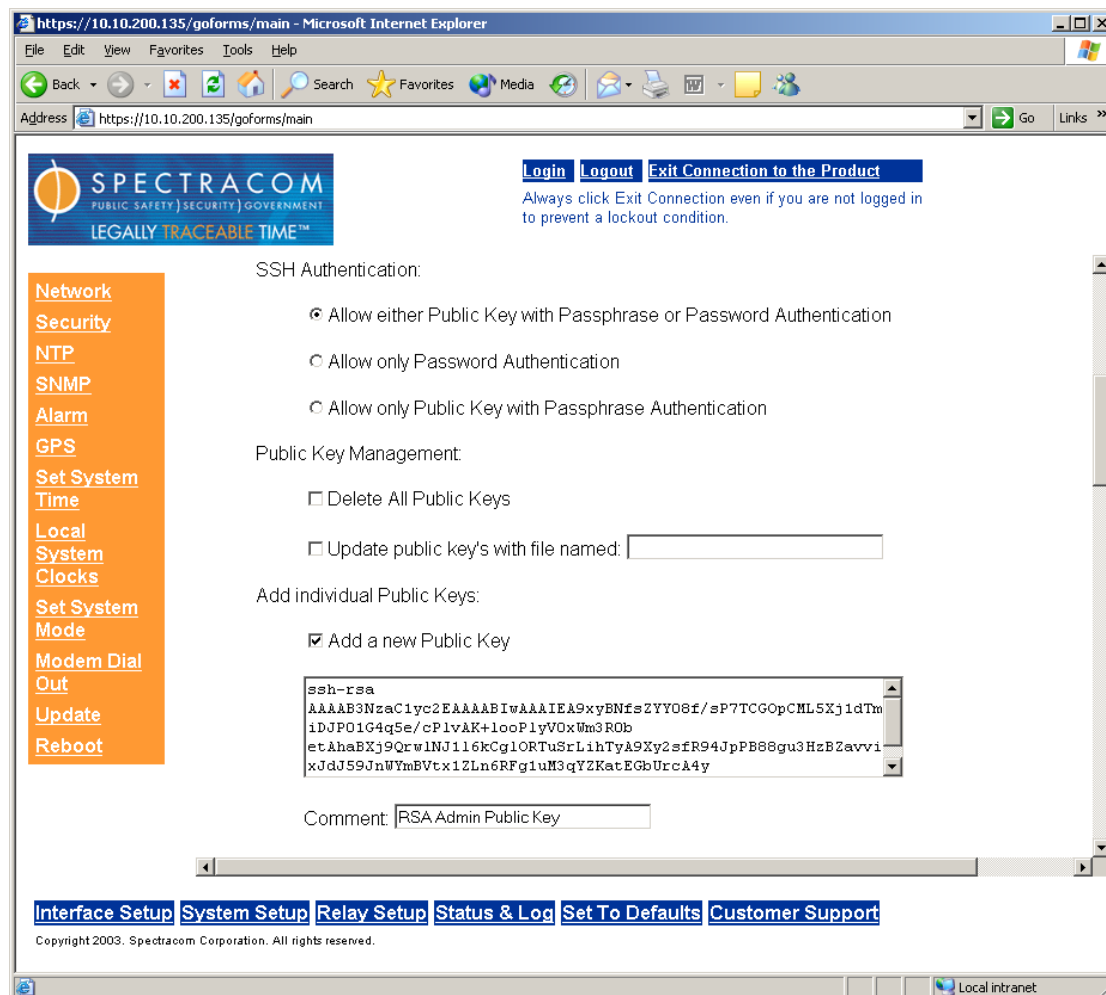


Figure 8-4: Adding SSH public key to authorized keys

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 the Ethernet Time Server. 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.

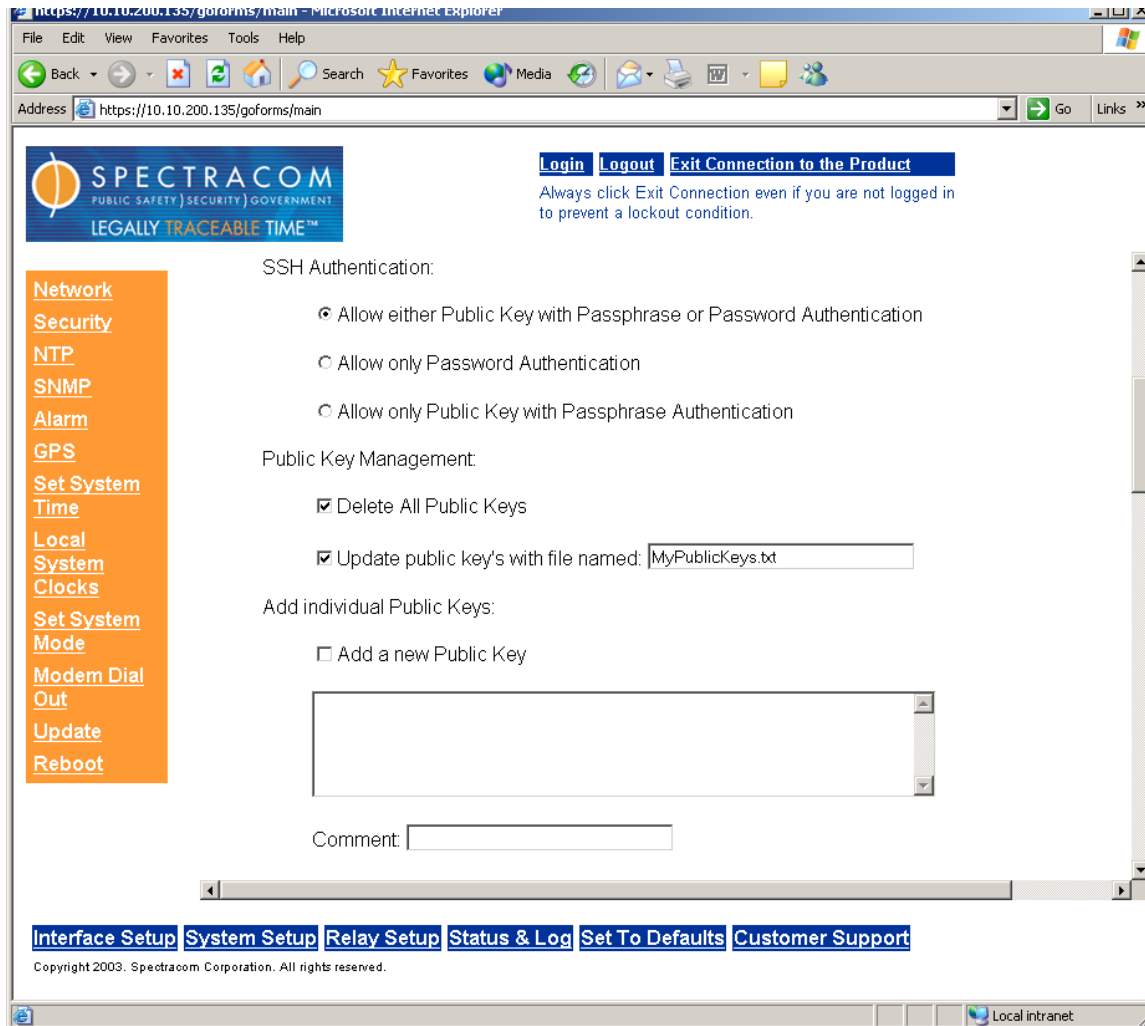


Figure 8-5: Adding a new SSH public key file

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.

8.3.2.1 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.

1. 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.

2. 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.

3. 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.

8.3.2.1 Secure File Transfer

The secure Spectracom products 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
|*****| 5 00:00 100%
```

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.

8.3.2.1 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/](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.

8.3 Configuring HTTPS

8.3.1 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 secure Spectracom products use 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.

8.3.2 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.

SPECTRACOM
PUBLIC SAFETY | SECURITY | GOVERNMENT
LEGALLY TRACEABLE TIME™

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

HTTPS Configuration:

The Web Server Certificate installed must use the same Private Key used to generate the Certificate Request. Both the Certificate and Private Key must be installed. Exit after the new Certificate and Private Key files are installed to ensure proper reloading by the web server.

Certificate Request Parameters:

☒ Delete Certificate, Certificate Request and Private Key Files

☐ Restore User's Self Signed Certificate and Private Key Files

☐ Create Certificate Request and Self Signed Certificate

Signature Algorithm:

Private Key Pass Phrase:

RSA Private Key Bit Length:

Country Name:

State Or Province Name:

Locality Name:

Organization Name:

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 8-6: Deleting SSL Certificate, Certificate Request and Private Key Files

8.3.3 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.

SPECTRACOM
PUBLIC SAFETY | SECURITY | GOVERNMENT
LEGALLY TRACEABLE TIME™

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

HTTPS Configuration:

The Web Server Certificate installed must use the same Private Key used to generate the Certificate Request. Both the Certificate and Private Key must be installed. Exit after the new Certificate and Private Key files are installed to ensure proper reloading by the web server.

Certificate Request Parameters:

☐ Delete Certificate, Certificate Request and Private Key Files

☒ Restore User's Self Signed Certificate and Private Key Files

☐ Create Certificate Request and Self Signed Certificate

Signature Algorithm:

Private Key Pass Phrase:

RSA Private Key Bit Length:

Country Name:

State Or Province Name:

Locality Name:

Organization Name:

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright 2003. Spectracom Corporation. All rights reserved.

Figure 8-7: Restoring user’s Self Signed Certificate and Private Key Files

8.3.4 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.

HTTPS Configuration:

The Web Server Certificate installed must use the same Private Key used to generate the Certificate Request. Both the Certificate and Private Key must be installed. Exit after the new Certificate and Private Key files are installed to ensure proper reloading by the web server.

Certificate Request Parameters:

☐ Delete Certificate, Certificate Request and Private Key Files

☐ Restore User's Self Signed Certificate and Private Key Files

☒ Create Certificate Request and Self Signed Certificate

Signature Algorithm:

Private Key Pass Phrase:

RSA Private Key Bit Length:

Country Name:

State Or Province Name:

Locality Name:

Organization Name:

Organizational Unit Name:

Common Name (e.g. IP Address):

Email Address:

Challenge Password:

Optional Company Name:

Self Signed Certificate Expiration (Days):

Figure 8-8: 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.

8.3.5 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.

The screenshot shows a web browser window with the address bar displaying `https://10.10.200.135/gofrms/main`. The page title is "SPECTRACOM" with the tagline "LEGALLY TRACEABLE TIME". The left sidebar contains a menu with options: Network, Security, NTP, SNMP, Alarm, GPS, Set System, Time, Local System, Clocks, Set System Mode, Modem Dial Out, Update, and Reboot. The main content area has a "Login Logout Exit Connection to the Product" header. Below this, there are checkboxes for "Delete Certificate, Certificate Request and Private Key Files", "Restore User's Self Signed Certificate and Private Key Files", and "Create Certificate Request and Self Signed Certificate" (which is checked). The form includes fields for "Signature Algorithm" (MD5), "Private Key Pass Phrase" (MySecretPassphrase), "RSA Private Key Bit Length" (1024), "Country Name" (US), "State Or Province Name" (New York), "Locality Name" (Rochester), "Organization Name" (Spectracom Corporation), "Organizational Unit Name" (Engineering), "Common Name (e.g. IP Address)" (www.spectracomcorp.com), "Email Address" (techsupport@spectracomcorp.com), "Challenge Password" (WhatTimeIsIT), "Optional Company Name" (Spectracom), and "Self Signed Certificate Expiration (Days)" (365). At the bottom, there is a "Certificate Request" section with a text box containing the following text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBKjCB6AIBADA/NQwvCQYpVQOGewJV0zEPMAOGA1UECBGTwV2YURhNCOw
Cwtp
VQOGewVQOGewVQOGewVQOGewVQOGewVQOGewVQOGewVQOGewVQOGewVQOGew
A4GN
-----
```

Figure 8-9: 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 Ethernet Time Server's web browser user interface 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.

8.3.6 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.

The screenshot shows a web browser window with the address bar displaying "https://10.10.200.135/gofoms/main". The page title is "SPECTRACOM PUBLIC SAFETY SECURITY GOVERNMENT LEGALLY TRACEABLE TIME™". The page has a navigation menu on the left with links: Network, Security, NTP, SNMP, Alarm, GPS, Set System Time, Local System Clocks, Set System Mode, Modem Dial Out, Update, and Reboot. The main content area is titled "Certificate Request" and contains the following sections:

- Update Certificate and Private Key Files via Web Interface:**
 - ☒ Update Certificate: A text box containing a sample certificate in PEM format.
 - ☐ Update Private Key: A text box for entering a private key.
- Update Certificate and Private Key Files by external File Transfer:**
 - ☐ Update Certificate with file named: [text box]
 - ☐ Update Private Key with file named: [text box]

At the bottom of the form are "Submit" and "Reset" buttons. The footer of the page includes links: Interface Setup, System Setup, Relay Setup, Status & Log, Set To Defaults, and Customer Support. Copyright 2003, Spectracom Corporation. All rights reserved.

Figure 8-10: 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 browser user interface 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.

8.3.7 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.

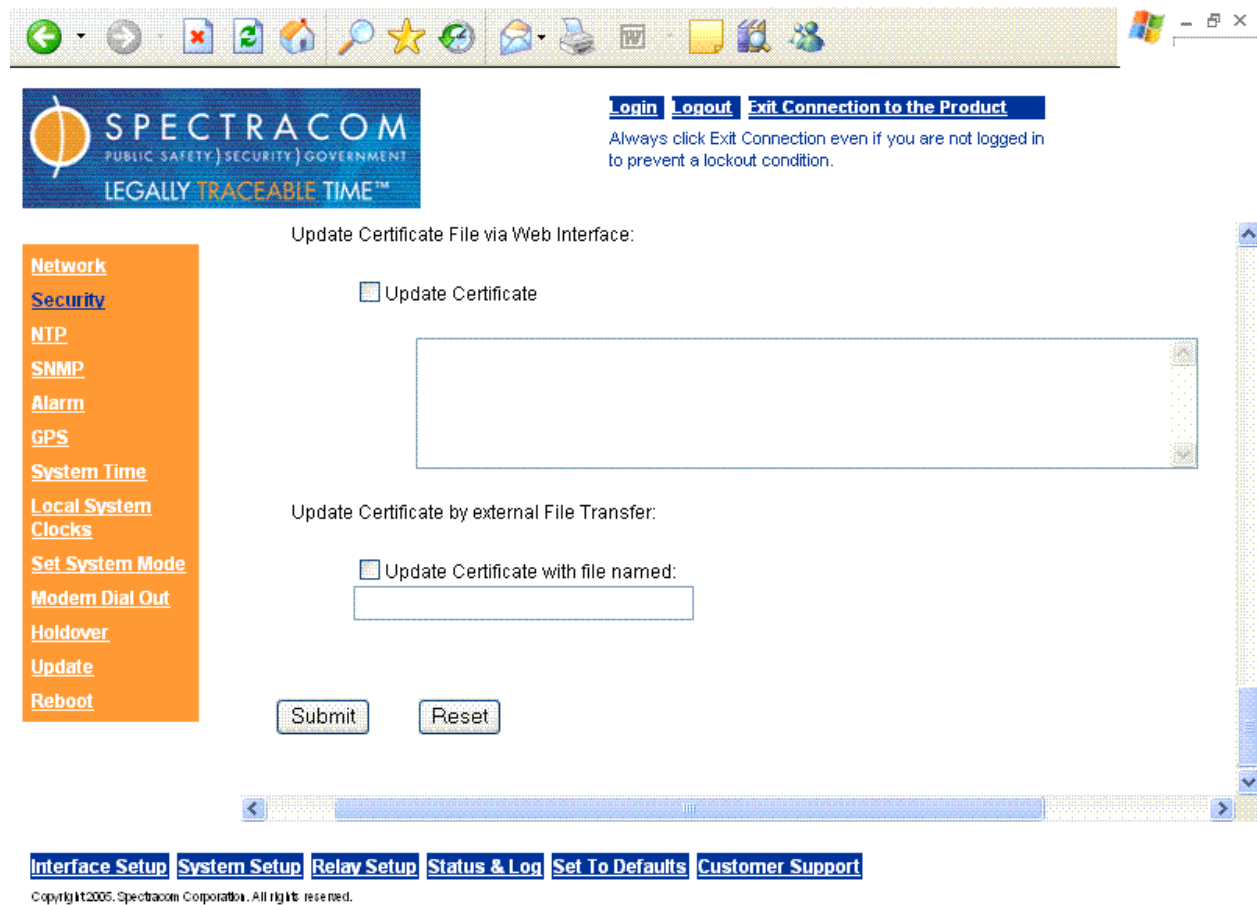


Figure 8-11: Using External Certificate

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 provide the file names. The user then enters the submit button.

In both cases the secure Spectracom product’s web browser user interface loads this new self-signed certificate after the user selects a few more web browser user interface 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.

8.3.8 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.

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

- [50] Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp> - TRAK clock driver
- [51] Paul A Vixie <vixie@vix.com> - TrueTime GPS driver, generic TrueTime clock driver
- [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@atsoft.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:Pete.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@fielvel.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/http-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 adhered 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 routines 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 9188
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 9188-5003-0050

Manual Addendum

22 December 2005

Copyright © 2005 Spectracom Corporation. The contents of this publication may not be reproduced in any form without the written permission of Spectracom Corporation. Printed in USA.

Specifications subject to change or improvement without notice.

Spectracom, NetClock, Ageless, TimeGuard, TimeBurst, TimeTap, LineTap, MultiTap, VersaTap, and Legally Traceable Time are Spectracom registered trademarks. All other products are identified by trademarks of their respective companies or organizations. All rights reserved.

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.

Table of Contents

1	CHANGES FOR V2.3.0 TO V2.3.1	1-1
2	NETWORK AND WEB USER INTERFACE CHANGES	2-1
2.1	Command Line Changes	2-2
2.1.1	net telnet	2-2
2.1.2	net ftp	2-2
2.1.3	net https	2-2
2.1.4	net sshd (Includes SSH, SCP, and SFTP)	2-2
2.2	Web Server Timeout	2-2
2.2.1	web exit	2-3
2.2.2	web timeout	2-3
2.3	HTTPS Certificate 20-Year Life	2-4
2.4	NTP	2-5
2.4.1	NTP Command Line	2-6
2.5	System Time	2-6
2.6	Further Assistance	2-7

List of Figures

Figure 2-1: Enabling and Disabling Network Interfaces	2-1
Figure 2-2: HTTPS Certificate Creation Web UI Page	2-4
Figure 2-3: Reference Identifier Field	2-5
Figure 2-4: Setting System Time Options	2-7

1 Changes for v2.3.0 to v2.3.1

This addendum to the operations and maintenance manual for the Spectracom NetClock® Model 9188 (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.

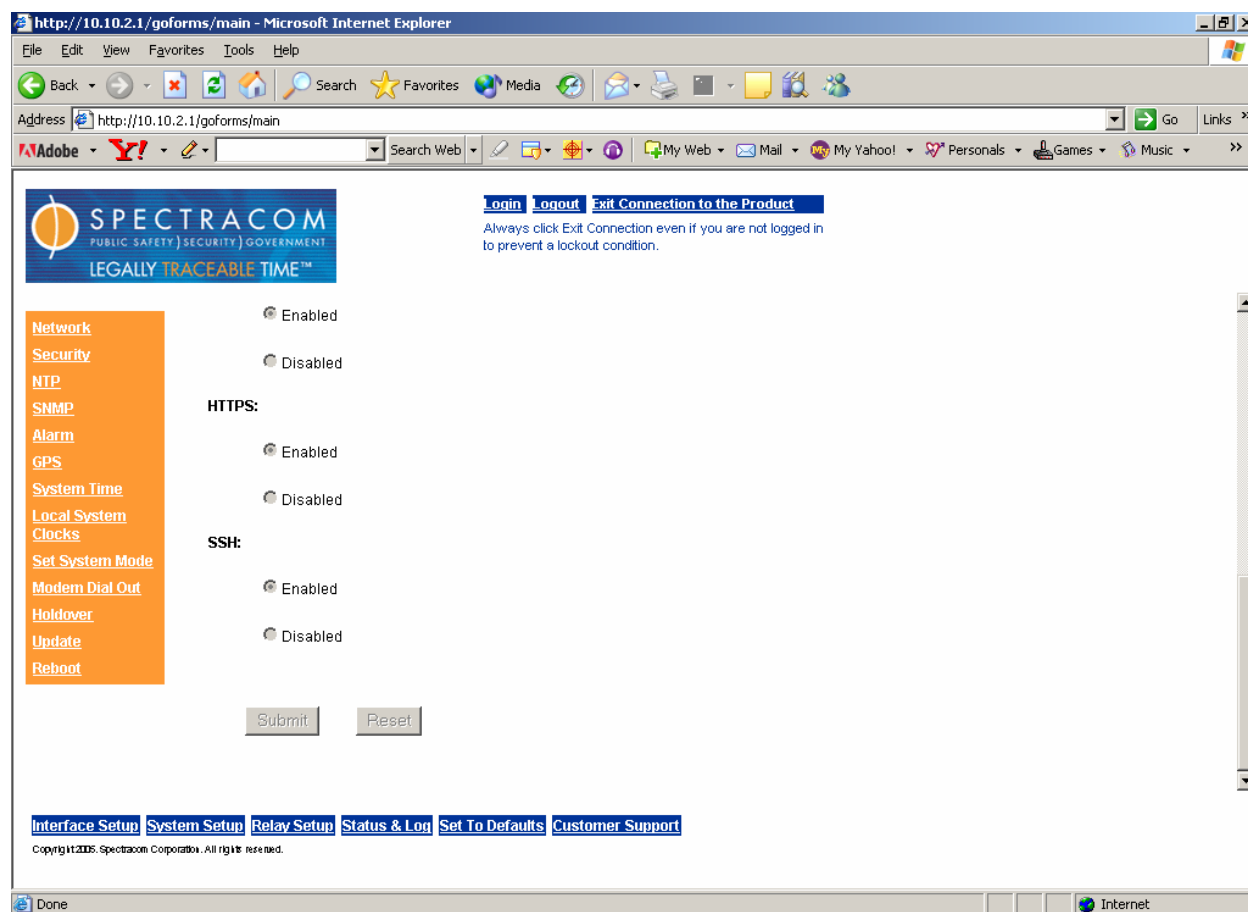


Figure 2-1: Enabling and Disabling Network Interfaces

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):

http://10.10.2.1/goforms/main - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Mail My Web Mail My Yahoo! Personals Games Music

Address http://10.10.2.1/goforms/main Go Links

Adobe Y! Search Web

SPECTRACOM
PUBLIC SAFETY | SECURITY | GOVERNMENT
LEGALLY TRACEABLE TIME™

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

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

* State Or Province Name:

* Locality Name:

* Organization Name:

* Organizational Unit Name:

* Common Name (e.g. IP Address):

* Email Address:

Challenge Password:

Optional Company Name:

* Self Signed Certificate Expiration (Days):

Certificate Request:

[Interface Setup](#) [System Setup](#) [Relay Setup](#) [Status & Log](#) [Set To Defaults](#) [Customer Support](#)

Copyright © 2005, Spectracom Corporation. All rights reserved.

Done Internet

Figure 2-2: HTTPS Certificate Creation Web UI Page

2.4 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.

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 unit, such as NYC, CHI, BOS, etc. Refer to Figure 2-3.

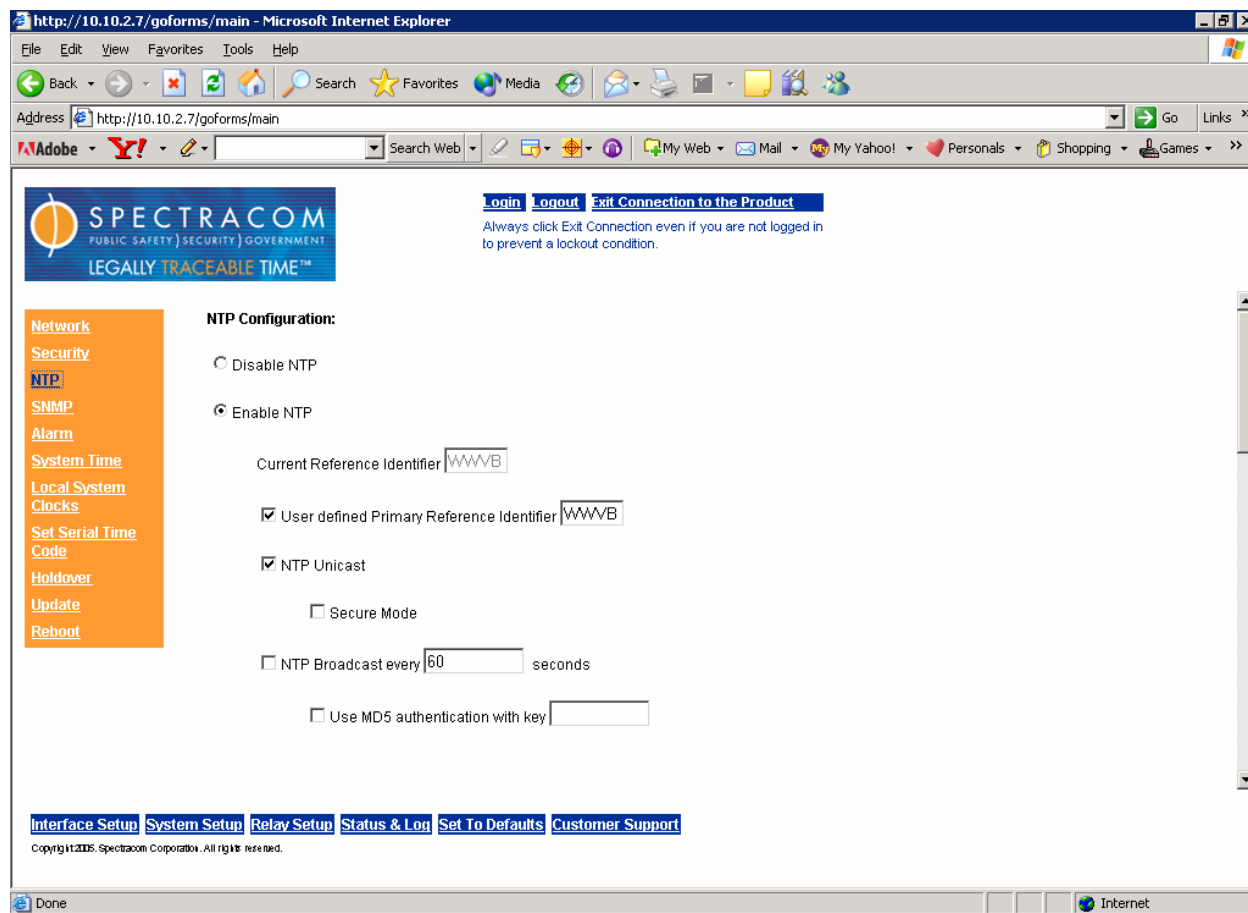


Figure 2-3: Reference Identifier Field

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

2.4.1 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

2.4.1.1 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.

2.4.1.2 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.

2.5 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 2-4.

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.

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying `http://10.10.2.3/goforms/main`. The page features the Spectracom logo and navigation links: [Login](#), [Logout](#), and [Exit Connection to the Product](#). A warning message states: "Always click Exit Connection even if you are not logged in to prevent a lockout condition." On the left, an orange sidebar contains a menu with links: [Network](#), [Security](#), [NTP](#), [SNMP](#), [Alarm](#), [GPS](#), [System Time](#), [Local System Clocks](#), [Set System Mode](#), [Modem Dial Out](#), [Holdover](#), [Update](#), and [Reboot](#). The main content area is titled "System Time" and contains two checkboxes: ☒ "Allow user to set time using SNMP or Web UI" and ☐ "Set System Time using user specified UTC Time below". Below these are input fields for Year (2005), Month (Dec), Day (6), Hour (13), Minute (5), and Second (13). At the bottom of the form are "Submit" and "Reset" buttons. A footer bar contains links: [Interface Setup](#), [System Setup](#), [Relay Setup](#), [Status & Log](#), [Set To Defaults](#), and [Customer Support](#). The copyright notice at the bottom reads: "Copyright 2005, Spectracom Corporation. All rights reserved."

Figure 2-4: Setting System Time Options

2.6 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