

**NETCLOCK ETHERNET
TIME SERVER MODEL 9288
INSTRUCTION MANUAL**

*95 Methodist Hill Drive
Rochester, NY 14623*

*Phone: US +1.585.321.5800
Fax: US +1.585.321.5219*



www.spectracomcorp.com

Part Number 1150-5000-0050

Manual Rev. F

21 April 2008

Copyright © 2007 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 any 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.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Table of Contents

1	GENERAL INFORMATION	1-1
1.1	Introduction.....	1-1
1.2	Warranty Information and Customer Support.....	1-2
1.3	Inspection.....	1-3
1.3.1	Inventory.....	1-3
1.4	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.....	1-5
1.4.5	RS-485 Input/Output	1-5
1.4.6	Front Panel LED Indicators	1-5
1.4.7	Relay Outputs.....	1-5
1.4.8	1PPS Input	1-6
1.4.9	Input Power	1-6
1.4.10	Mechanical and Environmental	1-6
2	INSTALLATION	2-1
2.1	Summary.....	2-1
2.2	Required Tools and Cables.....	2-3
2.3	Power and Ground Connection	2-3
2.4	Rack Mounting	2-5
2.5	Ethernet Network Cabling	2-5
2.5.1	Optional CNC3000 Cable Kit.....	2-5
2.6	Remote Port and Serial Comm Port Output Pin-outs and Wiring.....	2-6
2.6.1	Serial Comm Ports	2-6
2.6.2	RS-485 Remote Port.....	2-7
2.6.3	Remote Output Usage.....	2-8
2.6.4	RS-485 Guidelines and Cable Selection	2-9
2.6.5	Connection Method	2-9
2.6.6	Termination	2-13
3	PRODUCT CONFIGURATION	3-1
3.1	Network Configuration with DHCP	3-2
3.2	Initial Network Configuration	3-5
3.2.1	Using HyperTerminal to Connect to the Netclock.....	3-5
3.2.2	Initial Network Setup	3-10
3.2.3	Default and Recommended Configurations.....	3-13
3.3	Issuing the HALT Command before Removing Power	3-14
3.3.1	Issuing the HALT Command through the Web UI	3-14
3.3.2	Issuing the HALT Command through the CLI.....	3-16
3.3.3	Issuing the HALT Command through SNMP	3-17
3.4	Product Configuration using the WEB UI	3-20
3.4.1	Configuring NTP	3-20
3.4.2	NTP Support.....	3-28
3.4.3	Configuring the Interface	3-29
3.4.4	Sysplex Timing	3-33
3.4.5	Configuring the System: SNMP.....	3-34
3.4.6	Configuring Alarms.....	3-37

3.4.7	Configuring System Time and Local Clocks.....	3-38
3.4.8	Activating System Options and Rolling Back Updates	3-43
3.4.9	Rebooting the System	3-45
3.4.10	Configuring System Holdover.....	3-46
3.4.11	Serial Time Code Setup	3-48
3.4.12	Configuring System Logs	3-49
3.4.13	Configuring and Testing Relays	3-50
3.4.14	Configuring Network Security.....	3-58
3.4.15	If You Cannot Access a Secure NetClock	3-70
3.4.16	Configuring User Accounts.....	3-71
3.4.17	Configuring SNMP v1, v2, and v3	3-74
3.4.18	Configuring LDAP and RADIUS	3-78
3.4.19	Configuring IPsec	3-82
3.4.20	Logs and Status Reporting.....	3-93
4	OPERATION	4-1
4.1	Front Panel.....	4-1
4.1.1	Status Indicator	4-1
4.2	Rear Panel	4-3
4.2.1	Event and Alarm Relay Outputs.....	4-4
4.3	Leap Second occurrence	4-5
4.3.1	Reasons for a Leap Second Correction	4-5
4.3.2	Leap Second Alert Notification	4-5
4.3.3	Sequence of a Leap Second Correction Being Applied	4-6
5	SERIAL DATA FORMATS	5-1
5.1	Format 0.....	5-1
5.2	Format 1	5-2
5.3	Format 2.....	5-3
5.4	Format 3.....	5-5
5.5	Format 4.....	5-6
5.6	Format 7.....	5-7
5.7	Format 8.....	5-8
6	SERIAL SETUP INTERFACE COMMANDS.....	6-1
6.1	time	6-1
6.2	reboot	6-1
6.3	log	6-2
6.4	option	6-2
6.5	lrc.....	6-2
6.6	net	6-3
6.7	sys.....	6-3
6.8	ser	6-3
6.9	rem	6-4
6.10	frq.....	6-4
7	OPTIONS.....	7-1
8	LICENSE NOTICES	8-1

List of Figures

Figure 2-1: Serial Port Pin Configuration	2-6
Figure 2-2: Remote Outputs.....	2-7
Figure 2-3: RS-485 Output.....	2-7
Figure 2-4: One-Way Bus Installation	2-10
Figure 2-5: Split Bus Configuration	2-10
Figure 2-6: Wire Strain Relief.....	2-11
Figure 2-7: TimeView RS-485 Interface.....	2-11
Figure 2-8: Model 8179T TimeTap RS-485 Interface.....	2-12
Figure 2-9: Model 9288 RS-485 Interface.....	2-12
Figure 2-10: TimeBurst RS-485 Interface	2-13
Figure 3-1: Entering to the Configuration in the Web UI	3-1
Figure 3-2: Web Browser User Interface (Web UI)	3-2
Figure 3-3: Security – Network Screen (1 of 2).....	3-3
Figure 3-4: Security – Network Screen (2 of 2).....	3-4
Figure 3-5: Establishing a New Terminal Connection	3-5
Figure 3-6: Connecting to the Computer’s Serial Port.....	3-6
Figure 3-7: Configuring the Serial Port Connection Properties	3-6
Figure 3-8: Spectracom NetClock Command Line Interface (CLI).....	3-7
Figure 3-9: Available CLI Commands	3-8
Figure 3-10: Serial Port Pin Configuration	3-9
Figure 3-11: Net Commands.....	3-10
Figure 3-12: Prompt for Initial Configuration Values in the CLI	3-10
Figure 3-13: Initial Configuration using the CLI.....	3-11
Figure 3-14: Successful Completion of Network Configuration.....	3-12
Figure 3-15: System Reboot/Halt Screen (1 of 3).....	3-14
Figure 3-16: System Reboot/Halt Screen (2 of 3).....	3-15
Figure 3-17: System Reboot/Halt Screen (3 of 3).....	3-15
Figure 3-18: Command Line Interface (CLI)	3-16
Figure 3-19: Halting the System from the CLI.....	3-16
Figure 3-20: Rebooting the System from the CLI.....	3-17
Figure 3-21: Reboot MIB Location Options (SNMP)	3-17
Figure 3-22: Rebooting the Unit through SNMP.....	3-18
Figure 3-23: Halting the Unit through SNMP.....	3-19
Figure 3-24: Successful Halt.....	3-19
Figure 3-25: Web UI Primary Menu	3-20
Figure 3-26: Web UI NTP Menu.....	3-20
Figure 3-27: NTP General Screen	3-21
Figure 3-28: NTP References Screen (1 of 2).....	3-23
Figure 3-29: NTP References Screen (2 of 2).....	3-24
Figure 3-30: NTP Symmetrical Keys Screen.....	3-25
Figure 3-31: NTP Autokey Screen	3-26
Figure 3-32: Statistics FTP Screen	3-27
Figure 3-33: NTP Status Screen.....	3-28
Figure 3-34: Interface Menu.....	3-29
Figure 3-35: Interface Serial Port 1 Screen.....	3-30
Figure 3-36: Interface Remote Port 1 Screen	3-31
Figure 3-37: Interface Set to Defaults Screen.....	3-32
Figure 3-38: Configuring Serial Port 1 for Sysplex Timing.....	3-33

Figure 3-39: System Menu.....	3-34
Figure 3-40: System SNMP Screen.....	3-35
Figure 3-41: Spectracom's MIB.....	3-36
Figure 3-42: System Alarm Screen.....	3-37
Figure 3-43: System Time Screen.....	3-38
Figure 3-44: Local System Clocks Screen (1 of 2).....	3-39
Figure 3-45: Local System Clock Screen (2 of 2).....	3-40
Figure 3-46: System Update Screen.....	3-44
Figure 3-47: System Reboot Screen.....	3-45
Figure 3-48: System Holdover Screen.....	3-46
Figure 3-49: Serial Time Code Setup Screen.....	3-48
Figure 3-50: System Log Configuration Screen.....	3-49
Figure 3-51: Relay Menu.....	3-50
Figure 3-52: Relay Output Screen.....	3-51
Figure 3-53: Event Timer Relay Screen.....	3-52
Figure 3-54: Edit/View Event Timers.....	3-53
Figure 3-55: Relay Current Event Scheduler Screen.....	3-55
Figure 3-56: Relay Reset ALL Event Timers Screen.....	3-56
Figure 3-57: Test Relays Screen.....	3-57
Figure 3-58: Security Menu.....	3-58
Figure 3-59: Security Network Screen (1 of 2).....	3-59
Figure 3-60: Security Network Screen (2 of 2).....	3-60
Figure 3-61: Security SSH Screen (1 of 2).....	3-61
Figure 3-62: Security SSH Screen (2 of 2).....	3-62
Figure 3-63: Security HTTPS Screen (1 of 2).....	3-67
Figure 3-64: Security HTTPS Screen (2 of 2).....	3-68
Figure 3-65: Security User Account Screen.....	3-71
Figure 3-66: Security User Account Screen (Assigning Privileges).....	3-73
Figure 3-67: SNMP Security Screen (1 of 3).....	3-74
Figure 3-68: SNMP Security Screen (2 of 3).....	3-75
Figure 3-69: SNMP Security Screen (3 of 3).....	3-76
Figure 3-70: Security LDAP General Screen.....	3-77
Figure 3-71: Security LDAP Client Configuration Screen (1 of 2).....	3-78
Figure 3-72: Security LDAP Client Configuration Screen (2 of 2).....	3-79
Figure 3-73: Security RADIUS General Screen.....	3-80
Figure 3-74: Security RADIUS Client Configuration Screen.....	3-81
Figure 3-75: IPSEC IKE SA Configuration Screen (1 of 2).....	3-83
Figure 3-76: IPSEC IKE SA Configuration Screen (2 of 2).....	3-84
Figure 3-77: IPsec General Screen.....	3-87
Figure 3-78: IPsec Manual SA Configuration (1 of 2).....	3-89
Figure 3-79: IPsec Manual SA Configuration (2 of 2).....	3-90
Figure 3-80: IPsec General Screen.....	3-91
Figure 3-81: Status and Log Menu.....	3-93
Figure 3-82: Alarm Log Screen.....	3-94
Figure 3-83: Authorization Log Screen.....	3-95
Figure 3-84: Event Log Screen.....	3-96
Figure 3-85: Journal Log Screen.....	3-97
Figure 3-86: NTP Log Screen.....	3-98
Figure 3-87: IKE Log Screen.....	3-99
Figure 3-88: Operational Log Screen.....	3-100
Figure 3-89: System Log Screen.....	3-101

Figure 3-90: Update Log Screen.....	3-102
Figure 3-91: System Status Screen (1 of 2).....	3-103
Figure 3-92: System Status Screen (2 of 2).....	3-104
Figure 4-1: Front Panel.....	4-1
Figure 4-2: NetClock Rear Panel Detail.....	4-3
Figure 4-3: Event and Alarm Relay Contacts.....	4-4

Underwriters Laboratory (UL) has not tested the performance or reliability of the Global Positioning System (GPS) hardware, operating software, or other aspects of this product. UL has only tested for fire, shock, or casualties as outlined in UL's Standard(s) for Safety for Information Technology Equipment, UL60950-1. UL Certification does not cover the performance or reliability of the GPS hardware and GPS operating software.

UL MAKES NO REPRESENTATIONS, WARRANTIES, OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY GPS RELATED FUNCTIONS OF THIS PRODUCT.

1 General Information

Spectracom Corporation is a leading manufacturer of precise time-keeping devices used to synchronize critical operations. Our products provide accurate, reliable, Legally Traceable Time™ across your networks. The Spectracom 9200 series NetClock™ is a direct response to customer needs for affordable time synchronization equipment that includes a variety of necessary and widely used security, authentication, and networking features.

1.1 Introduction

The Model 9288 NetClock Ethernet Time Server time server provides synchronized timing using Network Time Protocol (NTP). The NetClock meets or exceeds the National Emergency Numbers Association (NENA) master clock standard and is ideally suited for delivering world-wide, split-second timing to mission critical systems.

The 9288 uses the Linux v2.6 operating system and features a high-speed processor. A variety of time code outputs are included to meet the requirements of numerous systems, including a 10/100 Base-T LAN port, an RS-232 serial port, and an RS-485 data bus port. Alarm outputs and programmable timer outputs are also provided. The NetClock allows users to accurately time stamp video surveillance systems, access points, card readers, time clocks, and alarm systems to provide necessary evidence and validation of events.

The 9200 series' new standard security features, which can be enabled and disabled by the user, include Secure Shell (SSH), Secure Copy Protocol (SCP), and Secure File Transfer Protocol (SFTP). Enhanced security features include Secure Sockets Layer (SSL) and SNMP v1, v2, and v3 with host access restriction. The NetClock supports IPv4, IPv6, and centralized user authentication (LDAP/Active Directory, RADIUS). NTP capabilities include peering, Stratum 2, and Autokey.

The NetClock can be configured and its reports accessed through a Web User Interface (Web UI). A Command Line Interface (CLI) is also provided for initial product configuration through the serial setup port. Once configured, the NetClock can be accessed, under appropriate security policies, anywhere within a network. The product features browser-based remote diagnostics 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 performed through SNMP and Telnet.

The NetClock also includes ancillary hardware.

1.2 Warranty Information and Customer Support

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

Spectracom constantly strives to improve its products. We greatly appreciate any and all customer feedback.

Technical support is available by telephone at **585.321.5800**. Please direct any comments or questions regarding application, operation, or service to Spectracom's Customer Service Department. Customer Service is available Monday through Friday from 8:00 a.m. to 5:00 p.m. EST, excluding holidays.

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

sales@spectracomcorp.com

For repairs and technical support, questions may be e-mailed to Spectracom Technicians at:

techsupport@spectracomcorp.com

Visit Spectracom's web page for product information, application notes, and upgrade notices as they become available:

<http://www.spectracomcorp.com/>

Please contact Customer Service before returning any equipment Spectracom. Customer Service must provide you with a Return Material Authorization Number (RMA#) prior to shipment. When contacting Customer Service, please be prepared to provide your equipment serial number(s) and a description of the failure symptoms or issues you would like resolved. Freight to Spectracom is to be prepaid by the customer.

Once you have obtained the RMA number, ship your equipment to the following address:

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

1.3 Inspection

On receipt, carefully examine the carton and its contents.

CAUTION:

Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

Verify that all material ordered has been received by checking the carton contents against the packing list. If there is a discrepancy, please contact Spectracom Customer Service at US 585.321.5800. If there is damage to the carton resulting in damage to the unit, contact the carrier immediately. Retain the carton and packing materials in the event the carrier wishes to witness the shipping damage. Failing to report shipping damaging immediately may forfeit any claim against the carrier. In addition, notify Spectracom Corporation of shipping damage or shortages in order to obtain a replacement or repair services.

NOTE: If equipment is returned to Spectracom, it must be shipped in its original packing material. Save all packaging material for this purpose.

1.3.1 Inventory

Your Spectracom time server package ships with the following components:

- 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
- Rubber footpads for desktop installation
- 3-pin terminal block connector for RS-485 connections
- 10-pin terminal block connector
- Jeweler's type screwdriver (for tightening the screws on the terminal blocks)
- Terminating Resistors, 120Ω

1.4 Specifications

NOTE: The specifications listed herein are based on “standard” operation with the unit synchronized through the RS-485 input.

1.4.1 RS-232 Serial Setup Interface Port

Function:	Accepts commands to locally configure the IP network parameters for initial connectivity. Also used as the interface to the dial-out modem (Option 03).
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 BaseT auto sensing LAN connection for NTP / SNTP and remote monitoring, diagnostics, configuration and upgrade.
-----------	--

1.4.3 Protocols Supported

NTP:	NTP v4.2.0. Provides MD5 and Autokey. Stratum 1 or higher. (RFC 1305, 4330)
Loading:	~4,000 requests per second, typical.
Clients supported:	The number of users supported depends on the class of network and the subnet mask for the network. A gateway greatly increases the number of users.
HTTP, HTTPS Servers:	For browser-based configuration and monitoring using Internet Explorer 5 or Netscape 6 per RFC 1945 and 2068.
FTP:	For remote upload of system logs and RFC 959.
Logging:	Syslog
SNMP:	Supports v1, v2c, and v3
Telnet:	For limited remote configuration per RFC 854.
Security Features:	Up to 32-character password, Telnet Disable, FTP Disable, Secure SNMP, SNMP Disable, HTTPS, HTTP Disable, SCP, SSH, SFTP.
Authentication:	LDAP v2 and v3, RADIUS, MD5 Passwords, NTP Autokey Protocol.
Connector:	RJ-45, Network IEEE 802.3.

1.4.4 RS-232 Communication Port

Signal:	Selected time Data Format in RS-232 levels when interrogated by the connected device. This port may also be configured to provide a continuous once-per-second output.
Connector:	DB9 female, pin assignments conform to EIA/TIA-574 standard, data communication equipment (DCE). No flow control.
Character structure:	ASCII, 1 start, 8 data, 1 stop, and no parity.
Accuracy:	Data stream on time marker within ± 100 microseconds of UTC on Sync in Data Formats 0, 1, 3 and 8. Data Formats 2, 4 and 7 within ± 1 millisecond of UTC.
Configuration:	Baud rate and output Data Formats are selected using the web browser user interface. Bit rate selections are 1200, 2400, 4800 and 9600 baud. There are eight Data Format selections available.

1.4.5 RS-485 Input/Output

Signal:	Selected time Data Format in RS-485 levels, output once-per-second.
Connector:	Removable 3-position terminal block (supplied).
Character structure:	ASCII, 1 start, 8 data, 1 stop, and no parity.
Accuracy:	Data stream on time marker within ± 100 microseconds of UTC on Sync in Data Formats 0, 1, 3 and 8. Data Formats 2, 4 and 7 within ± 1 millisecond of UTC.
Configuration:	Baud rate and output Data Formats are selected using the web browser user interface. Bit rate selections are 1200, 2400, 4800, and 9600 baud. There are eight Data Format selections available.

1.4.6 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: Network 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 1PPS Input

Signal: One pulse-per-second square wave.
Signal Level: TTL compatible (High trigger is 2.1 V, low is 0.9 V), High Z (> 10k ohms), Active rising edge.
Connector: BNC female

1.4.9 Input Power

Power source: 90 to 240 VAC, 47 to 63 Hz through an IEC 320 universal connector.
DC input: 9.5 to 30 VDC, 18 watts, through a CE/UL/CSA-approved power adapter (supplied).
Connector: Barrel, 5.5mm O.D., 2.5 mm I. D.
Polarity: Negative shell, positive center.

1.4.10 Mechanical and Environmental

Dimensions: EIA 19" rack mount W x 1.75" H [1U] x 11.00" D (483 mm W x 44 mm H x 305 mm D).
Weight: 6 lbs. (27 kg).
Temperature: 32° to 122°F (0° to 50°C) operating range.
 -40° to 185°F (-40° to 85°C) storage range
Humidity: 10% - 95% relative humidity, non-condensing

2 Installation

2.1 Summary

This section provides an overview summary of the installation process. The installation of the NetClock consists of the following steps. Refer to the table of contents in this manual for specific section references detailing how these summarized steps are accomplished.

WARNING:

This equipment has a connection between the earthed conductor of the DC supply circuit and the earthing conductor.

This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.

The DC supply source is to be located within the same premises as this equipment.

Switching or disconnected devices shall not be in the earthed circuit conductor between the DC source and the point of the connection of the earthing electrode conductor.

CAUTION:

Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

CAUTION:

Once power is applied to the unit, DO NOT disconnect power unless the HALT command is first issued to the NetClock. Refer to Product Configuration for information on issuing the HALT command.

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

- 2) Connect the NetClock's front panel Ethernet port to an available hub/switch on the network with a standard network cable.
- 3) Connect the DC power input jack to a standard AC outlet with the supplied power supply. Verify the green Good Link lamp next to the Ethernet connector illuminates.
- 4) From the network administrator, obtain an available static network IP address, the network subnet mask and the IP address of the immediate gateway (if installed) if the subnet must access the NetClock. This step is only necessary if you are not using DHCP.
- 5) Assign the IP address, net mask and gateway settings by using the rear panel Serial Setup Interface DB9F connector interfaced to a PC with the provided serial cable (PC should be running either Microsoft HyperTerminal or ProComm). (Refer to *Options* for more information.) This step is only necessary if you are not using DHCP.
- 6) Verify the NetClock front panel Sync lamp illuminates green. This will not happen until the NetClock is connected to a synchronized time source through the RS-485 input port. Once connected, the NetClock should synchronize within approximately 20 minutes.

NOTE: The Data Format and baud rate of the reference and of the NetClock must be set identically. Refer to Section 3.4.11, Serial Time Code Setup, for more information.

- 7) Interface the NetClock to wall display clocks and other peripheral devices as needed.
- 8) Configure each of the rear panel outputs to these devices for desired local times, baud rates and Data Formats using either the Web User Interface or the serial setup port (Each port is separately configured so each port used may need to be configured for your desired configuration).

NOTE: Unless you are using DNS in conjunction with DHCP (with the client configured using the NTP server's hostname instead of IP address), DHCP must be disabled and the IP address must be changed to a static address once the NetClock is properly configured. Failure to do this will result in a loss of time synchronization if the DHCP server assigns a new IP address to the NetClock. Verify your setup before synchronizing the network PCs via NTP.

- 9) Synchronize the network PCs via NTP using the Ethernet port as desired. (Refer to www.spectracomcorp.com for assistance and refer to Table 2-1 for information regarding local time.)
- 10) Review your security configuration settings.

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

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

2.2 Required Tools and Cables

- 1) Phillips screwdriver to install the unit's rack-mount ears.
- 2) Screwdriver to mount the unit in a standard 19-inch rack.
- 3) Wire strippers for the RS-485 cabling.
- 4) Supplied jeweler's type screwdriver for tightening the RS-485 wiring terminal block connectors (Located in the ancillary kit).
- 5) RS-232 straight-thru DB9 to DB9 cable (supplied)
- 6) Ethernet cables (Refer to Section 2.5).

2.3 Power and Ground Connection

WARNING:

This equipment has a connection between the earthed conductor of the DC supply circuit and the earthing conductor.

This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.

The DC supply source is to be located within the same premises as this equipment.

Switching or disconnected devices shall not be in the earthed circuit conductor between the DC source and the point of the connection of the earthing electrode conductor.

CAUTION:

Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

An external AC to DC power adapter powers the NetClock.

This International and US Desk Top adapter has a detachable AC power cord to an IEC 320 connector. The power adapter is shipped with a line cord compatible with AC receptacles (NEMA 5-15R) commonly found in the United States and Canada. Alternate type line cords or adapters may be obtained locally.

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

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

2.4 Rack Mounting

To rack-mount the unit, locate the rack-mount ears. Using the rack mounting screws provided in the ancillary kit (refer to 1.3.1, *Inventory*), mount the ears to the sides of the unit. (If the Netclock is to be mounted flush with the front of the rack, mount the ears to the front of the unit.) Slide the unit into the rack and connect the ears to the rack using appropriate screws (not provided).

2.5 Ethernet Network Cabling

Spectracom NetClocks provide a 10/100 Ethernet port for full NTP functionality as well as full web browser user interface enabled configuration, monitoring and diagnostic support.

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

Use standard CAT 5 cable with RJ45 connectors.

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

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

2.5.1 Optional CNC3000 Cable Kit

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

- 1) Six foot RS-232 Setup port cable DB9M to DB8F for initial configuration
- 1) Six foot Cat 5 crossover LAN cable for direct PC connection
- 1) Six foot Cat 5 patch LAN cable for LAN hub link.

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

2.6 Remote Port and Serial Comm Port Output Pin-outs and Wiring

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

2.6.1 Serial Comm Ports

The rear panel of the Model 9288 has one RS-232 SERIAL COMM port that is available to synchronize peripheral devices. This port can provide RS-232 output data to synchronize external devices that can accept RS-232 Data Formats as an input.

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

The configuration of the data, including the baud rate, the Data Format, the request character in the Interrogation mode, Time Zone Offsets and Daylight Saving Time rules is chosen from the web browser user interface.

The Serial Ports have a standard RS-232 pin configuration as shown in Figure 2-1 and Table 2-2.

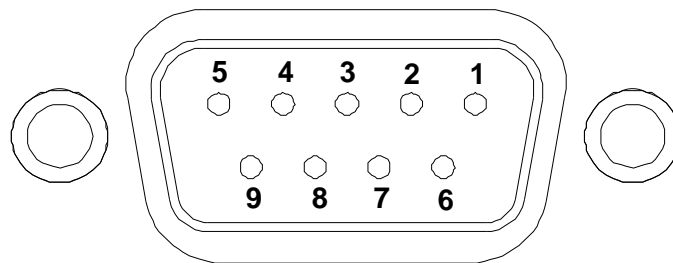


Figure 2-1: Serial Port Pin Configuration

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

Table 2-2: Serial Port Pin Assignments

2.6.2 RS-485 Remote Port

The NetClock has RS-485 output and input ports. The RS-485 output provides a continuous once-per-second time data stream in the selected Data Format. Two input time Data Formats, five output time Data Format selections, and one position data stream in NMEA 0183 format are available. Refer to Section 6 for a complete description of the Data Format structures.

In addition to Data Formats, baud rate and UTC time difference of each output are selectable.

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

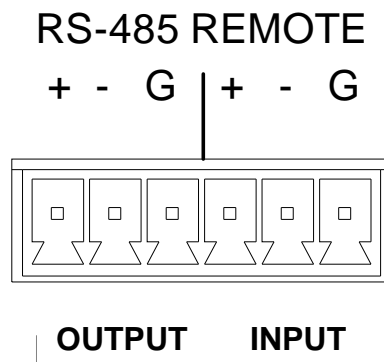


Figure 2-2: Remote Outputs

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 the RS-485 Output diagram for a schematic representation of each RS-485 output driver. Relative to RS-485 specifications, the A terminal (Pin 2) is negative with respect to the B terminal (Pin 1) for a mark or binary 1. The A terminal is positive to the B terminal for a space or binary 0.

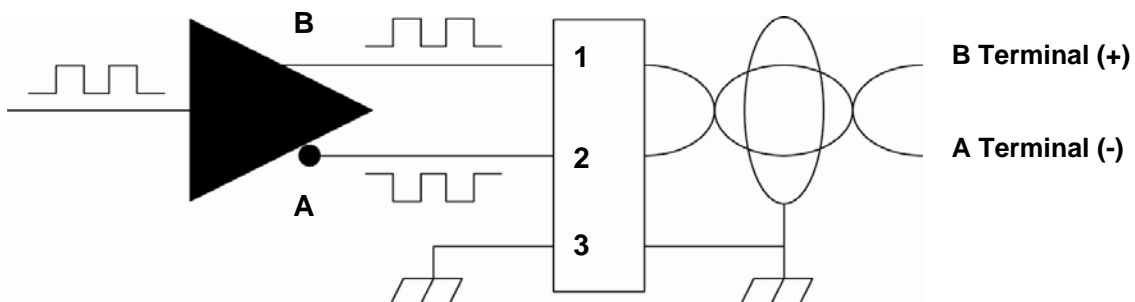


Figure 2-3: RS-485 Output

Spectracom offers many devices that accept the RS-485 data stream as an input reference. These products include display clocks, RS-485 to RS-232 converters, Ethernet Time Servers,

and radio link products to meet various time applications and requirements. For information on Remote Output usage refer to Section 2.6.2.

2.6.3 Remote Output Usage

The Remote Outputs provide a continuous once-per-second time data stream in RS-485 levels. RS-485 is a balanced differential transmission, which offers exceptional noise immunity, long cable runs and multiple loading. These characteristics make RS-485 ideal for distributing time data throughout a facility.

Each Remote Output can drive 32 devices over cable lengths up to 4000 feet. Spectracom manufactures wall clocks, Ethernet Time Servers, RS-485 to RS-232 converters and radio link products that utilize the RS-485 data stream as an input.

Refer to sections 2.6.4, 2.6.5, and 2.6.6 for more information on time data bus interconnections. Follow the guidelines contained therein when constructing the RS-485 data bus.

2.6.4 RS-485 Guidelines and Cable Selection

Low capacitance, shielded twisted pair cable is recommended for installations where the RS-485 cable length is expected to exceed 1500 feet. Table 2-3 suggests some manufacturers and part numbers for extended distance cables. These cables are specifically designed for RS-422 or RS-485 applications; they have a braided copper shield, nominal impedance of 120 ohms, and a capacitance of 12 to 16 picofarads per foot.

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

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

Table 2-3: Cable Sources for RS-485 Lines Over 1500 Feet

For cable runs less than 1500 feet, a lower-cost twisted pair cable may be used. Refer to Table 2-4 for possible sources. In addition, Category 5 cables may be used for cable runs less than 1500 feet.

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

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

2.6.5 Connection Method

The RS-485 transmission line must be connected in a daisy chain configuration as shown in Figure 2-4. In a daisy chain configuration, the transmission line connects from one RS-485 receiver to the next. The transmission line appears as one continuous line to the RS-485 driver.

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

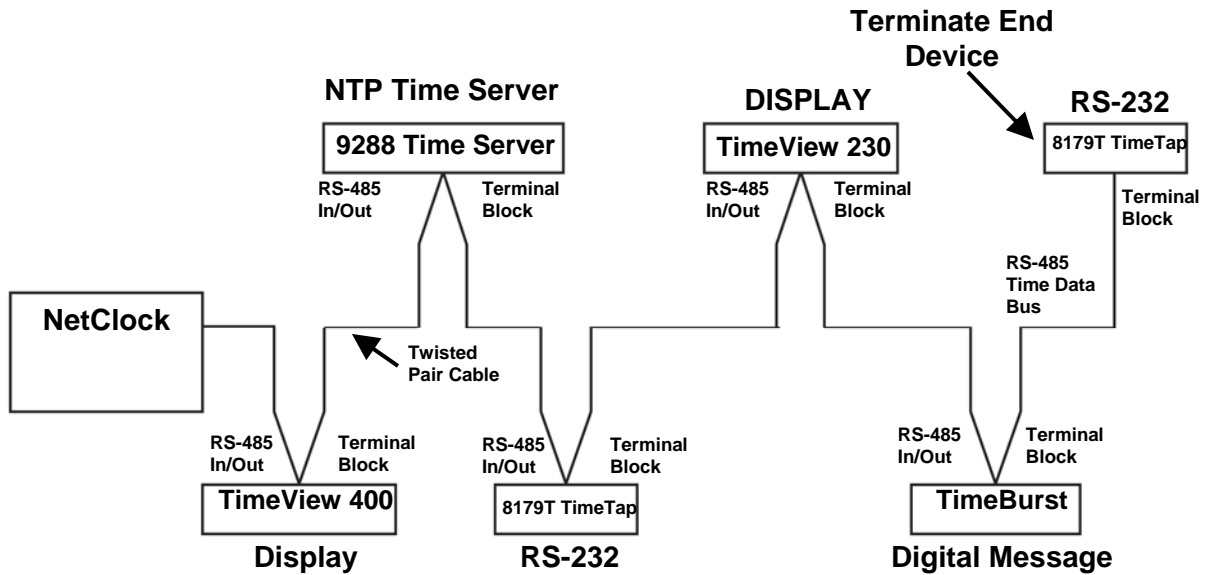


Figure 2-4: One-Way Bus Installation

The RS-485 Output can be split in a total of two directions as shown in Figure 2-5. This allows the NetClock to be centrally located. Connecting in this method can simplify installation and possibly reduce the amount of cable required.

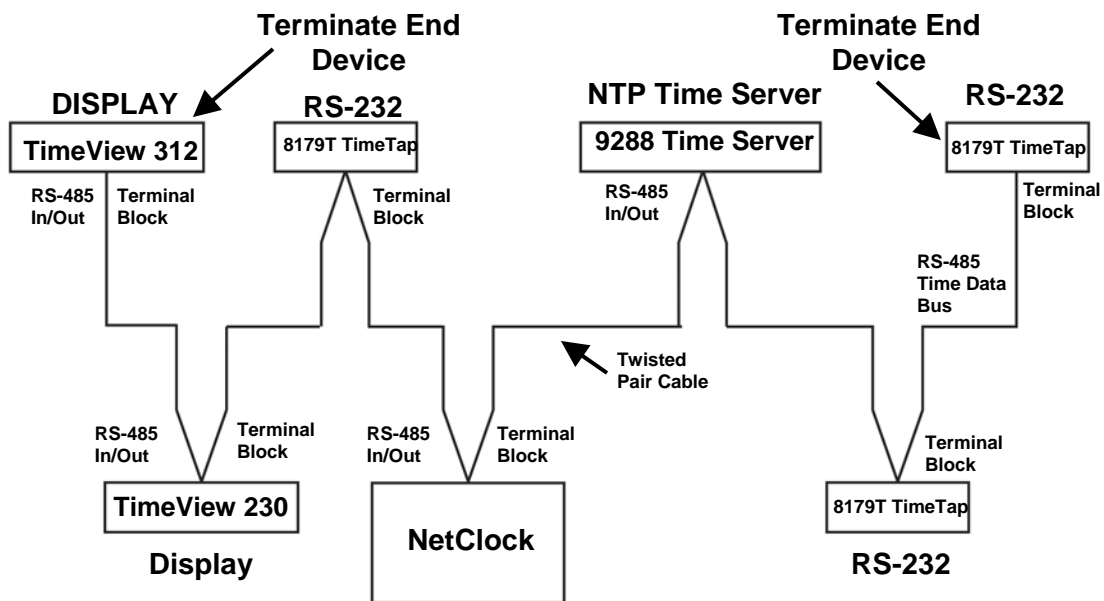


Figure 2-5: Split Bus Configuration

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

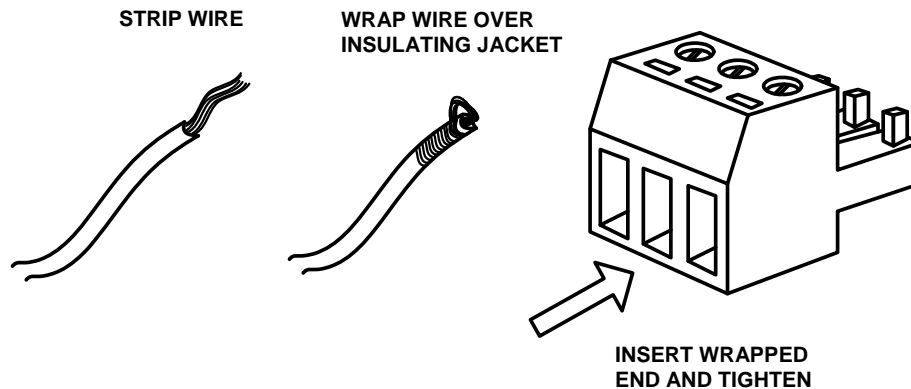


Figure 2-6: Wire Strain Relief

TimeView display clocks use a 6-position terminal block to connect to the RS-485 data bus. Connect the TimeView to the NetClock RS-485 Output as shown in Figure 2-7. The TimeView display clocks accept only Data Formats 0 or 1.

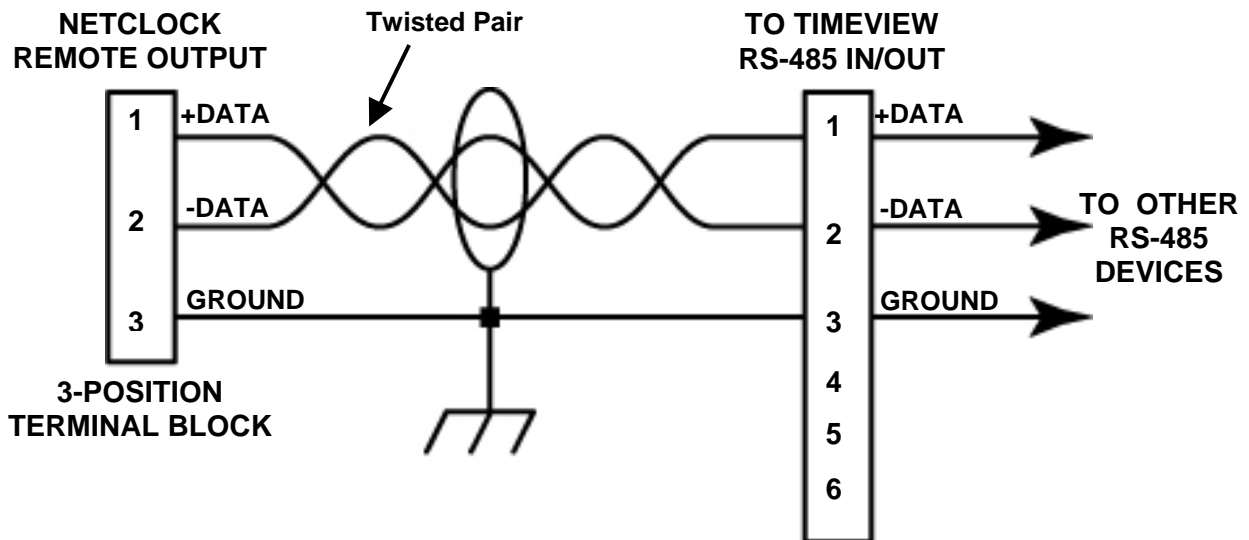


Figure 2-7: TimeView RS-485 Interface

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 2-8.

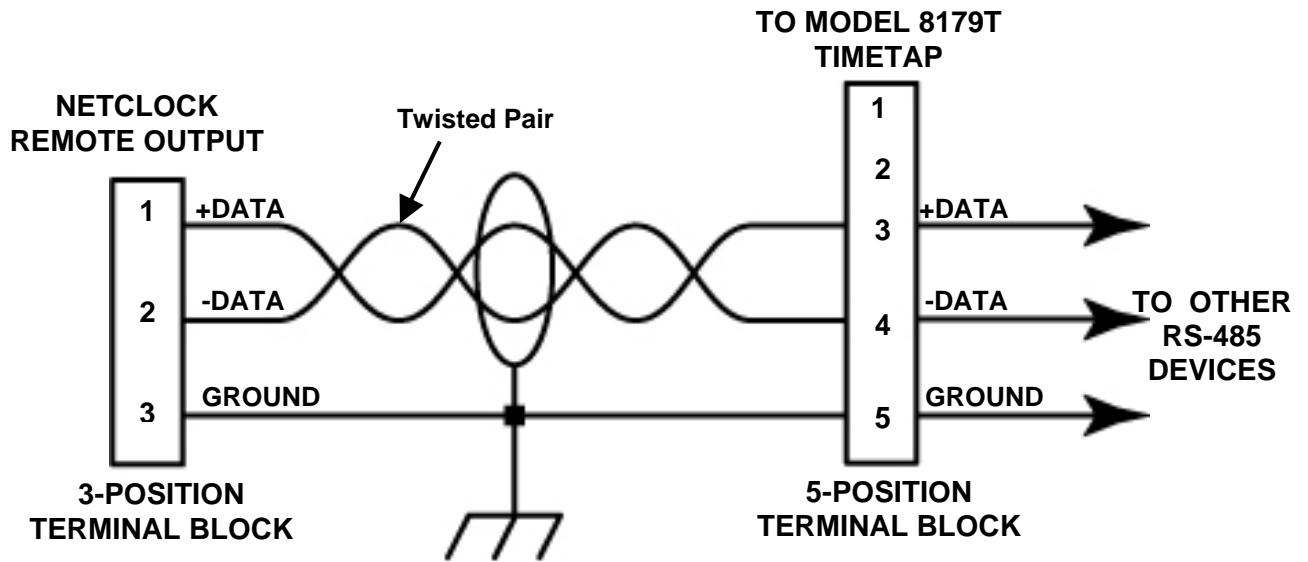


Figure 2-8: Model 8179T TimeTap RS-485 Interface

Spectracom Model 9288 is an Ethernet Time Server that supports NTP and SNTP time protocols. The Model 9288 accepts Format 0, Format 2, Format 7, or Format 8 (Formats 7 and 8 are not available on all time sources – Contact Tech Support for additional information) and connects to the RS-485 data bus through a three-position terminal block. Connect the Model 9288 to the NetClock as shown in Figure 2-9.

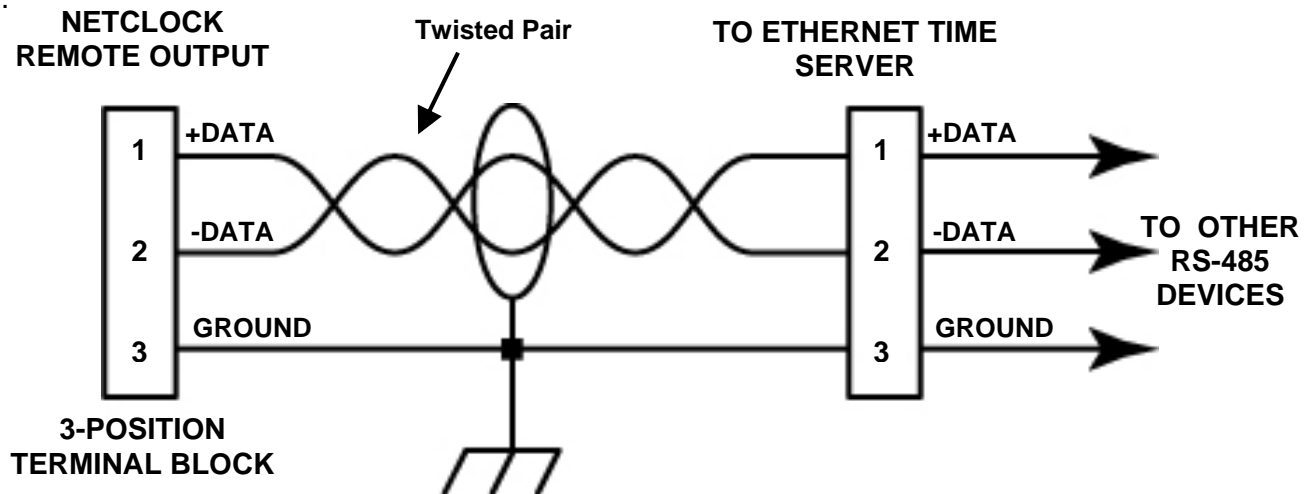


Figure 2-9: Model 9288 RS-485 Interface

The Model 8185, TimeBurst™, provides a digital time-of-day data burst to a radio transmitter. The TimeBurst accepts Data Format 0 or 1. Connect the TimeBurst to the RS-485 data bus using a 3-position terminal block as shown in Figure 2-10.

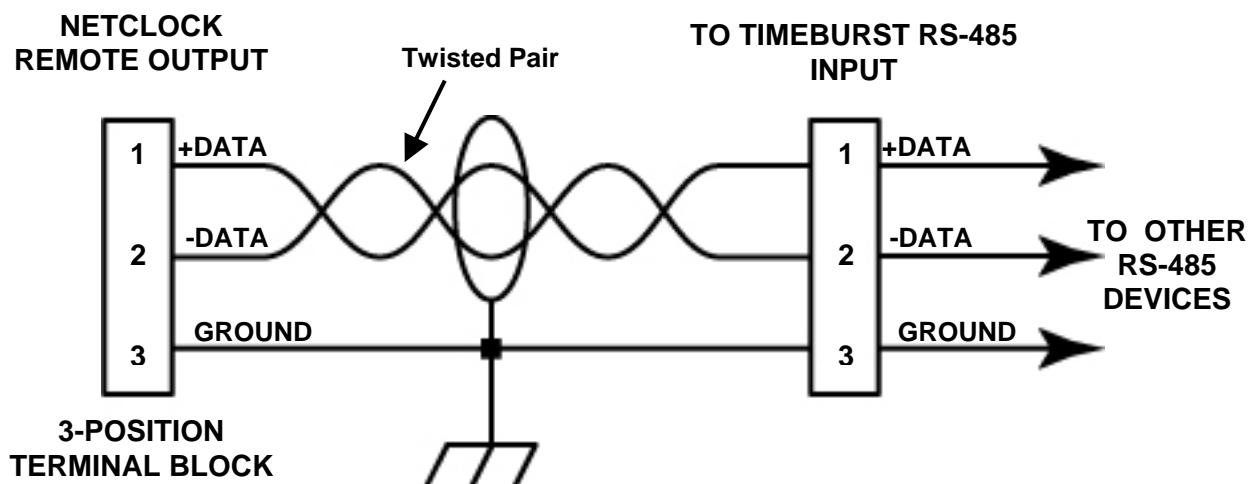


Figure 2-10: TimeBurst RS-485 Interface

2.6.6 Termination

A 120 Ohm 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 2-4), terminate the last device on the bus. The RS-485 data bus can be split in two directions as shown in Figure 2-5. In a split bus configuration, terminate the devices installed on each end of the bus. Some Spectracom products include a built-in termination switch to terminate the RS-485 bus when required or a resistor is supplied with the equipment if no termination switch is available. The terminating resistor is installed between the positive and negative connections on the terminal block of the last RS-485 connection.

3 Product Configuration

NOTE: Screens shown in this manual are for illustrative purposes. Actual screens may vary. Software common to multiple NetClock models may be used to generate these screens. As a result, labels in the screens displayed may refer to units other than your specific NetClock. Software operation should be common among these models, where appropriate.

After installing the NetClock, verify that power is connected and wait for the device to boot up.

NOTE: If using DHCP, the IP address will be assigned automatically. You may use a Web browser to connect to this IP address and configure the NetClock through the Web Browser User Interface (Web UI) (Figure 3-1). Refer to *Network Configuration with DHCP*, Section 3.1.

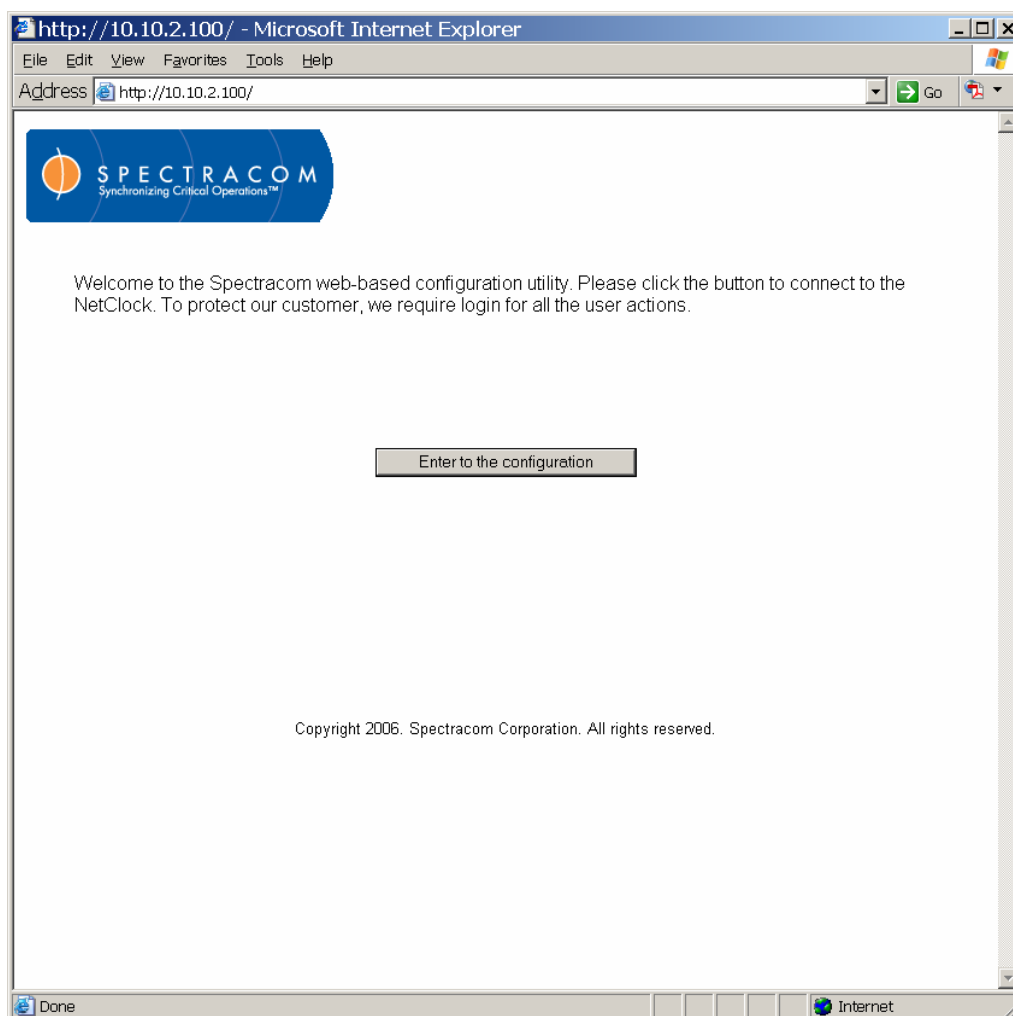


Figure 3-1: Entering to the Configuration in the Web UI

When configuring a NetClock without DHCP, or to configure a NetClock that has not been assigned an IP address, refer to *Network Configuration*, Section 3.2.

3.1 Network Configuration with DHCP

Once connected to the DHCP server through the network, the NetClock is assigned an IP address. This address and other network information is displayed on the front panel when the device boots up. Enter the IP address in your browser (on a computer connected to the network) and log in as an administrator. The http session will be redirected automatically to an https session and a security certificate pop-up window will be displayed. Accept the certificate by clicking “OK.”

NOTE: Unless you are using DNS in conjunction with DHCP (with the client configured using the NTP server’s hostname instead of IP address), DHCP must be disabled and the IP address must be changed to a static address once the NetClock is properly configured. Failure to do this will result in a loss of time synchronization if the DHCP server assigns a new IP address to the NetClock.



➔ Your login name is **admin**
The password is **admin123**

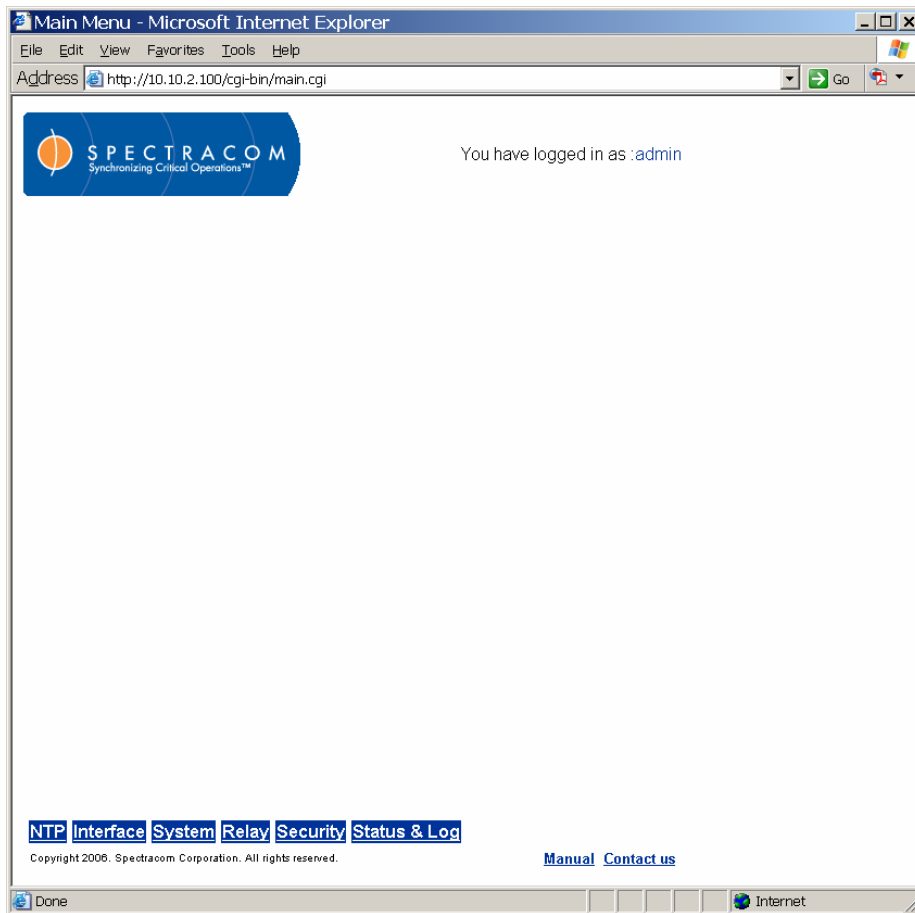


Figure 3-2: Web Browser User Interface (Web UI)

When you enter the NetClock IP address in your browser (which will differ from the IP address shown in the examples in this manual), you will be prompted to log in (Figure 3-1). The default administrator account is set at the factory as **admin**. The password is **admin123**.

After entering the login name and password and successfully logging into the NetClock, the user will see a Web UI screen similar to Figure 3-2. From this screen, click the Security tab. The Security menu will be displayed on the left side of the Web UI. Click the Network link to access the necessary Network configuration fields (Figure 3-3 and Figure 3-4).

Network

SSH
HTTPS
User Account
SNMP Security
LDAP General
LDAP Client Configuration
RADIUS General
RADIUS Client Configuration
IPSEC General
IPSEC Manual SA Configuration
IPSEC IKE SA Configuration

You have logged in as :admin

Hostname:

DNS Servers:

Primary DNS Server:

Secondary DNS Server:

IPv4 Configuration:

Enable DHCP

IP Address:

Subnet Mask:

Enable Gateway

Gateway Address:

IPv6 Configuration:

Enable DHCP6

IP Address	Prefix Length	Delete?
fe80::230:64ff:fe04:4aa3	64	<input type="checkbox"/>

Add a static IPv6 Address and Prefix Length:

IP Address:

Prefix Length:

Default Gateway:

NTP Interface System Relay Security Status & Log

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

https://10.10.2.103/cgi-bin/shownetconf.cgi 10.10.2.103

Figure 3-3: Security – Network Screen (1 of 2)

Refer to the *Initial Network Configuration* section to continue your product configuration.

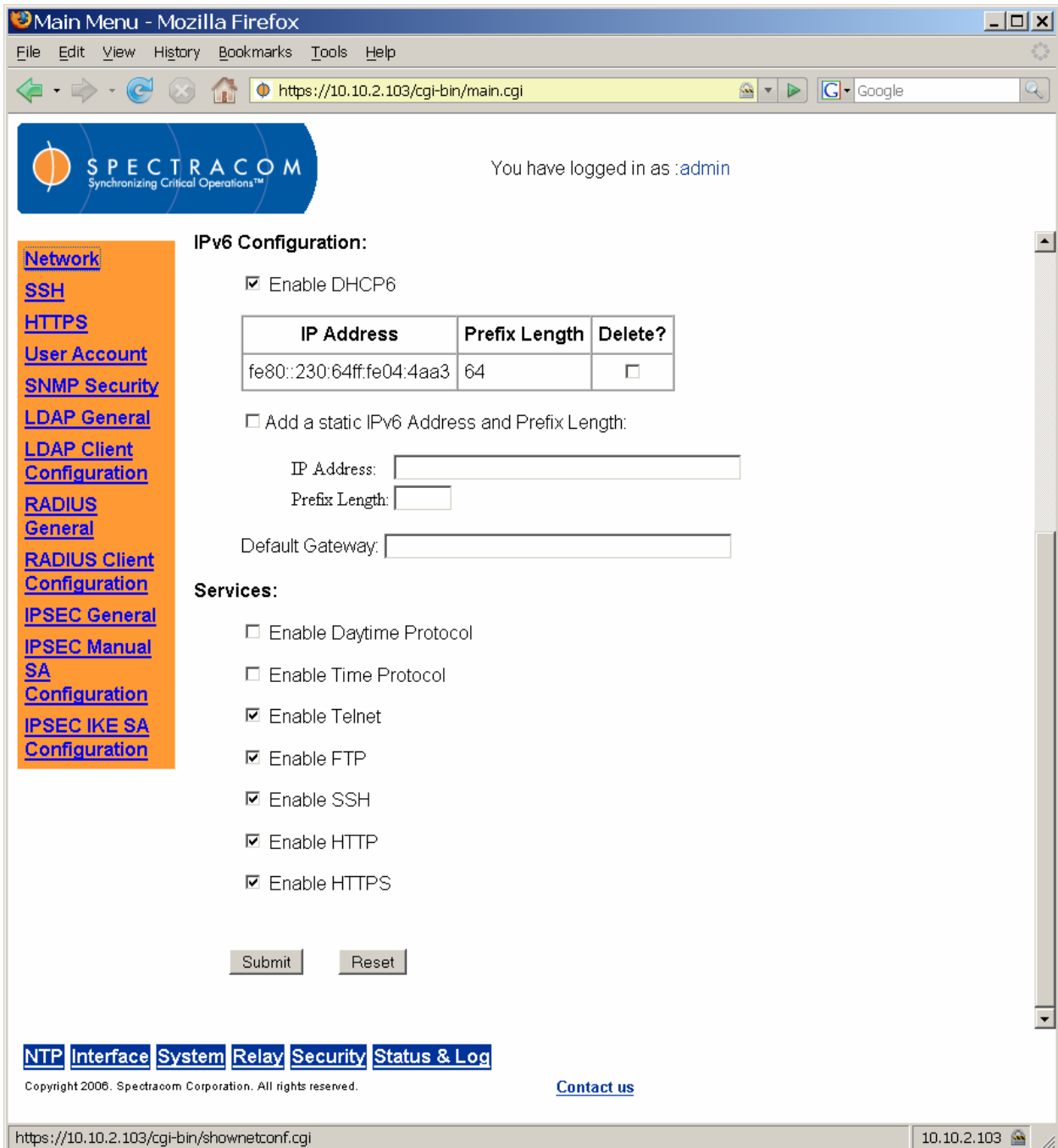


Figure 3-4: Security – Network Screen (2 of 2)

3.2 Initial Network Configuration

NOTE: The IP address assignment in this configuration may be performed even if your network has a DHCP server. There may be times when you do not wish DHCP to assign the IP address for the NetClock.

To configure a NetClock without DHCP or to configure a NetClock that has not been assigned an IP address, use the provided serial cable to connect a PC or laptop computer to the serial setup port on the back of the NetClock. After making this connection, use a terminal program (such as HyperTerminal) to log into the NetClock as an administrator. Use the Command Line Interface (CLI) in the terminal program to configure initial values and determine the NetClock's network address.

3.2.1 Using HyperTerminal to Connect to the Netclock

Microsoft's HyperTerminal program is typically located under *Accessories – Communications* in the Windows PC Start Menu. (Most terminal programs can be used to connect to the NetClock. it is not necessary to use HyperTerminal specifically.) Establish a new connection using the serial port to which you have connected the NetClock (typically COM1).



Figure 3-5: Establishing a New Terminal Connection



Figure 3-6: Connecting to the Computer's Serial Port

Configure the COM1 properties as shown in Figure 3-7. *Bits per second* should be **9600**. *Data bits* should be **8**. *Parity* should be **none**. *Stop bits* should be **1**. *Flow control* should be **none**. When the connection is established in the terminal window, the command line prompt will appear (Figure 3-8).

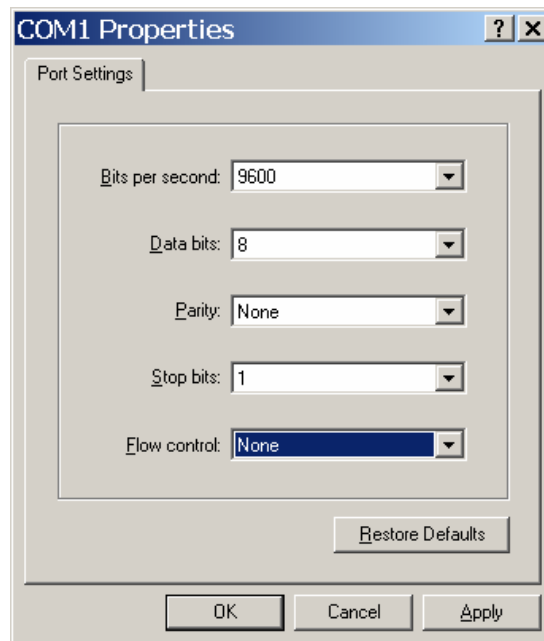


Figure 3-7: Configuring the Serial Port Connection Properties

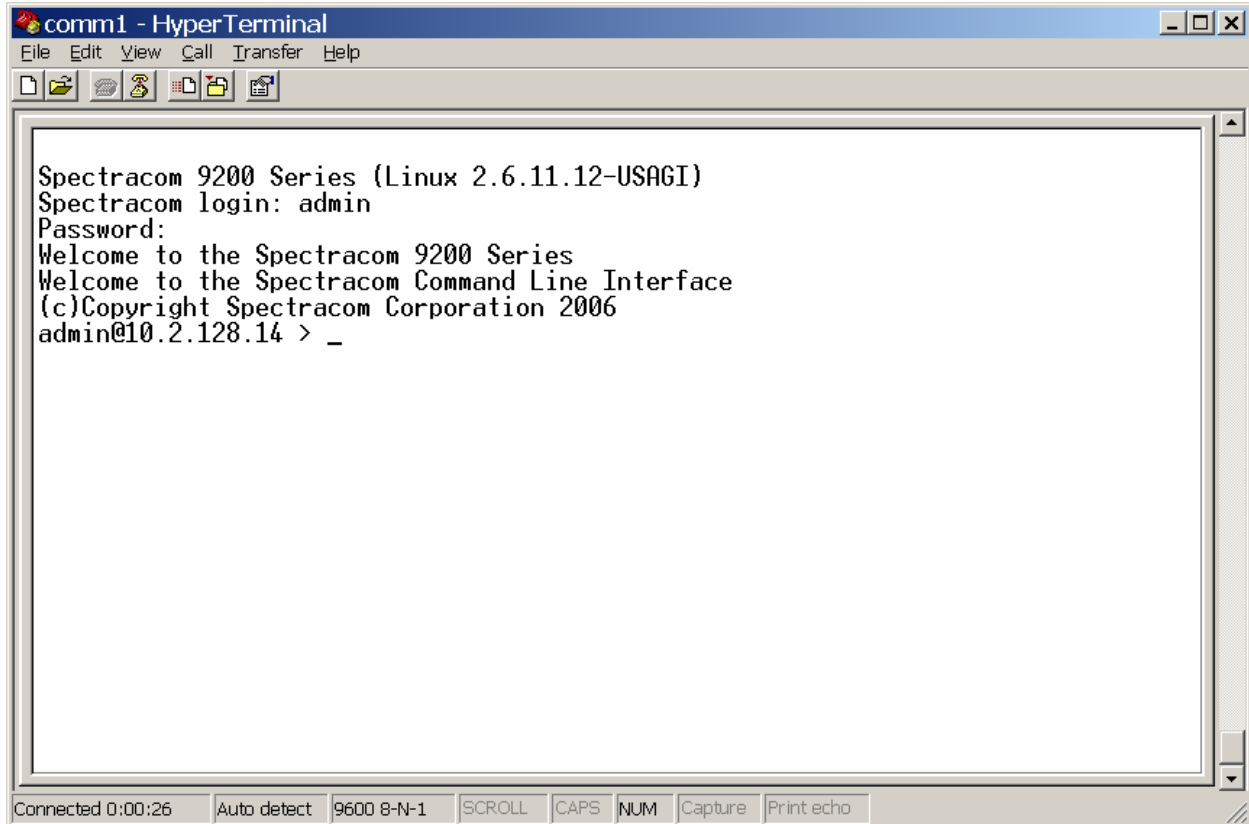


Figure 3-8: Spectracom NetClock Command Line Interface (CLI)

Log in as an administrator using the name **admin** and the password **admin123**. (Login names and passwords are case-sensitive.) A successful login will return the prompt *admin@x.x.x.x*, where *x.x.x.x* is the IP address of the NetClock.

Typing **help** in the Command Line Interface (CLI) will display a list of available commands (Figure 3-9). Typing **net** will display the CLI net commands. The command **net config** will walk the user through initial configuration.

```

comm1 - HyperTerminal
File Edit View Call Transfer Help
Spectracom 9200 Series (Linux 2.6.11.12-USAGI)
Spectracom login: admin
Password:
Welcome to the Spectracom 9200 Series
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.2.128.14 > help
Command line interface (CLI) help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
    time      - time
    reboot    - reboot
    log       - log COMMAND OBJECT [ HANDLE ]
    option    - option COMMAND [OPTION | PRODUCT] [VALUE]
    ltc       - ltc COMMAND [INDEX | NAME] [...]
    net       - net COMMAND [Arguments]
    sys       - sys COMMAND [Arguments]
    mdo       - mdo COMMAND [Arguments]
    ser       - ser COMMAND SERIAL [Arguments]
    rem       - rem COMMAND REMOTE [Arguments]
    irig      - irig COMMAND ARG
    frq       - frq COMMAND INDEX [Arguments]
admin@10.2.128.14 >

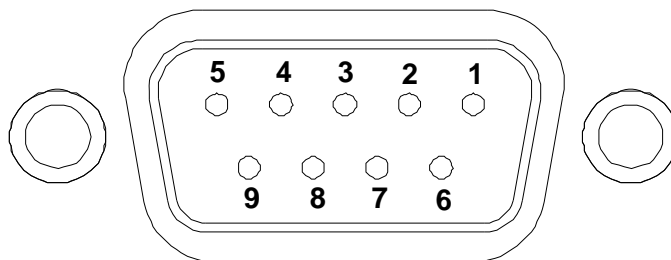
```

Connected 0:00:12 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 3-9: Available CLI Commands

Initial configuration settings can be modified subsequently through either the serial port or the Web UI. The values entered in the following fields are specific to your setup. Your network administrator may assign and provide some or all of the required information.

If you are not using DHCP in conjunction with DNS (using domain names rather than IP addresses), the IP address of the NetClock must be changed from the factory default to the new static address for your particular network before the NetClock can be accessed through the Web UI (and before it can provide NTP time stamps to synchronize the network).

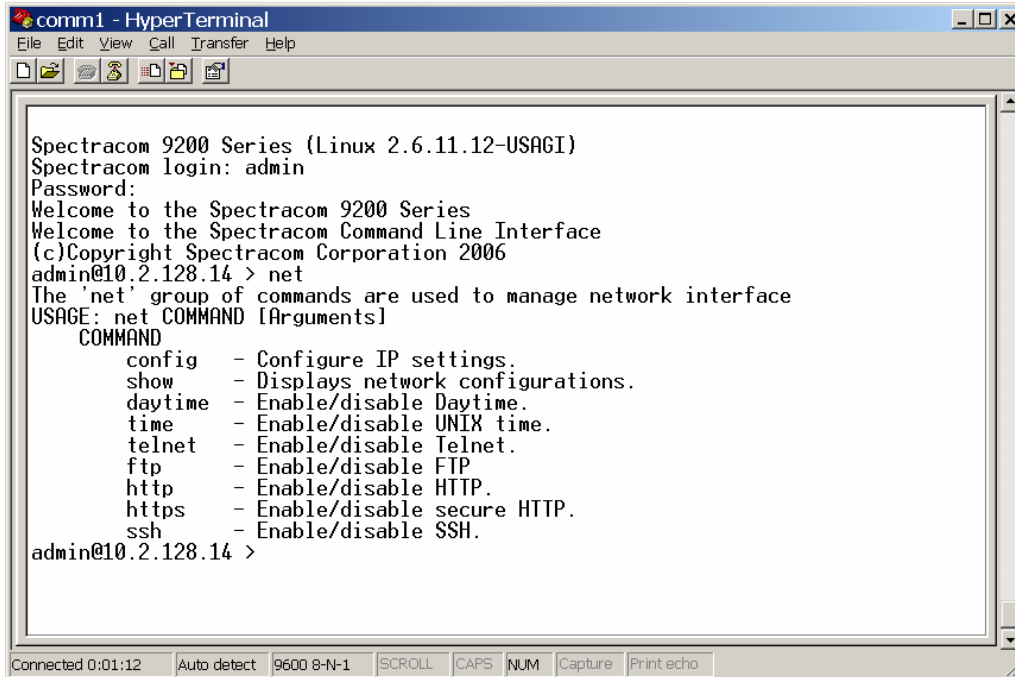
**Figure 3-10: Serial Port Pin Configuration**

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 Cable Pin-Outs

3.2.2 Initial Network Setup

At the CLI, enter the command **net config**. Set the prompted values to complete initial network setup. In this manual, the convention <enter> is used to indicate pressing the enter key.

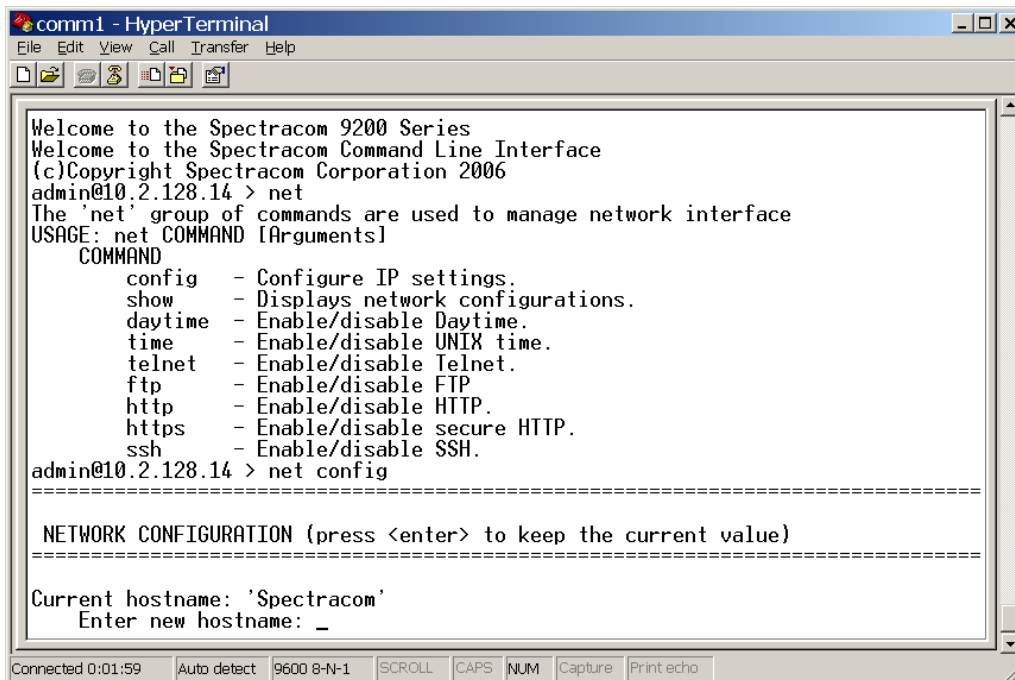


```

comm1 - HyperTerminal
File Edit View Call Transfer Help
Spectracom 9200 Series (Linux 2.6.11.12-USAGI)
Spectracom login: admin
Password:
Welcome to the Spectracom 9200 Series
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.2.128.14 > net
The 'net' group of commands are used to manage network interface
USAGE: net COMMAND [Arguments]
COMMAND
config - Configure IP settings.
show - Displays network configurations.
daytime - Enable/disable Daytime.
time - Enable/disable UNIX time.
telnet - Enable/disable Telnet.
ftp - Enable/disable FTP
http - Enable/disable HTTP.
https - Enable/disable secure HTTP.
ssh - Enable/disable SSH.
admin@10.2.128.14 >

```

Figure 3-11: Net Commands



```

comm1 - HyperTerminal
File Edit View Call Transfer Help
Welcome to the Spectracom 9200 Series
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.2.128.14 > net
The 'net' group of commands are used to manage network interface
USAGE: net COMMAND [Arguments]
COMMAND
config - Configure IP settings.
show - Displays network configurations.
daytime - Enable/disable Daytime.
time - Enable/disable UNIX time.
telnet - Enable/disable Telnet.
ftp - Enable/disable FTP
http - Enable/disable HTTP.
https - Enable/disable secure HTTP.
ssh - Enable/disable SSH.
admin@10.2.128.14 > net config
=====
NETWORK CONFIGURATION (press <enter> to keep the current value)
=====
Current hostname: 'Spectracom'
Enter new hostname: _

```

Figure 3-12: Prompt for Initial Configuration Values in the CLI

During initial configuration, you will be prompted to enable or disable and enter, as necessary, various settings and addresses. The include the following:

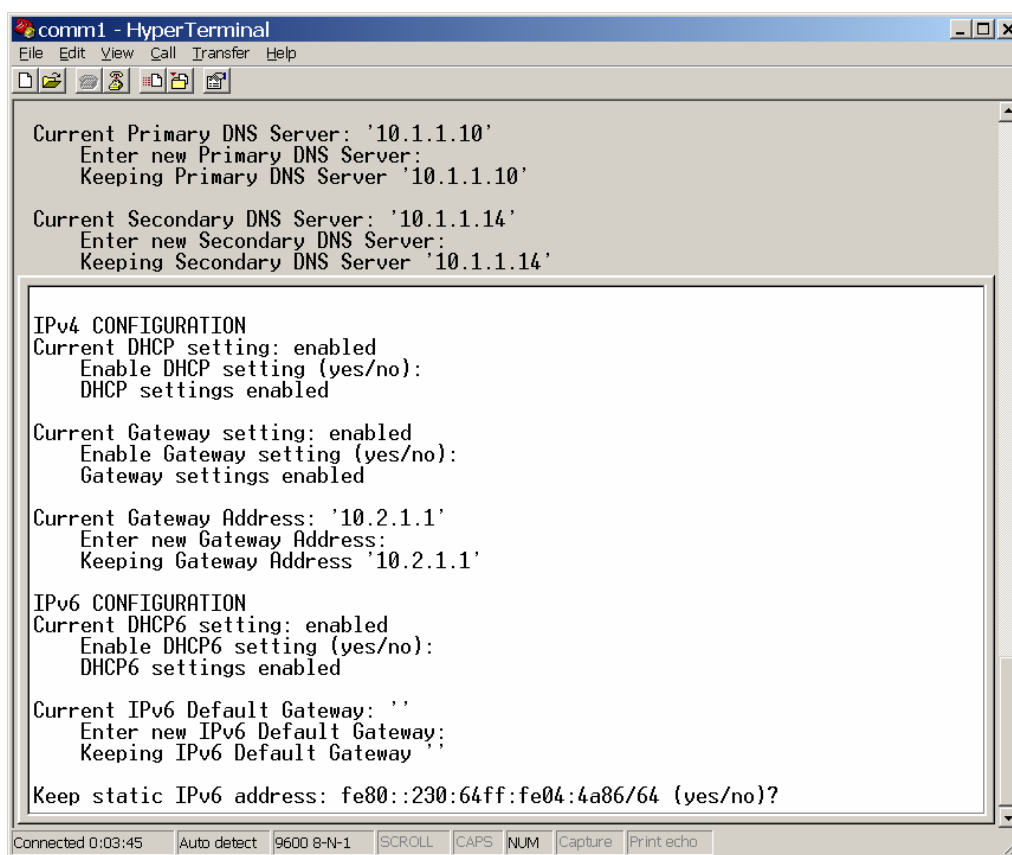
Hostname: This is the network hostname that identifies the NetClock.

DNS Server: This is the IP address of the DNS server (if any).

DHCP Setting: This enables or disables DHCP. This must be set for IPv4 and IPv6. The NetClock always generates a static IPv6 address in addition to the dynamic IPv6 address(es).

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 must be specified. The default is disabled.

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



```
comm1 - HyperTerminal
File Edit View Call Transfer Help

Current Primary DNS Server: '10.1.1.10'
Enter new Primary DNS Server:
Keeping Primary DNS Server '10.1.1.10'

Current Secondary DNS Server: '10.1.1.14'
Enter new Secondary DNS Server:
Keeping Secondary DNS Server '10.1.1.14'

IPv4 CONFIGURATION
Current DHCP setting: enabled
Enable DHCP setting (yes/no):
DHCP settings enabled

Current Gateway setting: enabled
Enable Gateway setting (yes/no):
Gateway settings enabled

Current Gateway Address: '10.2.1.1'
Enter new Gateway Address:
Keeping Gateway Address '10.2.1.1'

IPv6 CONFIGURATION
Current DHCP6 setting: enabled
Enable DHCP6 setting (yes/no):
DHCP6 settings enabled

Current IPv6 Default Gateway: ''
Enter new IPv6 Default Gateway:
Keeping IPv6 Default Gateway ''

Keep static IPv6 address: fe80::230:64ff:fe04:4a86/64 (yes/no)?

Connected 0:03:45 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Figure 3-13: Initial Configuration using the CLI

```

comm1 - HyperTerminal
File Edit View Call Transfer Help
[Icons]

Current Gateway setting: enabled
  Enable Gateway setting (yes/no):
  Gateway settings enabled

Current Gateway Address: '10.2.1.1'
  Enter new Gateway Address:
  Keeping Gateway Address '10.2.1.1'

IPv6 CONFIGURATION
Current DHCP6 setting: enabled
  Enable DHCP6 setting (yes/no):
  DHCP6 settings enabled

Current IPv6 Default Gateway: ''
  Enter new IPv6 Default Gateway:
  Keeping IPv6 Default Gateway ''

Keep static IPv6 address: fe80::230:64ff:fe04:4a86/64 (yes/no)?
  Keeping static IPv6 address: fe80::230:64ff:fe04:4a86/64

Add static IPv6 Address (<enter> for none):

Network configuration successful
admin@10.2.128.14 >

Connected 0:04:04  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo

```

Figure 3-14: Successful Completion of Network Configuration

- NOTE:** All IPv4 addresses must be entered in “dotted quad” format. All IPv6 addresses must be entered in standard IPv6 address format.
- NOTE:** Setting the gateway to Disabled will cause the values in the Gateway Address field to be ignored.
- NOTE:** Changing the IP address of the NetClock to a different subnet will prompt the NetClock to start using the new IP address immediately. If you are connected to the CLI through a network instead of directly through the serial setup port, your session will end when the IP address is changed. Start a new session and use the new IP address to reconnect to the CLI.

3.2.3 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.


Configuration	Default	Recommended	Where Enabled
HTTP	Enabled	Disabled	Web User Interface or Command Line Interface
SNMP	Disabled	Disabled or Enabled	Web User Interface
NTP	Enabled – With no MD5 Values Entered	Enabled – Use MD5 authentication with user-defined keys	Web User Interface
Daytime Protocol	Disabled	Disabled	Web User Interface
Time Protocol	Disabled	Disabled	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

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

Table 3-2: Default and Recommended Configurations

3.3 Issuing the HALT Command before Removing Power

Once power is applied to the NetClock, it should not be removed unless the HALT command is issued to the unit. This prevents corruption of the NetClock file system.

CAUTION:		<p>Once power is applied to the unit, DO NOT disconnect power unless the HALT command is first issued to the NetClock. To be absolutely certain that it is safe to remove power, wait 30 seconds after the HALT command is issued before removing power.</p>
-----------------	---	---

The HALT command may be issued to the NetClock through the Web UI, through the CLI, or through SNMP.

3.3.1 Issuing the HALT Command through the Web UI

From the System Reboot/Halt page (Figure 3-15), click the Halt Now button. Wait 30 seconds after making the HALT request before removing power to the unit. (The system may also be rebooted from this screen.)

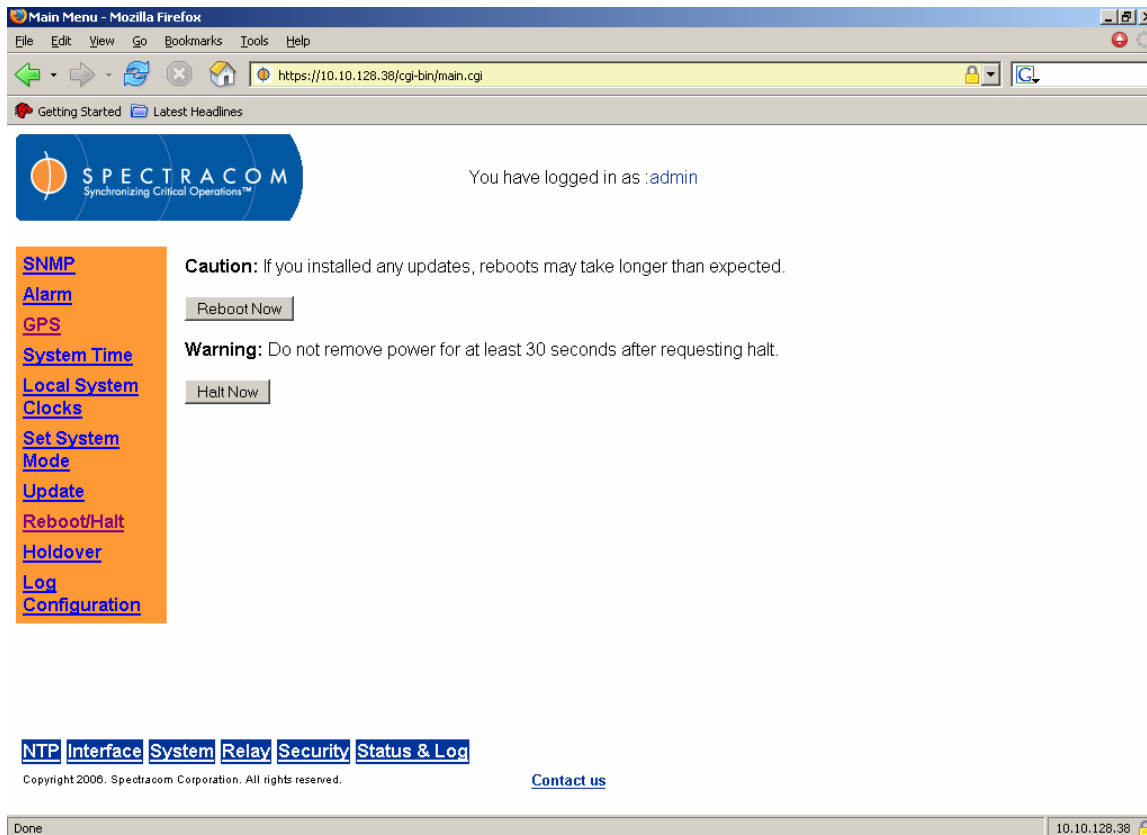


Figure 3-15: System Reboot/Halt Screen (1 of 3)

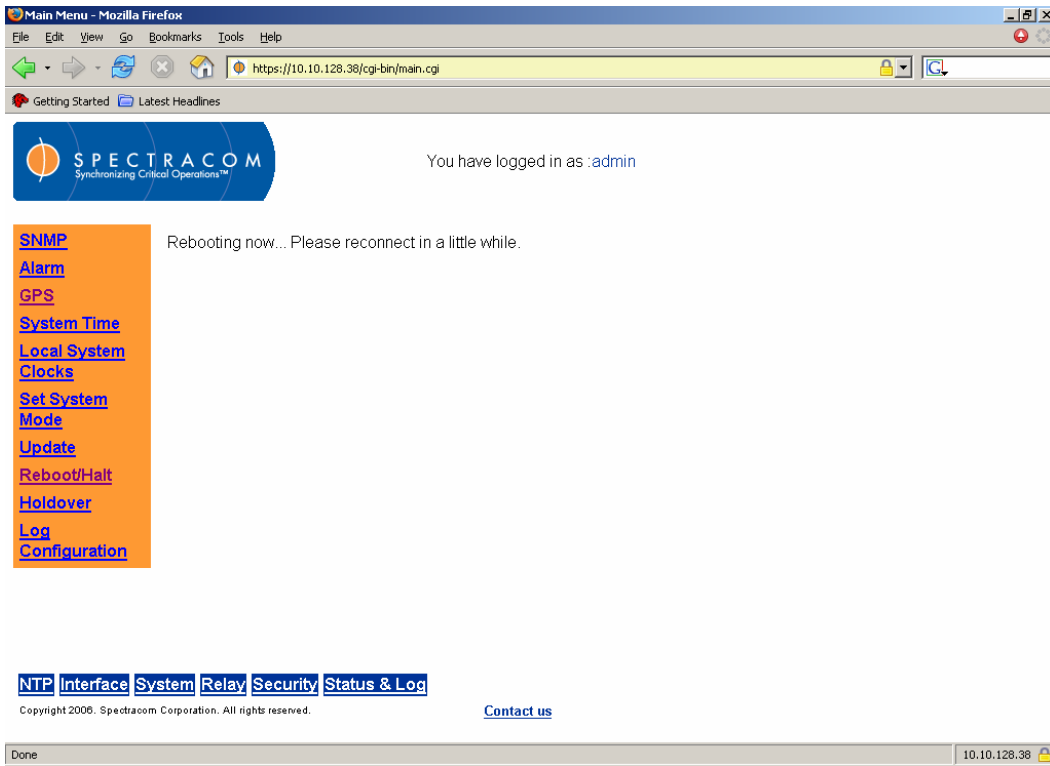


Figure 3-16: System Reboot/Halt Screen (2 of 3)

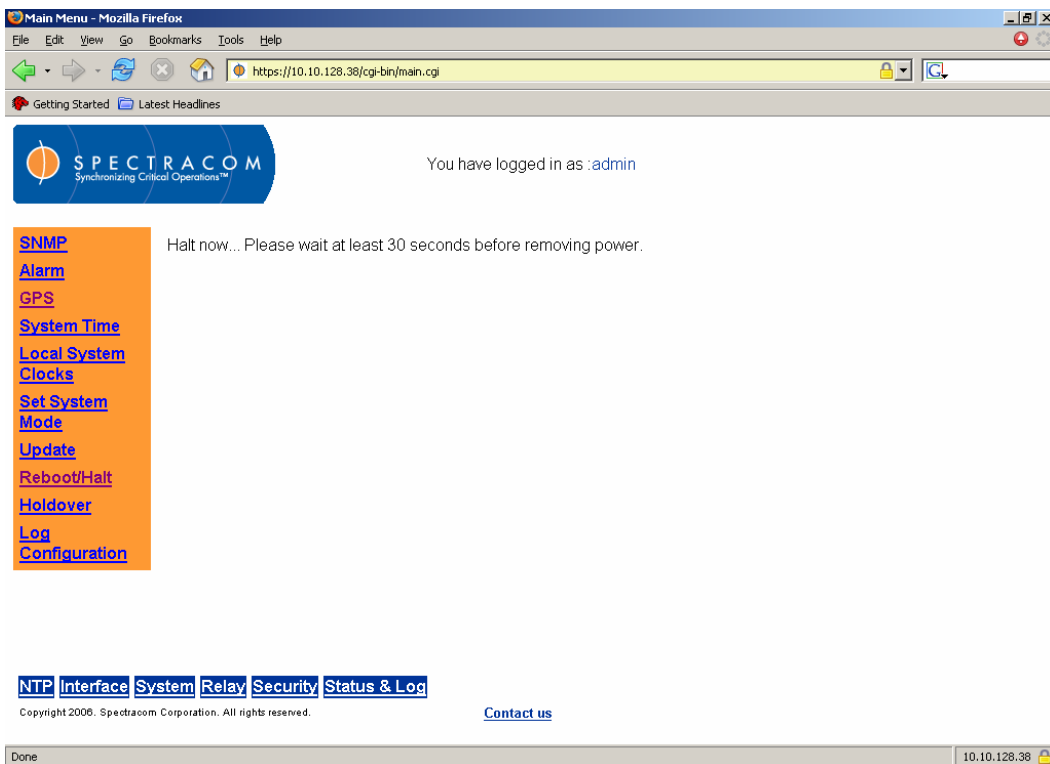
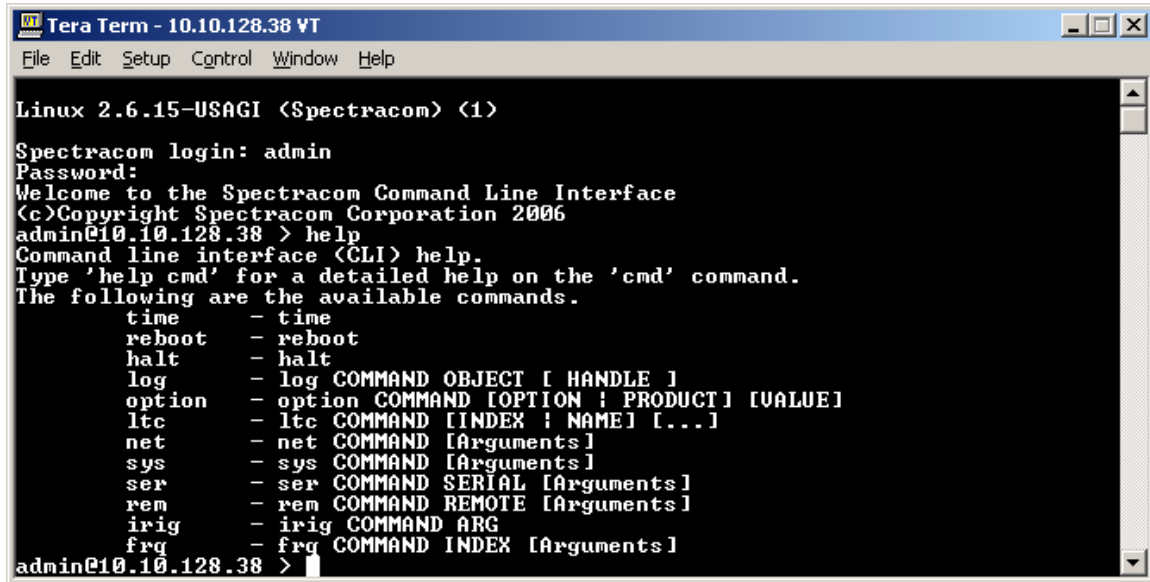


Figure 3-17: System Reboot/Halt Screen (3 of 3)

3.3.2 Issuing the HALT Command through the CLI

From the CLI (Figure 3-18), enter halt (Figure 3-19) Entering reboot will reboot the system (Figure 3-20).

NOTE: Wait 30 seconds after entering the HALT command before removing power.



```

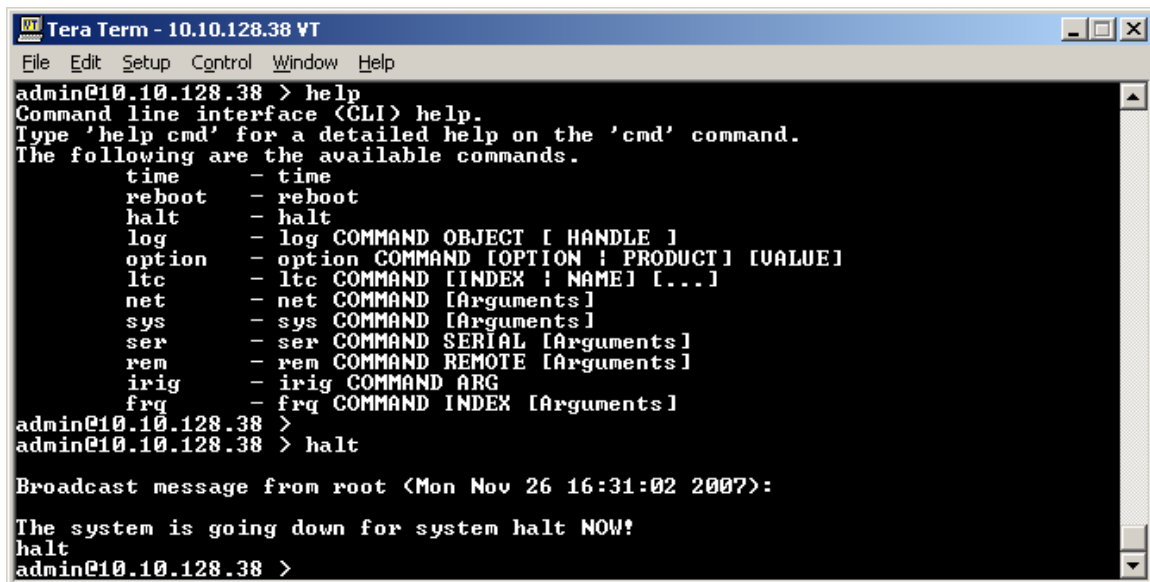
Tera Term - 10.10.128.38 VT
File Edit Setup Control Window Help

Linux 2.6.15-USAGI <Spectracom> <1>

Spectracom login: admin
Password:
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.10.128.38 > help
Command line interface <CLI> help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
    time      - time
    reboot    - reboot
    halt      - halt
    log       - log COMMAND OBJECT [ HANDLE ]
    option    - option COMMAND [OPTION ! PRODUCT] [VALUE]
    ltc       - ltc COMMAND [INDEX ! NAME] [...]
    net       - net COMMAND [Arguments]
    sys       - sys COMMAND [Arguments]
    ser       - ser COMMAND SERIAL [Arguments]
    rem       - rem COMMAND REMOTE [Arguments]
    irig      - irig COMMAND ARG
    frq       - frq COMMAND INDEX [Arguments]
admin@10.10.128.38 >

```

Figure 3-18: Command Line Interface (CLI)



```

Tera Term - 10.10.128.38 VT
File Edit Setup Control Window Help

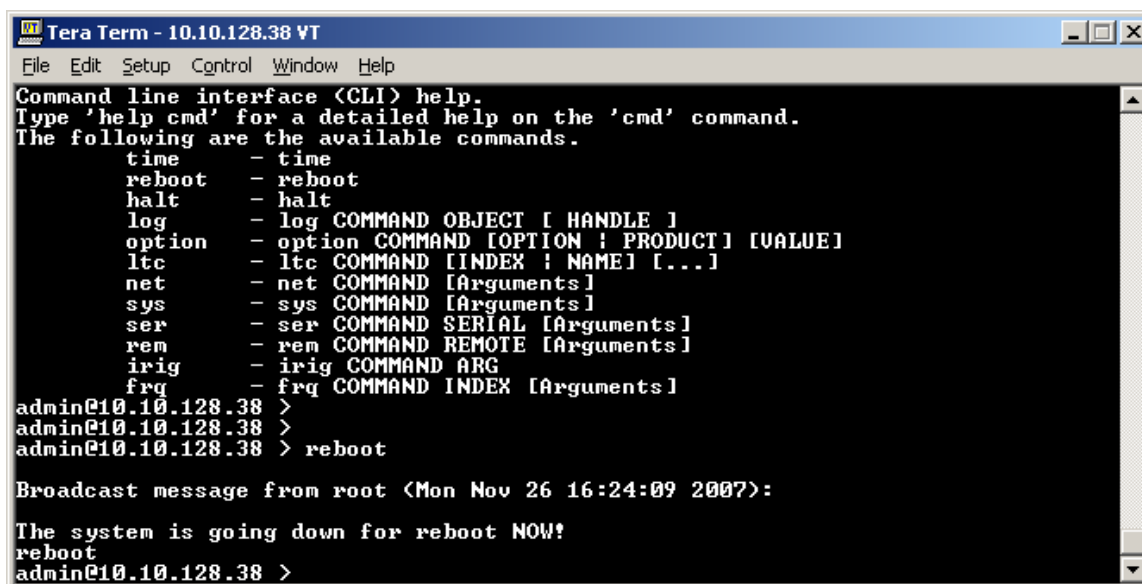
admin@10.10.128.38 > help
Command line interface <CLI> help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
    time      - time
    reboot    - reboot
    halt      - halt
    log       - log COMMAND OBJECT [ HANDLE ]
    option    - option COMMAND [OPTION ! PRODUCT] [VALUE]
    ltc       - ltc COMMAND [INDEX ! NAME] [...]
    net       - net COMMAND [Arguments]
    sys       - sys COMMAND [Arguments]
    ser       - ser COMMAND SERIAL [Arguments]
    rem       - rem COMMAND REMOTE [Arguments]
    irig      - irig COMMAND ARG
    frq       - frq COMMAND INDEX [Arguments]
admin@10.10.128.38 >
admin@10.10.128.38 > halt

Broadcast message from root <Mon Nov 26 16:31:02 2007>:

The system is going down for system halt NOW!
halt
admin@10.10.128.38 >

```

Figure 3-19: Halting the System from the CLI



```

Tera Term - 10.10.128.38 VT
File Edit Setup Control Window Help
Command line interface <CLI> help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
  time      - time
  reboot    - reboot
  halt      - halt
  log       - log COMMAND OBJECT [ HANDLE ]
  option    - option COMMAND [OPTION ; PRODUCT] [VALUE]
  ltc       - ltc COMMAND [INDEX ; NAME] [...]
  net       - net COMMAND [Arguments]
  sys       - sys COMMAND [Arguments]
  ser       - ser COMMAND SERIAL [Arguments]
  rem       - rem COMMAND REMOTE [Arguments]
  irig      - irig COMMAND ARG
  frq       - frq COMMAND INDEX [Arguments]
admin@10.10.128.38 >
admin@10.10.128.38 >
admin@10.10.128.38 > reboot

Broadcast message from root <Mon Nov 26 16:24:09 2007>:

The system is going down for reboot NOW!
reboot
admin@10.10.128.38 >

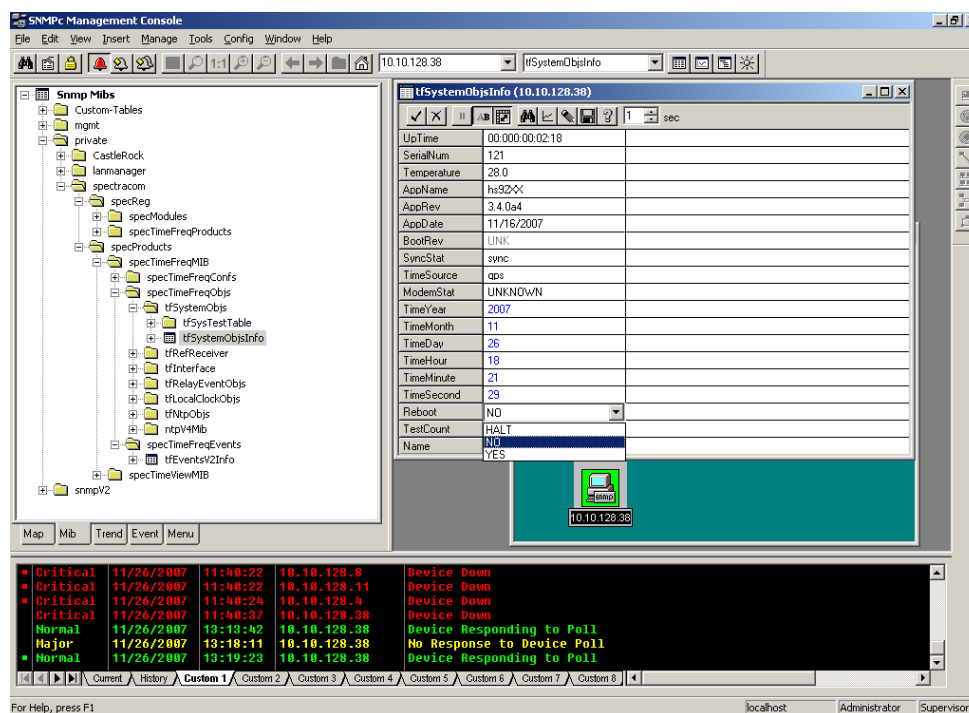
```

Figure 3-20: Rebooting the System from the CLI

3.3.3 Issuing the HALT Command through SNMP

The Reboot MIB location options in the NetClock (Figure 3-21) are as follows:

- HALT to shutdown (**NOTE:** Wait 30 seconds after shutting down before removing power)
- NO to do nothing
- YES to reboot the NetClock.



The screenshot shows the SNMP Management Console interface. On the left, a tree view displays the MIB structure under 'snmpMib', with 'tSystemObjInfo' selected. On the right, the configuration window for 'tSystemObjInfo (10.10.128.38)' is open, showing various parameters. The 'Reboot' dropdown is set to 'NO', and 'TestCount' is set to 'HALT'. Below the configuration window, a log window displays several events:

Severity	Date	Time	IP Address	Event Description
Critical	11/26/2007	11:40:22	10.10.128.8	Device Down
Critical	11/26/2007	11:40:22	10.10.128.11	Device Down
Critical	11/26/2007	11:40:24	10.10.128.4	Device Down
Critical	11/26/2007	11:40:37	10.10.128.38	Device Down
Normal	11/26/2007	13:13:42	10.10.128.38	Device Responding to Poll
Major	11/26/2007	13:18:11	10.10.128.38	No Response to Device Poll
Normal	11/26/2007	13:19:23	10.10.128.38	Device Responding to Poll

Figure 3-21: Reboot MIB Location Options (SNMP)

To reboot or halt the NetClock through SNMP, Spectracom provides a REBOOT MIB option. This is found in the tfSystemObjsInfo table in the Spectracom Time and Frequency MIB under Spectracom Products specProduct, specTimeFreqMIB, in the specTimeFreqObjs under tfSystemObjs, in the table tfSystemObjsInfo. The REBOOT option (Figure 3-22) provides the choices of NO or YES for Reboot, and Halt to initiate a shut-down request.

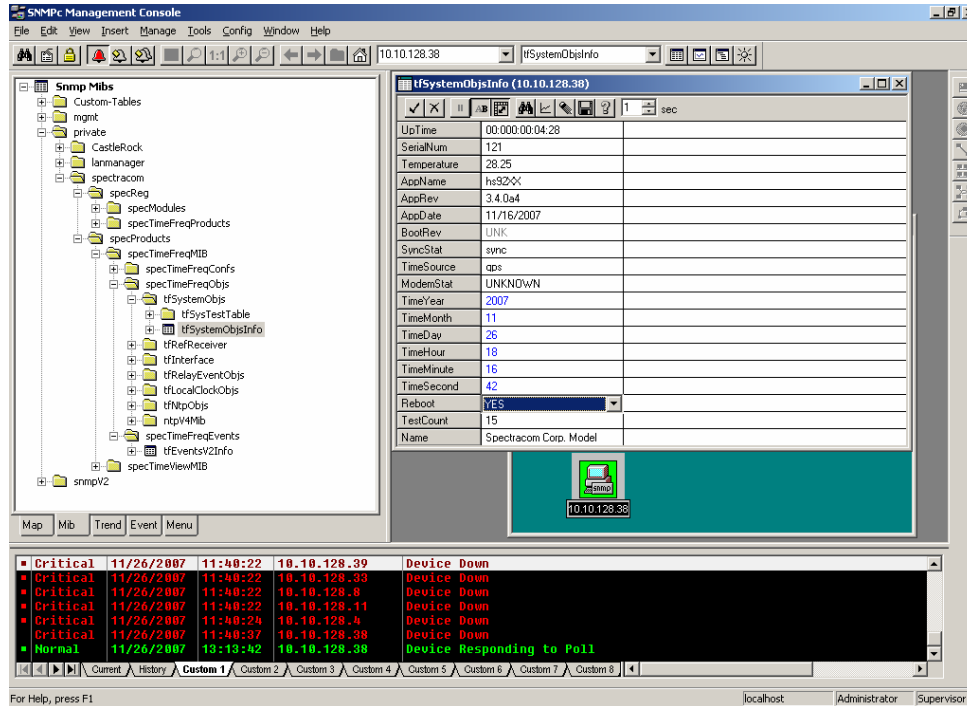


Figure 3-22: Rebooting the Unit through SNMP

To Reboot the unit, select YES and select the SET check box in the upper left corner of the SNMPc management console application. The Set operation reports success, but can with some SNMP managers return *Set Unsuccessful* due to a race condition in rebooting the unit and replying over SNMP. This is not an error.

To Halt the unit, select HALT and select the SET checkbox (Figure 3-23).

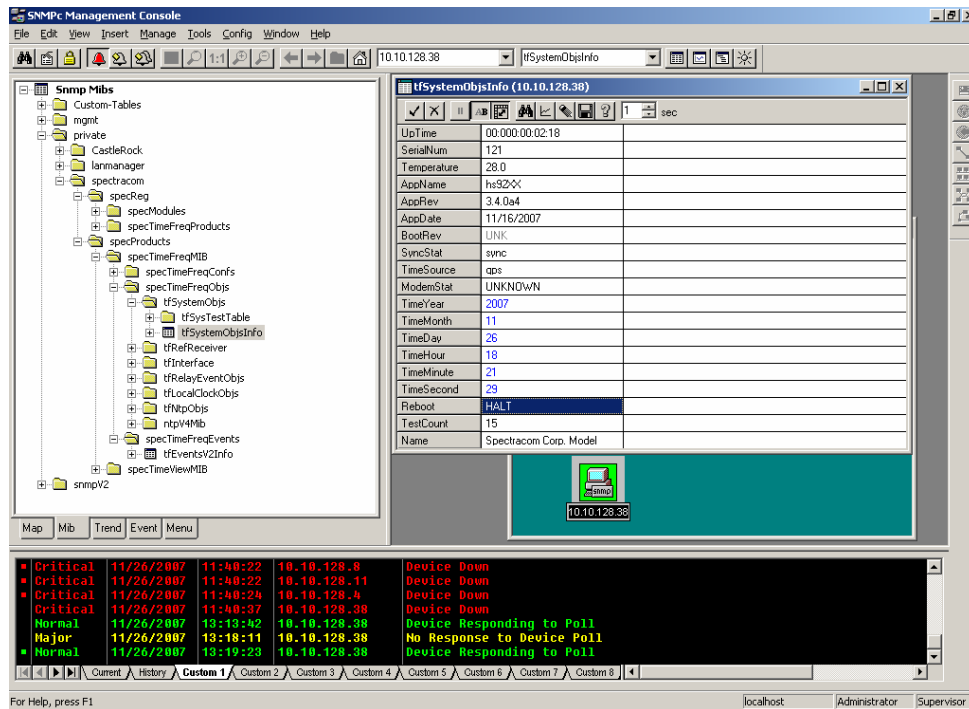


Figure 3-23: Halting the Unit through SNMP

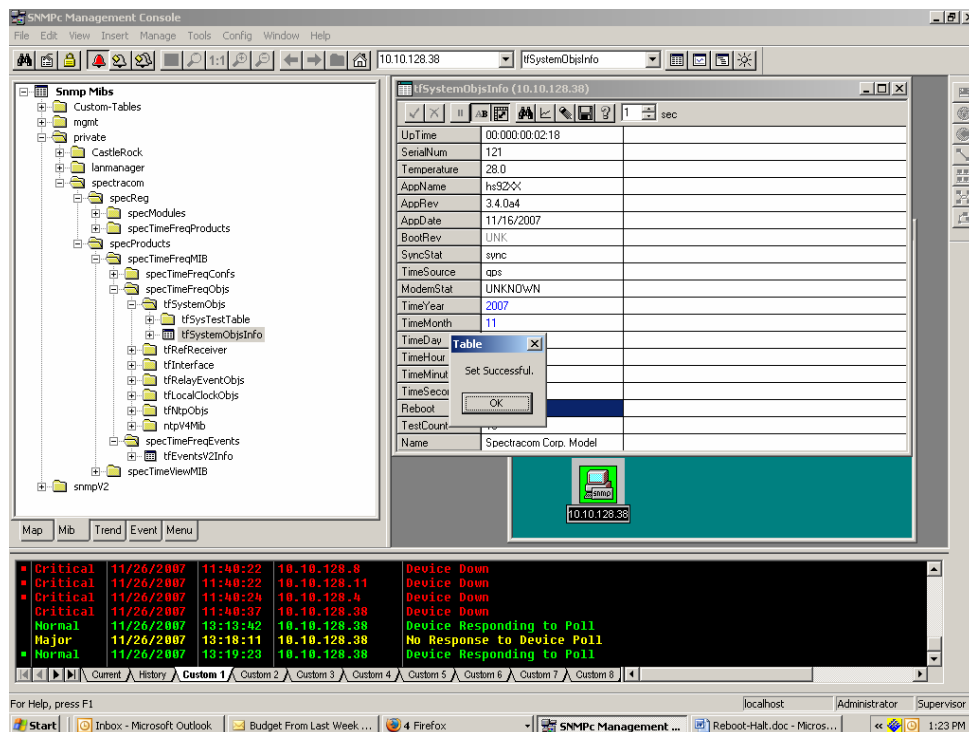


Figure 3-24: Successful Halt

The Set Successful Table box (Figure 3-24) will display to indicate that the Halt request to shut down the NetClock has been accepted. Wait 30 seconds before removing power.

3.4 Product Configuration using the WEB UI

With the NetClock connected to the network, you may configure it, change its operating settings, check its status, and generate reports from the Web UI as needed and desired. All Web UI screens are accessible through the menu at the bottom of the screen, which is displayed after a successful login. These screens, their functions, and example configurations (where applicable) are presented in this section.

NOTE: At any time during configuration in the Web UI, click “Submit” to save the settings or “Reset” to restore the settings to their previous state.



Figure 3-25: Web UI Primary Menu

3.4.1 Configuring NTP

The NTP menu groups the NetClock’s NTP configuration and reporting functions (Figure 3-26). From this menu, the user may access the NTP General, References, Symmetrical Keys, Autokey, and Status screens.

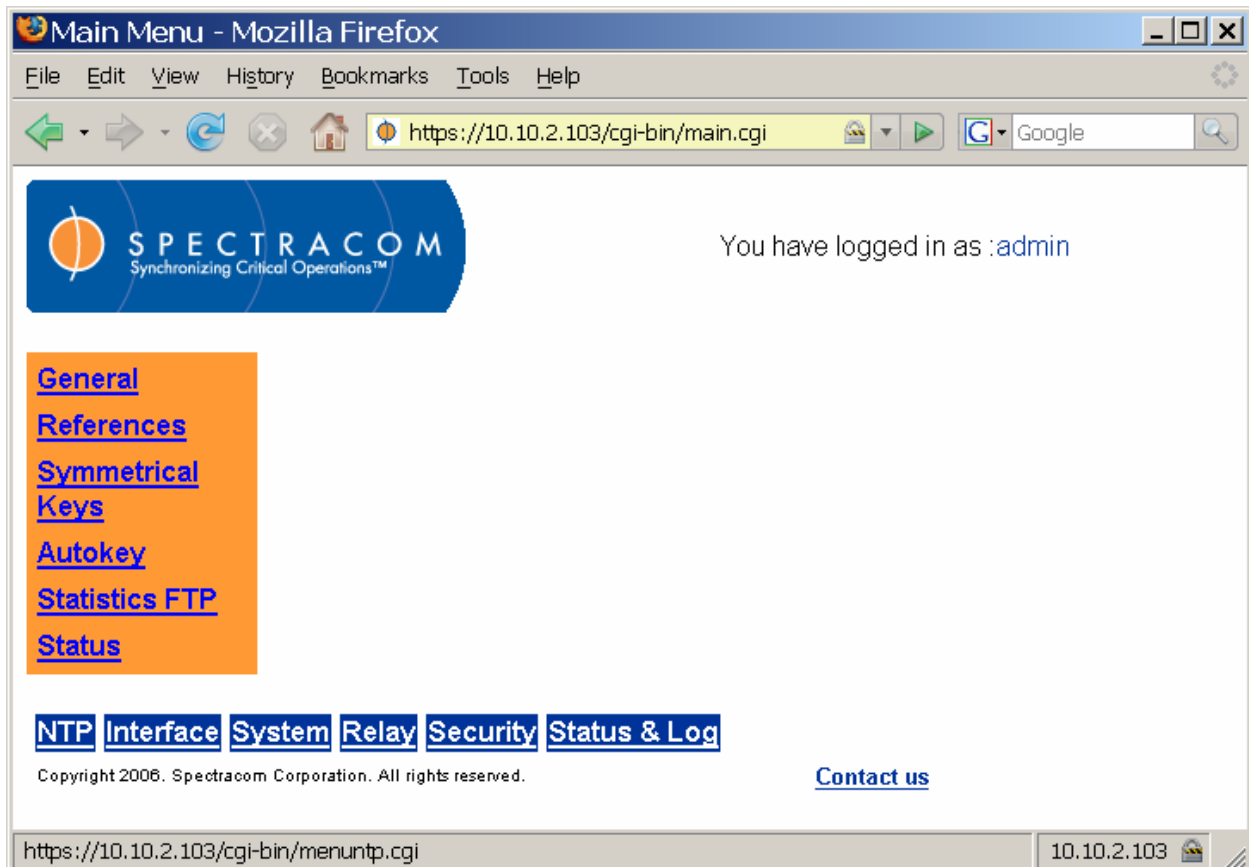


Figure 3-26: Web UI NTP Menu

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

General
[References](#)
[Symmetrical Keys](#)
[Autokey](#)
[Statistics FTP](#)
[Status](#)

NTP Service:
 Enabled Disabled

NTP Broadcasting:
 NTP Broadcast every
 Use MD5 authentication with trusted key ID:

NTP Access:
 Service all IPv4 requests by default.
 Service all IPv6 requests by default.

Type	IPv4/IPv6	IP Address/Hostname	IP Mask	Auth Only
<input type="text" value="Empty"/>	<input type="text" value="IPv6"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="text" value="Empty"/>	<input type="text" value="IPv4"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="text" value="Empty"/>	<input type="text" value="IPv4"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="text" value="Empty"/>	<input type="text" value="IPv4"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="text" value="Empty"/>	<input type="text" value="IPv4"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

NOTE: NTP Access can only be configured while the NTP Service is disabled.

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-27: NTP General Screen

Refer to Figure 3-27. The NetClock can operate in unicast mode, broadcast mode, or both. The user can enable or completely disable the NTP Service. When enabled, the NTP Service operates in unicast mode. In unicast mode the NTP Service responds to NTP requests only. The NTP Service supports a broadcast mode in which it sends a NTP time packet to the network broadcast address. Check the box for NTP Broadcast to enable broadcast mode and select a rate at which to broadcast from the dropdown box. The NTP Broadcast mode is intended for 1 or a few servers and many clients. The NTP Broadcast rate should be selected based upon the network utilization and time drift in the clients. NTP broadcast can utilize MD5 authentication. Select a single MD5 key to use for broadcast from the pulldown menu. Use of MD5 authentication requires that MD5 symmetrical keys already be defined on the NTP Symmetrical Keys page. With the NTP service enabled and NTP broadcasting checked, the NetClock will operate in both modes.

When the NTP service is enabled, 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 4,000 NTP requests per second without MD5 encryption enabled (and a somewhat lower rate with MD5 encryption enabled).

When NTP broadcasting is selected, the NTP server will send unsolicited NTP time packets to the local broadcast address at a user-selected rate. The rates available are included in the dropdown menu. The NTP clients can use unicast, broadcast or a combination of both to discover and synchronize with the NTP server.

The NTP server supports authenticated NTP packets using 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 with trusted key ID, both the NTP client and the NetClock 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 65532; the key string must be readable ASCII and between 1 and 16 characters long. Duplicate key IDs are not permitted. NTP requests received by the NTP server that do not contain an authenticator containing a valid Key ID and MD5 message digest pair will be responded to, but no authentication will be performed. NTP requests with valid authenticator result in a valid NTP response with its own valid authenticator using the same Key ID provided in the NTP request.

The NTP Access grid on the NTP General screen allows the user to enable or disable all IPv4 and IPv6 requests, as well as to allow or deny users or network segments. Clicking the “Auth Only” box on each line where a user or network segment is defined will prompt the NetClock to accept only authenticated requests (MD5 or Autokey) from this user or network segment.

From the NTP References screen (Figure 3-28), the user may check the “Enable Stratum 0 Reference” box. This makes the 9383 a Stratum 1 reference. If this box is not checked, it means the NetClock is a Stratum 2 (or higher) reference.

The grids on the NTP References screen allow the user to define, by IP address or hostname, the locations of other NTP servers to use as time references (instead of the configured NetClock’s GPS reference) and the locations of other NTP servers to use as peers. Peers are

NTP servers at the same stratum level that are used as an additional check on the NetClock's timing accuracy. This prevents it from moving to stratum levels farther away from Stratum 1 if the primary timing reference is lost. The maximum number of Peers allowed is 12. It is recommended to use one or more Peers when you desire to provide mutual backup. Each peer is normally configured to operate from one or more time sources including reference clocks or other higher stratum servers. If a peer loses all reference clocks or fails the other peers continue to provide time to other clocks on the network.

NTP servers can be configured as potential time references. The maximum number of NTP servers used as time references allowed is 12. For best results, more than 4 NTP time servers are recommended. As few as 1 NTP time server may be used, however, depending on your needs and network timing architecture. A specific NTP server can be configured as the preferred time reference by selecting the preferred checkbox. Only a single time reference can be selected as preferred and only when the Netclock is not in Stratum-1 mode using a Stratum-0 reference such as GPS, IRIG, Modem, or Serial Time Code Input.

For both NTP Peers and NTP Servers the Minimum and Maximum Poll rate for NTP packets can be configured. Both NTP Peers and NTP Servers support either manually configured Symmetric Key-ID/Key string pairs or the use of Auto-Key. However, these choices are mutually exclusive and must be identically configured on both the Netclock and the NTP Peer or NTP Server. If the Symmetric Key-ID/Key string pair method is selected the Key-ID must be first defined on the Symmetric Key page.

The entry for NTP Peer or NTP Server can be deleted by checking the Clear button and entering submit.

NTP Peers:

NTP Peers may be specified in the following table to form a peer server group. Servers in a peer group should each specify the other servers in the peer group. When a server in the peer group loses sync with its primary reference, it will choose another member of the peer group as backup, dropping to one above the stratum level of the chosen peer.

Peer IPv4/IPv6/Hostname	Min Poll	Max Poll	Trusted Sym Key ID	Autokey	Clear
	6 (1m 4s)	10 (17m 4s)	None	<input type="checkbox"/>	<input type="checkbox"/>
	6 (1m 4s)	10 (17m 4s)	None	<input type="checkbox"/>	<input type="checkbox"/>
	6 (1m 4s)	10 (17m 4s)	None	<input type="checkbox"/>	<input type="checkbox"/>
	6 (1m 4s)	10 (17m 4s)	None	<input type="checkbox"/>	<input type="checkbox"/>
	6 (1m 4s)	10 (17m 4s)	None	<input type="checkbox"/>	<input type="checkbox"/>

NTP Servers:

NTP Servers specified in the following table are used only as potential time references. If a server is chosen by the NetClock as the best reference, the stratum level of the NetClock will drop to one above the stratum level of the chosen server.

Enable Stratum-0 Reference (ie. GPS, Modem, Serial Time Code)

NOTE: When enabled, the Stratum-0 reference is ALWAYS preferred.

Server	Trusted
	<input type="checkbox"/>

Copyright 2000, Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-28: NTP References Screen (1 of 2)

NOTE: Check only ONE server as the preferred reference.

NOTE: You cannot use both a Trusted Symmetrical Key ID and Autokey. Autokey essentially automates the symmetrical key function and the two cannot be used together. If trusted keys have been defined (Figure 3-29), they will appear in the “Trusted Sym Key ID” dropdown menu.

NOTE: Checking the “Clear” box in the NTP References grids will immediately remove a defined server from the list.

The dropdown menus for “Min Poll” and “Max Poll” in the NTP References grids allow the user to choose, from within the available ranges, how often the NetClock will poll the defined servers for timing information. Check with your network administrator for guidelines regarding network traffic and recommended polling intervals, if any.

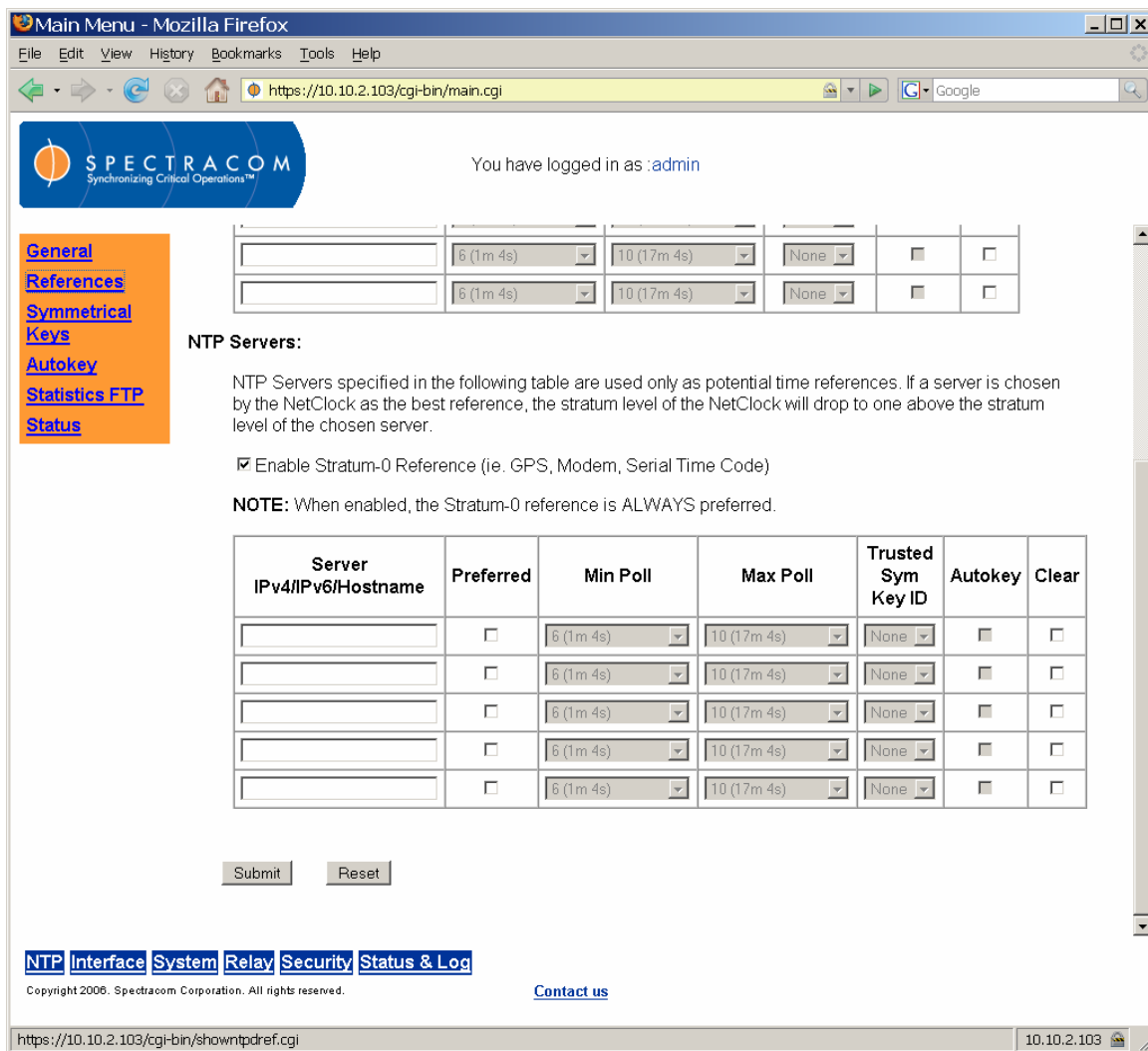


Figure 3-29: NTP References Screen (2 of 2)

From the Symmetrical Keys screen (Figure 3-30), the user may define the trusted symmetrical keys that must be entered on both the NetClock and any network client with which the NetClock is to communicate. The maximum number of Key-ID/Key String pairs is 15. Only those keys for which the “Trusted” box has been checked will appear in the dropdown menus on the NTP References screen (Figure 3-28).

Main Menu - Mozilla Firefox
 File Edit View History Bookmarks Tools Help
 https://10.10.2.103/cgi-bin/main.cgi
 Google

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as :admin

NTP Symmetrical Keys:

Trusted	Key Id (1 - 65532)	Key String (1 - 31 chars)
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Submit Reset

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006, Spectracom Corporation. All rights reserved. [Contact us](#)

Done 10.10.2.103

Figure 3-30: NTP Symmetrical Keys Screen

NOTE: It may be necessary to enter your username and password again in order to access the Symmetrical Keys screen.

Using Autokey essentially automates the trusted symmetrical key feature. From the Autokey screen (Figure 3-31), the user can click to enable or disable Autokey, enter a passphrase (readable ASCII, no spaces), and check “Generate Certificate” to generate a certificate in the text window at the bottom of the screen.

NOTE: Generate Certificate must always be clicked to generate the first certificate. If generating a new certificate after the first certificate, the menu will change to read “Regenerate Certificate.”

NOTE: Click the “Trusted” box on only ONE NetClock unit (the one that is closest to Stratum 0.)

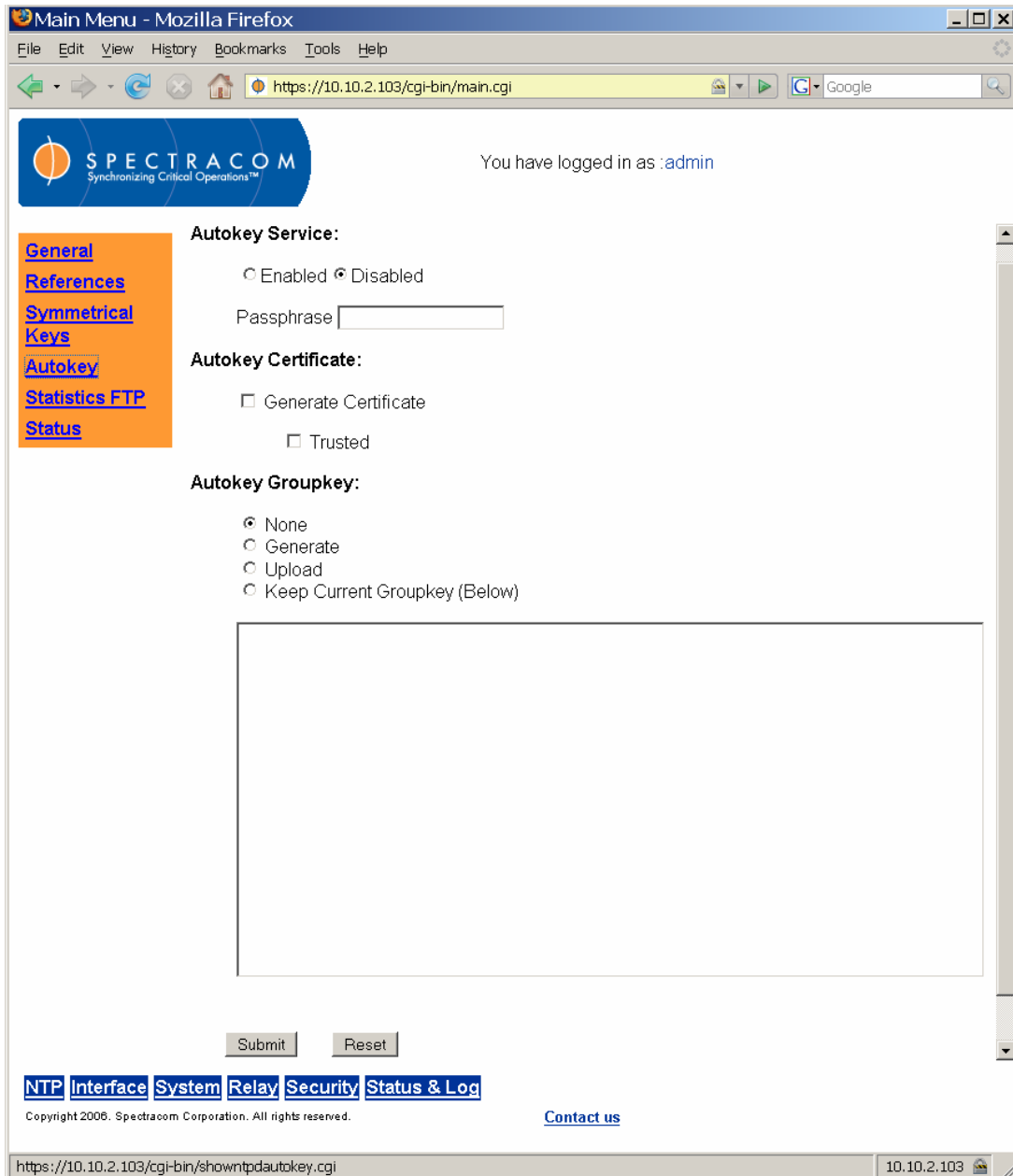


Figure 3-31: NTP Autokey Screen

NOTE: The Autokey feature can only be configured when NTP is disabled. If NTP is enabled, the fields in the Autokey screen cannot be accessed. To configure Autokey, disable NTP from the NTP General screen.

The user may also choose to use a Groupkey, which adds another level of authentication when using Autokey certificates. Click the “Generate” option under Autokey Groupkey to generate a certificate in the text window. Cut and paste this text into the text window on the other unit(s) and click the “Upload” option to upload it. Once an Autokey Groupkey has been generated the first time, the “Keep Current Groupkey (Below)” option will be selected by default.

The Statistics FTP screen (Figure 3-32) allows the user to configure the locations to which the unit transmits NTP statistical data. Files are sent to the remote server thirty minutes into every hour. Remote file names are appended with the UTC date stamp (YYYYMMDD).

The screenshot shows a web browser window titled "Main Menu - Mozilla Firefox" with the address bar displaying "https://10.10.2.103/cgi-bin/main.cgi". The page header includes the Spectracom logo and the text "You have logged in as :admin". A left-hand navigation menu contains links for General, References, Symmetrical Keys, Autokey, Statistics FTP (highlighted), and Status. The main content area is titled "Automatic FTP of NTP Statistics:" and features a radio button selection for "Enabled" (unselected) and "Disabled" (selected). Below this are input fields for "User Name:", "Password:", "FTP Server:", and "Remote Path:". A section titled "Remote File Names:" contains three input fields for "NTP Clock Statistics:", "NTP Loop Statistics:", and "NTP Peer Statistics:". Two notes are provided: "NOTE 1: Files are sent to the remote server 30 minutes into every hour." and "NOTE 2: Remote file names will be appended with a UTC date stamp (YYYYMMDD).". At the bottom of the form are "Submit" and "Reset" buttons. The footer includes a navigation bar with links for "NTP", "Interface", "System", "Relay", "Security", and "Status & Log", along with copyright information and a "Contact us" link.

Figure 3-32: Statistics FTP Screen

The NTP Status screen (Figure 3-33) provides statistics and a graphical representation of various NTP statistics relevant to the NetClock's function. This includes whether the NetClock is time synchronized, its stratum level, the location of its selected reference, its delay, offset, and jitter, and statuses for defined timing references on the network.

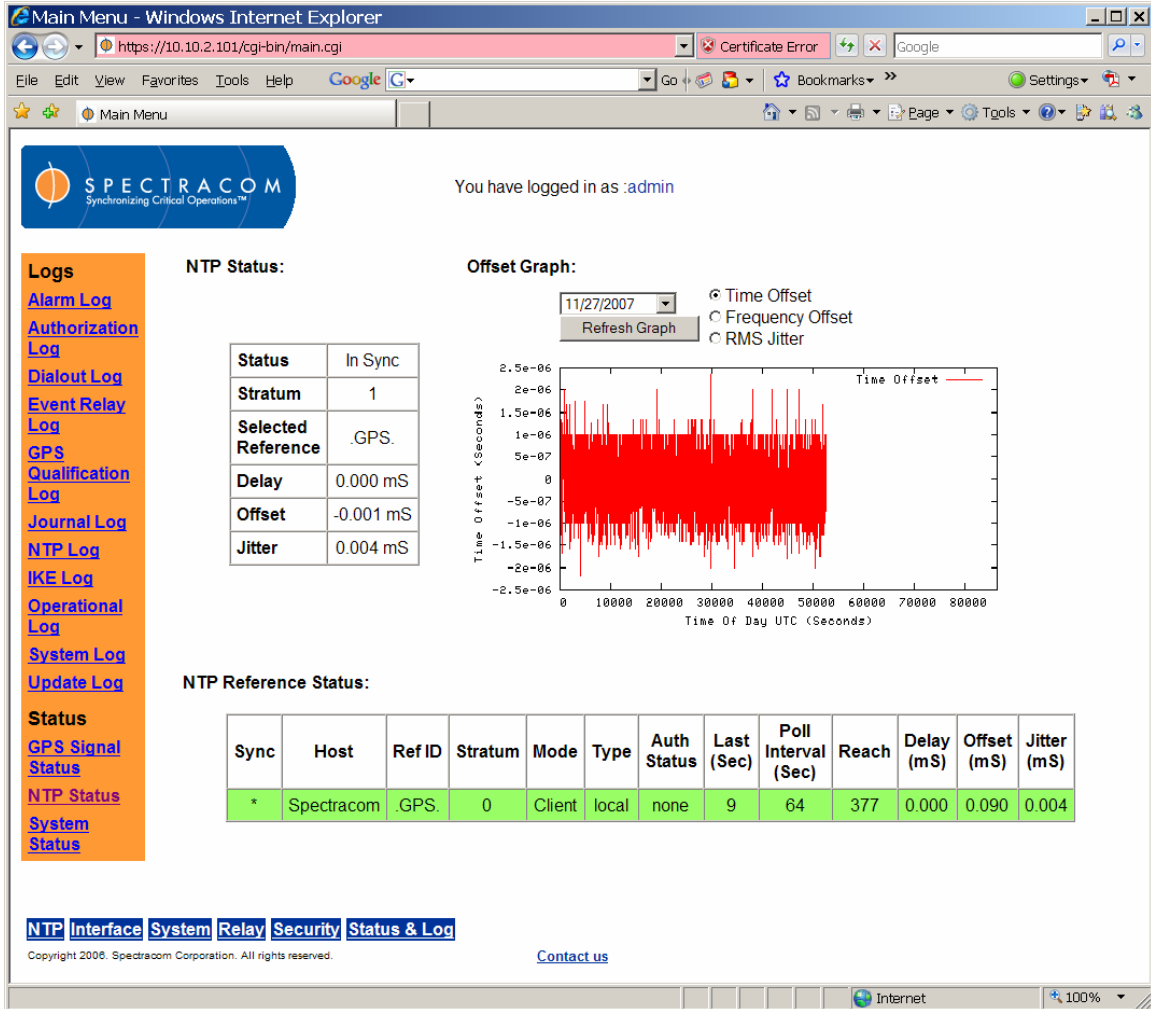


Figure 3-33: NTP Status Screen

NOTE: The NTP Reference Status lines bear different colors for different codes. Red is a reject (the peer is discarded as unreachable). Yellow is an outlier (the peer is discarded by the clustering algorithm). Green is a candidate (the peer is a survivor and a candidate for the combining) or a syspeer/ppspeer (the peer has been declared the system peer and lends its variables to the system variables).

3.4.2 NTP Support

Spectracom cannot provide technical assistance for configuring and installing NTP on Unix-based applications. Please refer to 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, Windows 2000, and Windows XP time synchronization. Refer to the Spectracom Web page, www.spectracomcorp.com, for more information, or contact Spectracom Technical Support by phone at **US +1.585.321.5800**.

3.4.3 Configuring the Interface

The Interface menu (Figure 3-34) groups the NetClock's Interface configuration functions. From this menu, the user may access the Interface Serial Port and Remote Port screens. The user may also use this menu to set the interface configuration to the factory default settings.

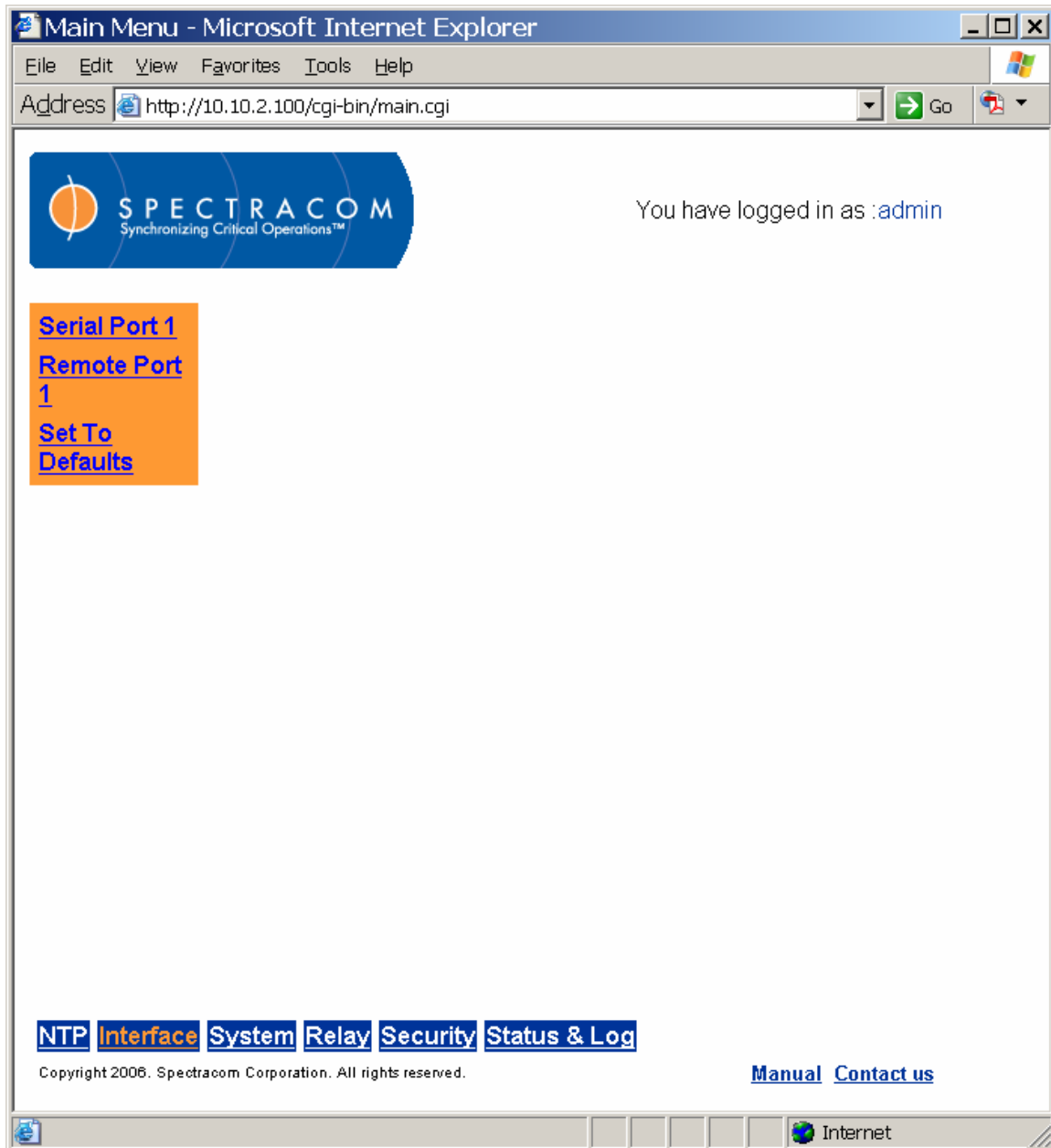


Figure 3-34: Interface Menu

The NetClock has one serial port and one remote output port that support independent output of date/time stamps from the NetClock. From the respective screens for the serial and remote ports (Figure 3-35 and Figure 3-36), the user may define the baud rate and the Data Format for each port. The system clock may also be selected if a local clock (set for a local time zone) has been defined. Serial ports include the “Request Char” feature, which allows the user to choose between multicast (broadcasting once per second on the second through the port) and a user-defined character. When the character of the user’s choice is entered, the NetClock will broadcast through the port only when that character is received by the unit.



Figure 3-35: Interface Serial Port 1 Screen

The baud rate is the speed at which the port will output values. This speed must be selected from the dropdown box. The default is 9600 baud.

The Data Format is the format in which the date and time stamps are sent from the NetClock. Several Data Formats are supported. The default is Format 0.

NOTE: Data Format 2 is always a Coordinated Universal Time (UTC) output. It cannot have Time Zone Offset or Daylight Saving Time (DST) rule enabled. Conversion to local time is accomplished by the device receiving the data. An error will be generated if a Time Zone Offset or DST rule is applied to Data Format 2. NTP never outputs local time.



Figure 3-36: Interface Remote Port 1 Screen

Clicking the link to create and edit local systems clocks will display the Local System Clock screen. Refer to the System configuration screens in this manual for information on setting and editing local system clocks.

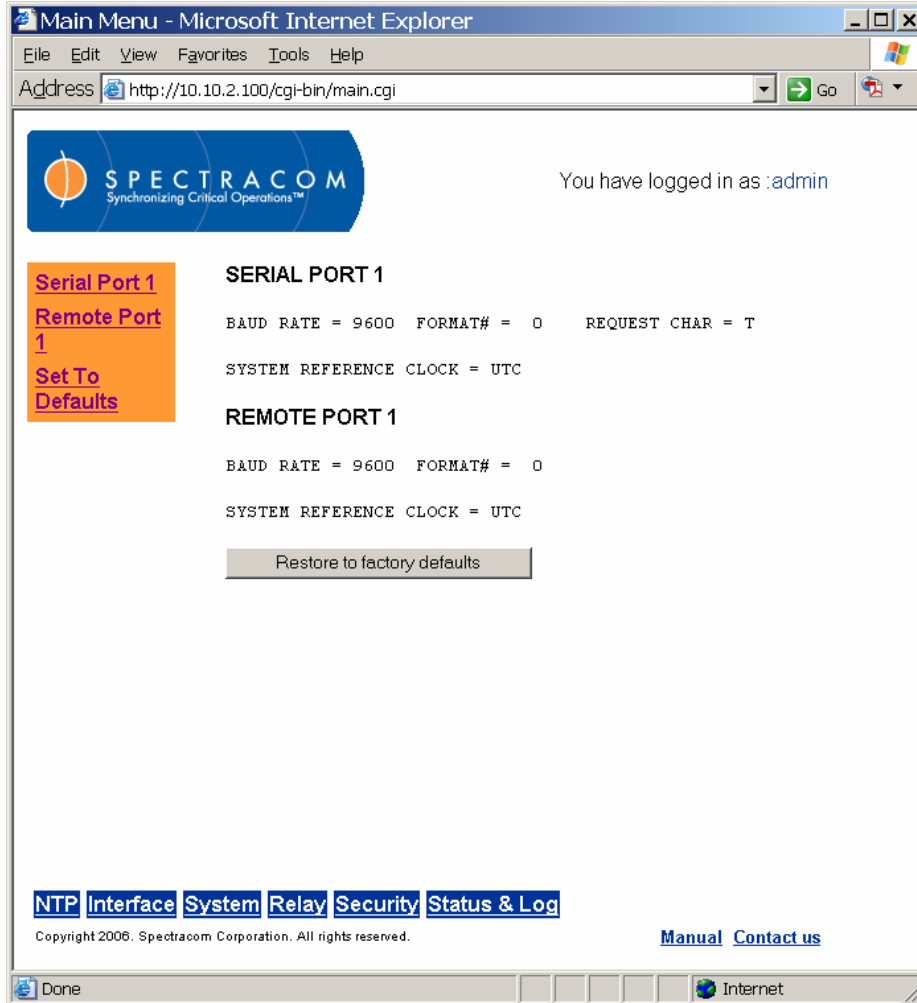


Figure 3-37: Interface Set to Defaults Screen

From the Interface Set to Defaults screen (Figure 3-37), the user may click the “Restore to factory defaults” button to set the Interface values (and the Interface values ONLY) to the factory settings.

3.4.4 Sysplex Timing

The NetClock may be used as an external time source (ETS) to synchronize an IBM Sysplex Timer. This is achieved by configuring Serial Port 1 (refer to *Configuring the Interface*) on the NetClock to the following settings (Figure 3-38):

Baud Rate: 9600
Data Format: 02
Request Char: User-defined, 'T'
System Clock: UTC

Main Menu - Microsoft Internet Explorer
Address <https://10.10.50.20/cgi-bin/main.cgi> Go

SPECTRACOM
Synchronizing Critical Operations™

You have logged in as :admin

Serial Port 1
[Remote Port 1](#)
[IRIG](#)
[Front Panel Display](#)
[Frequency Output](#)
[Set To Defaults](#)

BAUD RATE: 9600
DATA FORMAT: 02
REQUEST CHAR: Multicast User defined T
SYSTEM CLOCK: UTC Click [here](#) to edit or create local system clocks.

Submit Reset

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Internet

Figure 3-38: Configuring Serial Port 1 for Sysplex Timing

The Sysplex Timer must be configured to use Protocol 2 (NetClock/2) and connected to the NetClock Serial Comm 1 port via a 9-pin serial cable (not included). Older Sysplex Timers (9037-001) may connect to an ETS through the Sysplex Timer's console port, while later model Sysplex Timers (9037-002) feature a dedicated ETS port.

3.4.5 Configuring the System: SNMP

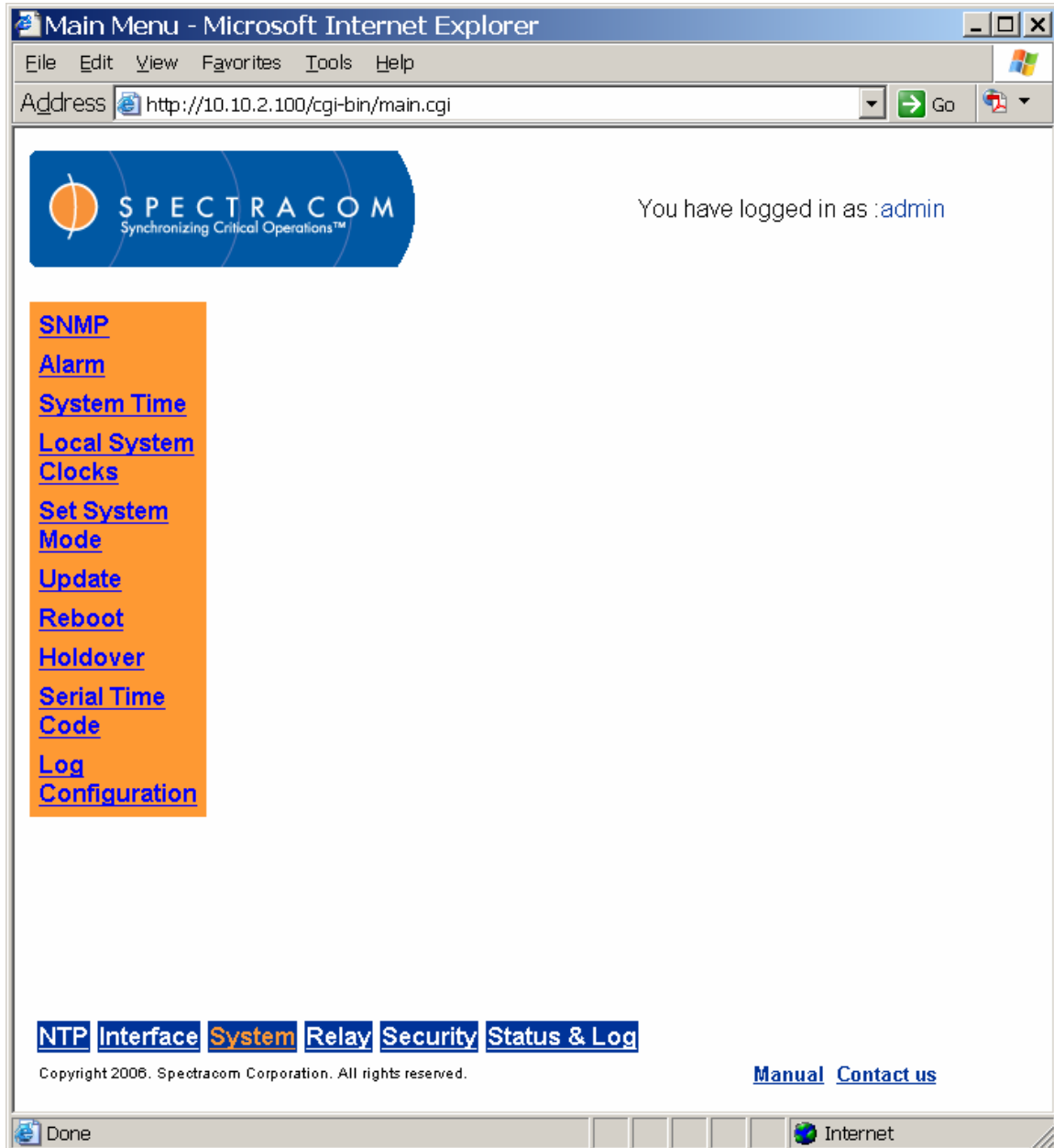


Figure 3-39: System Menu

The System menu groups the NetClock's various system configuration functions (Figure 3-39). From this menu, the user may access screens for SNMP, Alarms, GPS, System Time, Local

System Clocks, System Mode, Modem Configuration (if the NetClock includes the modem option), Reboot, Holdover, and Log Configuration.

NOTE: Refer to *Options* for modem configuration and related screens. If your NetClock does not have the modem option (which is activated at the factory), the modem menu links will not appear on the System screen. If you purchase the Modem option after receipt of your NetClock system, Spectracom will provide you with a product key for modem activation.

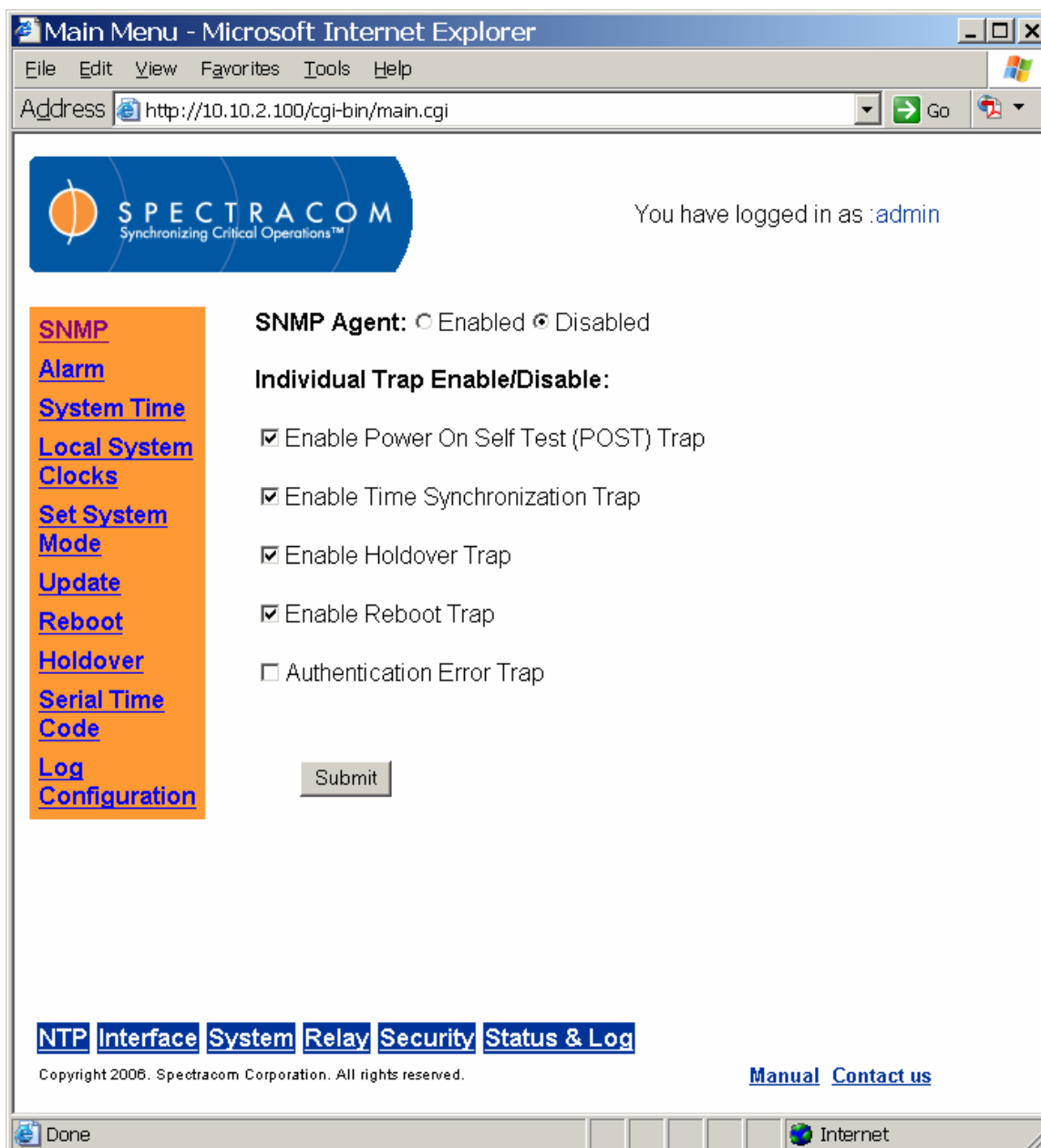


Figure 3-40: System SNMP Screen

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 Management Information Base (MIB).

Click the radio buttons at the top of the System SNMP screen (Figure 3-40) to enable or disable SNMP. You may also check the boxes to enable or disable individual traps. (Traps are asynchronous status messages sent from NetClock to the locations specified in the SNMP security screens.)

3.4.5.1 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.

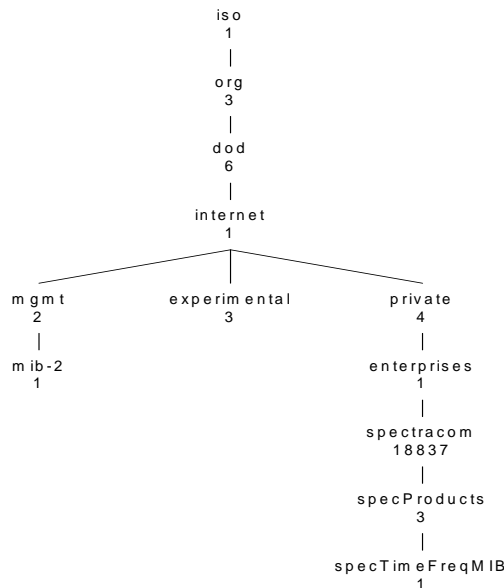


Figure 3-41: Spectracom's MIB

3.4.5.2 SNMP Support

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

To obtain the MIB file via FTP, using your FTP program, log in as an administrator and change the file transfer mode to "binary." The Spectracom MIB files are located in the /MIBS directory and include global, time-frequency, and NTPv4 files. There is a Global (generic) MIB file and a NetClock-specific MIB file called "Time and Frequency." FTP the files to the 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 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 these requirements.

3.4.6 Configuring Alarms

An alarm is asserted when predefined error conditions exist AND the associated alarm has been enabled.

Through the System Alarm screen (Figure 3-42), the user may define what conditions constitute Major and Minor alarm conditions. These are the only user-defined Netclock Alarms. Clicking the check box to the left of a particular user-defined alarm will enable that alarm condition. Each alarm condition may be set to exist for a specified duration before activating the alarm. This is done by filling in the Timeout fields directly beneath the alarm condition.

Main Menu - Microsoft Internet Explorer
 Address http://10.10.2.100/cgi-bin/main.cgi

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as :admin

SNMP Alarm

Unable to read current alarm configuration.

Major Alarm Condition

Tracking fewer than 1 Satellites

Timeout: 0 Days 0 Hours 0 Minutes 0 Seconds

Minor Alarm Condition

Tracking fewer than 1 Satellites

Timeout: 0 Days 0 Hours 0 Minutes 0 Seconds

Submit Reset

NTP Interface System Relay Security Status & Log

Copyright 2006. Spectracom Corporation. All rights reserved. Manual Contact us

Figure 3-42: System Alarm Screen

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

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

Time Sync Alarm: The period of time allotted for operation without tracking sufficient qualified satellites has expired. The factory default period is 2 hours. This is a Major alarm.

Power Failure: The NetClock has lost power. This is both a Major and a Minor alarm.

3.4.7 Configuring System Time and Local Clocks

The System Time screen (Figure 3-43) allows the user to set the system time manually for test purposes or if there is no external time reference available. Setting the system time when the NetClock is connected to an external time reference will result in the external reference overriding the manually set time. The user may also view (or change) the number of leap seconds difference between UTC and GPS time.

Main Menu - Microsoft Internet Explorer
 Address: <https://10.10.2.100/cgi-bin/main.cgi>

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as: **admin**

SNMP
[Alarm](#)
[System Time](#)
[Local System Clocks](#)
[Update](#)
[Reboot](#)
[Holdover](#)
[Serial Time Code](#)
[Log](#)
[Configuration](#)

If the NetClock is currently receiving valid time from a reference source (i.e. GPS, IRIG, Serial Time Code, etc.), any date/time information configured using this page will be overwritten.

Note: Date/time information configured using this page is considered to be UTC.

System Time:

Set System Time using user-specified UTC time below

Date: 14 Sep 2006
 Time: 13 : 41 : 22

Leap Seconds:

Number of leap seconds between UTC and GPS time: 14

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-43: System Time Screen

Choosing Create/New from the Local System Clocks screen (Figure 3-44) allows the user to define up to five local times (times other than UTC or GPS) to display using the NetClock.

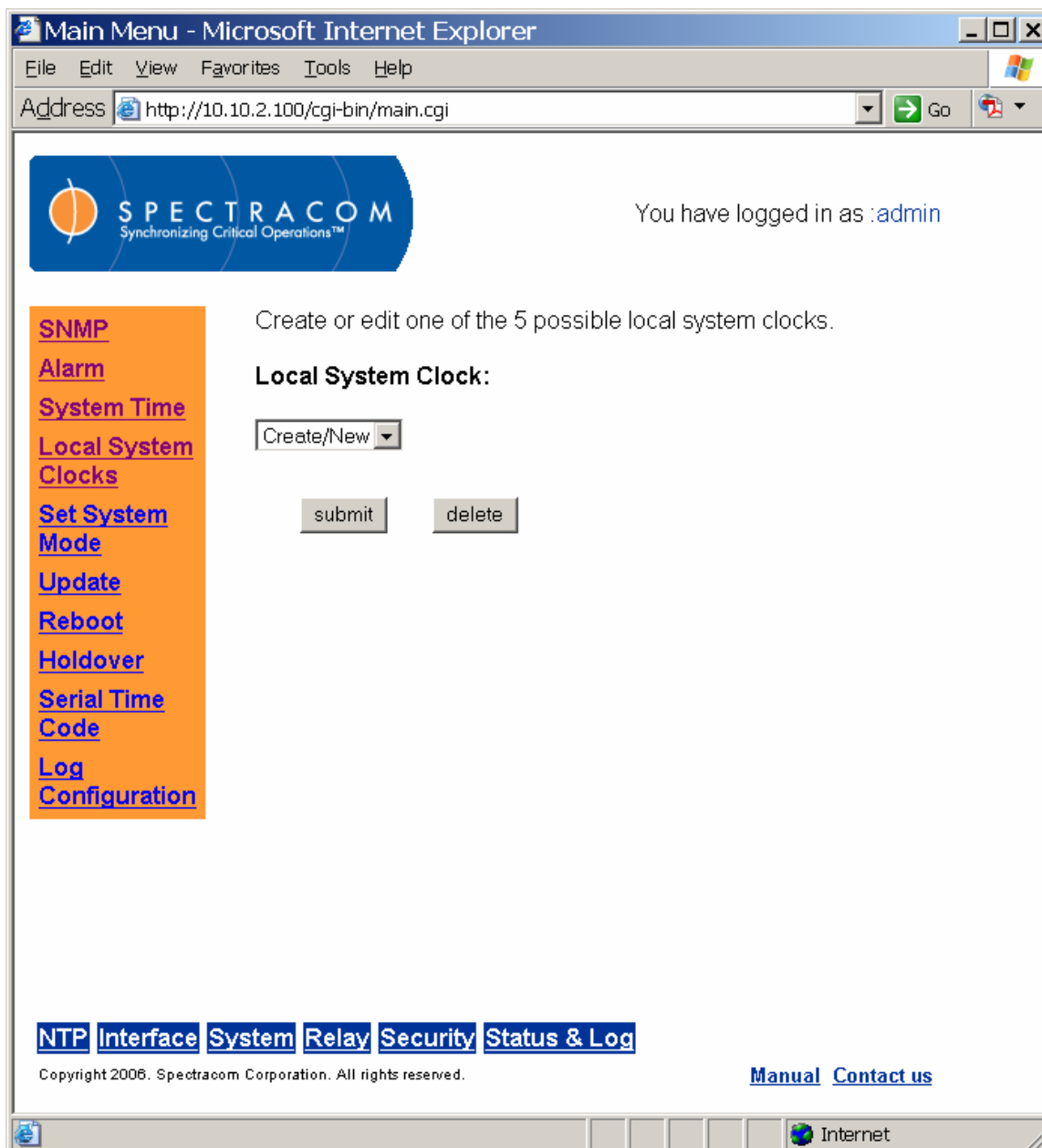


Figure 3-44: Local System Clocks Screen (1 of 2)

You can define up to five local clocks or time zones to be used with any of the remote ports, serial ports, and event timers.

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 Daylight Saving Time (DST) conditions. To configure a local clock, perform the following steps.

NOTE: The local clock is not available from the front panel Ethernet output per the NTP specifications. NTP ALWAYS provides UTC time. Each client on the network must handle corrections for local time.

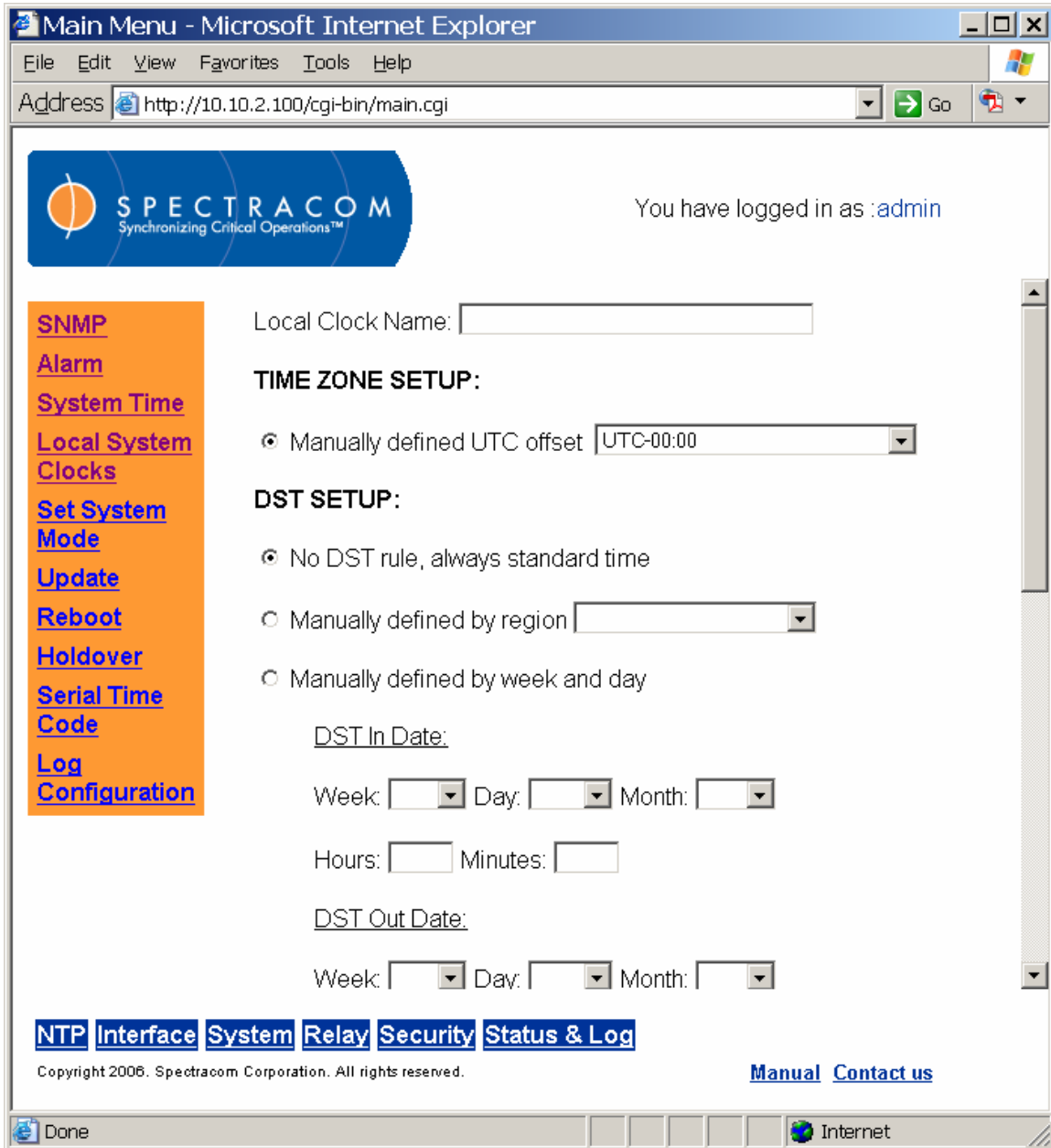


Figure 3-45: Local System Clock Screen (2 of 2)

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

Under the TIME ZONE SETUP, you will see one choice:

- Manually defined UTC offset

Manually Defined by UTC Offset

A dropdown box is provided (with definitions as appropriate) that permits the user to select a specific number of hours added or subtracted from UTC for the desired time zone.

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

DST SETUP

Daylight Saving Time (DST) observance varies with locality and application. Choose the configuration that reflects your location and needs. Under the DST SETUP, you will see four choices:

- 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

When this option is selected, the NetClock will not observe DST time changes.

Manually Defined by Region

From this dropdown box, the user may select commonly defined geographic regions that share DST rules. There may be exceptions based on your location. The options include the following:

- Europe
- USA (thru 2006)
- USA (post 2006)
- Australia-1
- Australia-2

Select **Europe** if your location complies with the European DST Rule. This rule differs from all other rules because the DST changes occur based on UTC time, not local time. (All time zones in Europe change for DST at precisely the same time relative to UTC, rather than offset by local time zone.)

Select **USA (thru 2006)** if your location complies with the USA DST Rule and it is not yet the year 2007. The USA DST Rule changes in 2007.

NOTE: If you set your DST rule in 2006, you must change it manually on January 1, 2007.

Select **USA (post 2006)** if your location complies with the USA DST Rule and it is the year 2007 or later.

Select **Australia-1** if your location complies with the Australia-1 DST Rule (*Australian Capital Territory, New South Wales, South Australia, Tasmania, Victoria*).

Select **Australia-2** if your location complies with the Australia-2 DST Rule (*Western Australia*).

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. *Manual definitions are ALWAYS based on local time, not UTC.*

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. *Manual definitions are ALWAYS based on local time, not UTC.*

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 Saving Time are available here. There is no DST observed. This is the default.

Manually specify a pre-defined DST rule.

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:

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

Click on the "Manually Defined UTC Offset" button.

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

Select the 'No DST rule' radio button.

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

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

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

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

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

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

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

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

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

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

Select the desired Clock Name.

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

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

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

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

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

The unit will allow you to define different Time Zone and DST rules for different Interfaces. 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>.

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

3.4.8 Activating System Options and Rolling Back Updates

From the System Update screen (Figure 3-46), the user may activate system options and "rollback" software updates, effectively returning the NetClock to its previous software version and configuration settings.

To activate system modem or security options, click the "Activate Option" box, choose the option you wish to activate, and enter the activation key provided by Spectracom before clicking "Submit."

To return the NetClock to its previous setup configuration ("Configuration") or software version ("Firmware"), click the appropriate selections and click "Submit."

NOTE: The NetClock must be rebooted (Figure 3-47) for the active option and configuration/firmware rollback(s) to take effect.

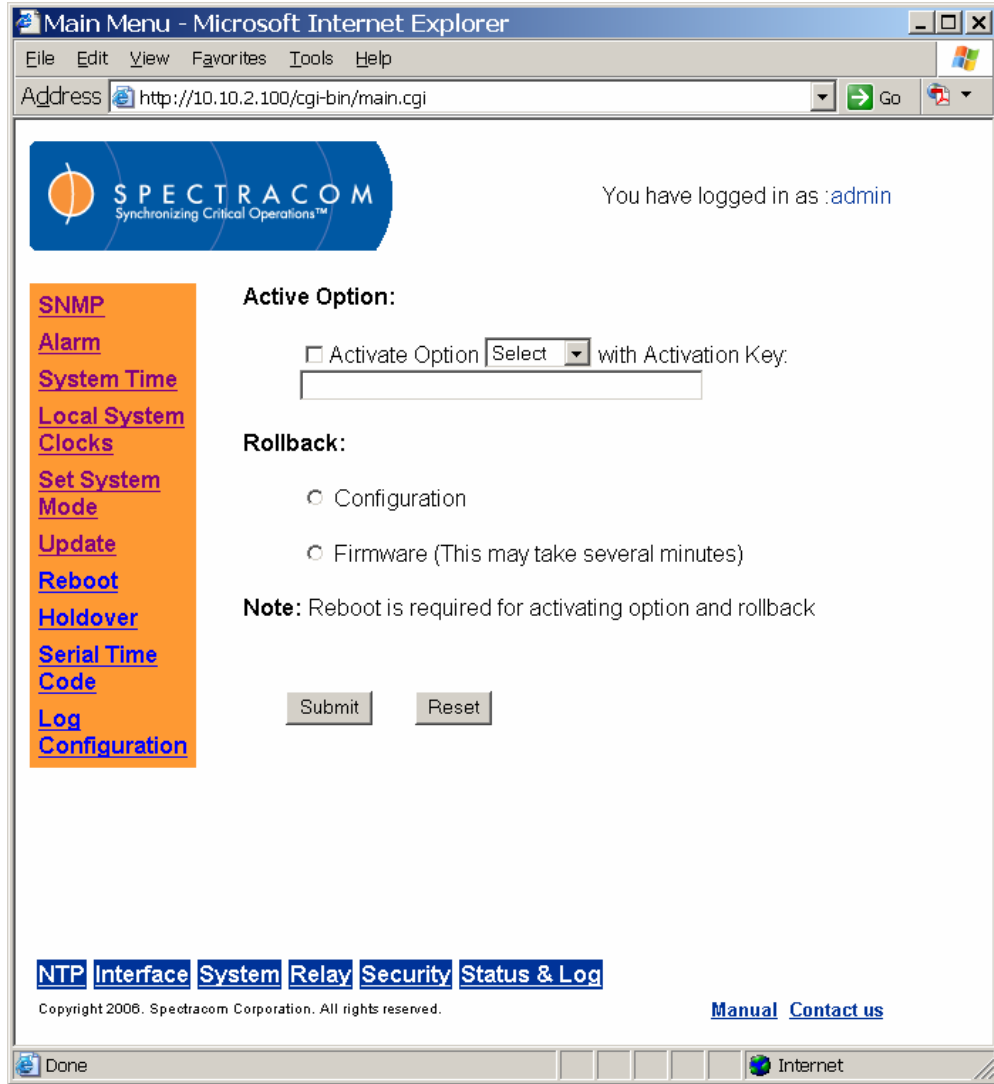


Figure 3-46: System Update Screen

3.4.9 Rebooting the System

The system can be rebooted from the System Reboot screen (Figure 3-47). Simply click the “Reboot Now” button and wait for the NetClock to reboot.

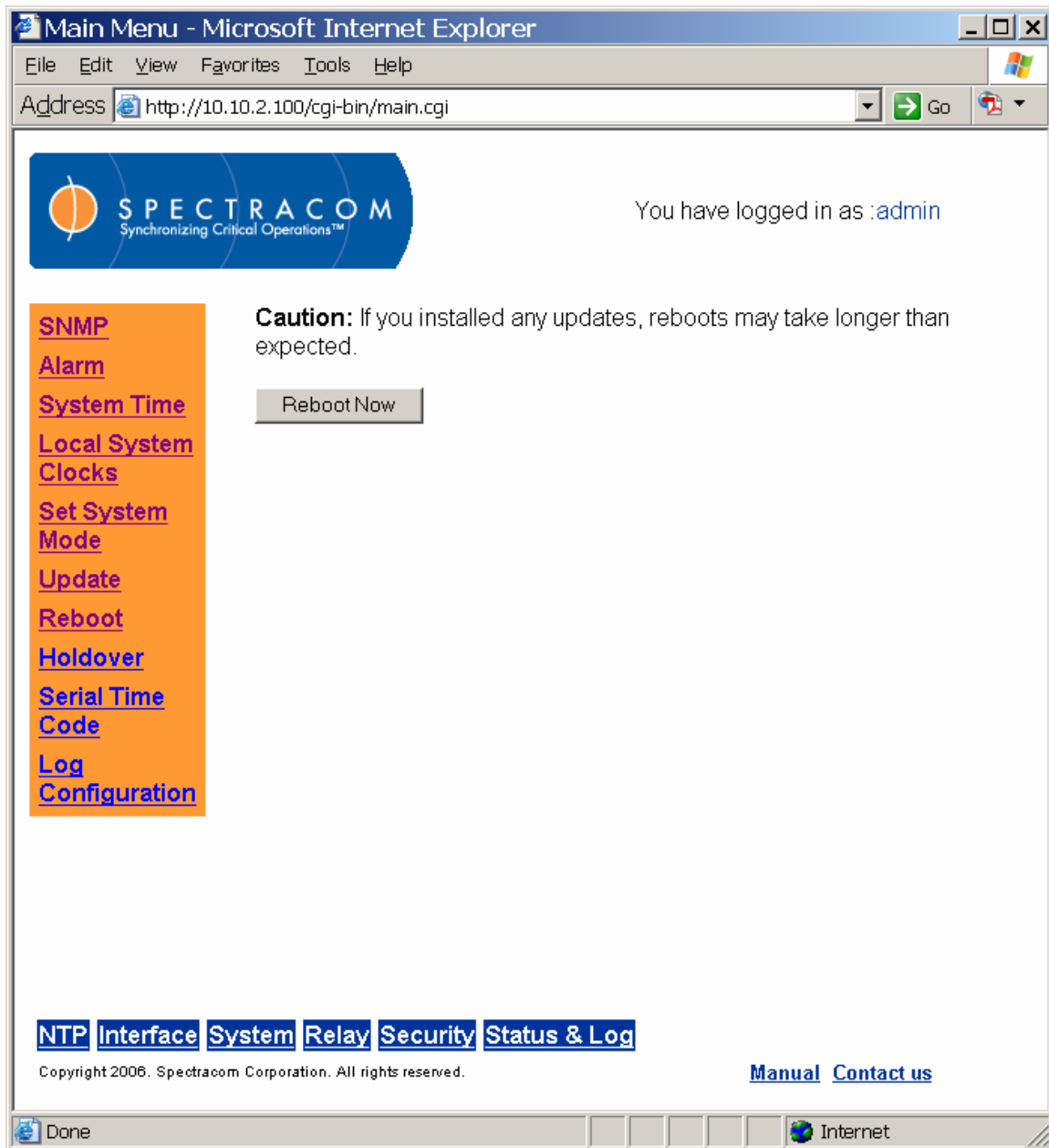


Figure 3-47: System Reboot Screen

3.4.10 Configuring System Holdover

The user may set the system holdover from the System Holdover screen (Figure 3-48). The time interval between the loss of the primary external reference and the moment that the NetClock declares loss of time synchronization is known as *holdover*. While the unit is in 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 synchronization and the availability of the time outputs is not immediately lost when the reference is no longer available.

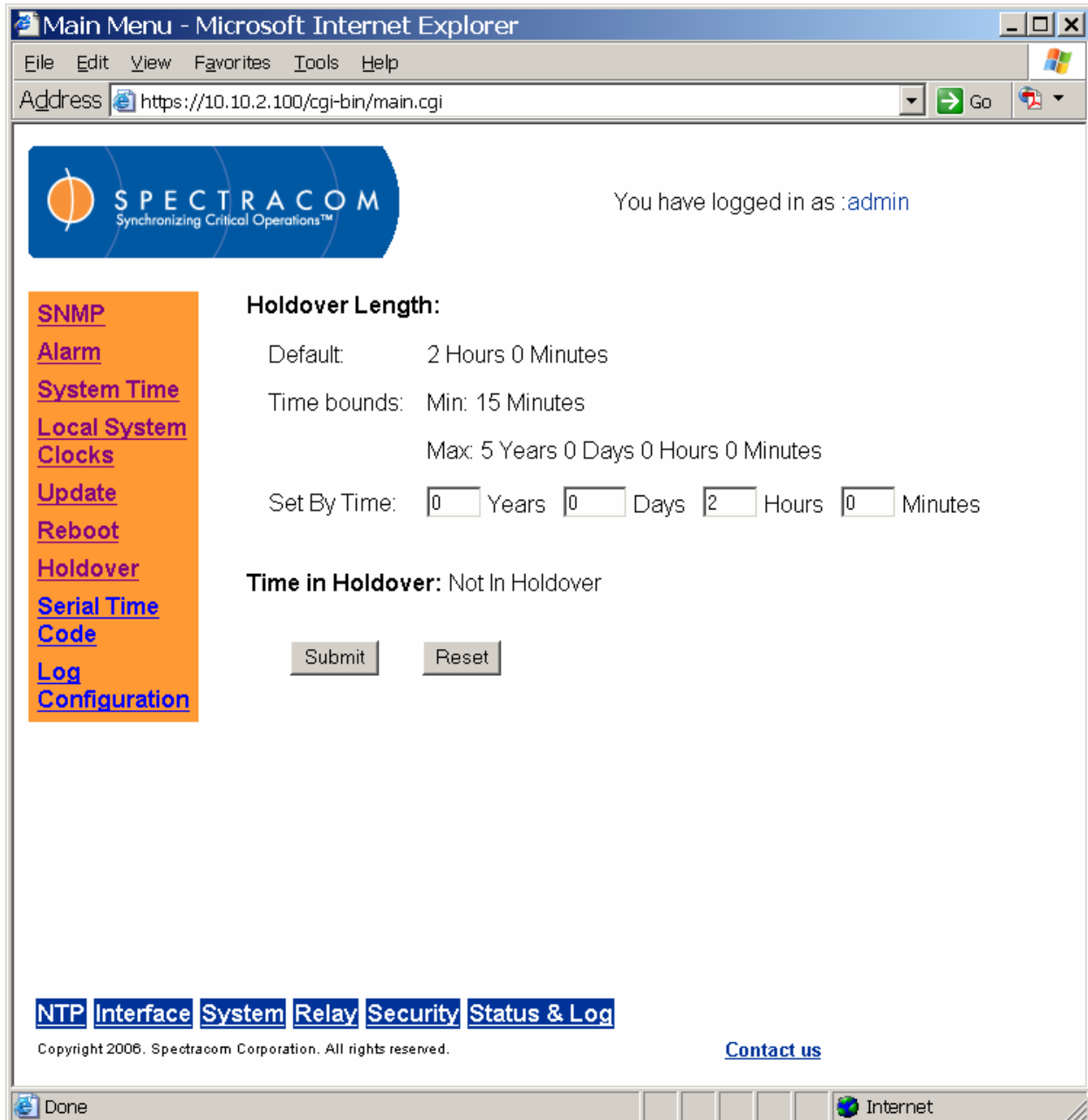


Figure 3-48: System Holdover Screen

The NetClock has a user configurable variable holdover period so that it can be adjusted for personal requirements and desires. A user can change the length of time that a unit waits in the holdover mode before loss of time sync. The holdover can be defined by a specific number of hours to wait, such as 4 hours and 30 minutes.

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

Table 3-3: Estimated TCXO Oscillator Error Rates

NOTE: The TCXO Error rate is a worst-case estimate and not typically this value. The nominal value assumed has been 1 millisecond / hour yielding 2 hours holdover times. The TCXO does not estimate error for holdover. Typically, the error rates for a disciplined oscillator at 25 degrees Celsius will be lower than these values.

Limits on the minimum and maximum length of allowable holdover have been placed on the oscillator as shown below in Table 3-4.

Oscillator	Minimum Length	Maximum Length
TCXO	15 minutes	24 hours

Table 3-4: 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, the NetClock will notify the user that this setting is outside its allowable parameters.

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

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

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

3.4.11 Serial Time Code Setup

From the Serial Time Code Setup screen (Figure 3-49), the user must configure the network input to be received by the Model 9288. Obtain the source output settings from your network administrator and enter the baud rate and Data Format. (The year must be entered for Data Format 0.) Click the “Submit” button when all values have been entered.

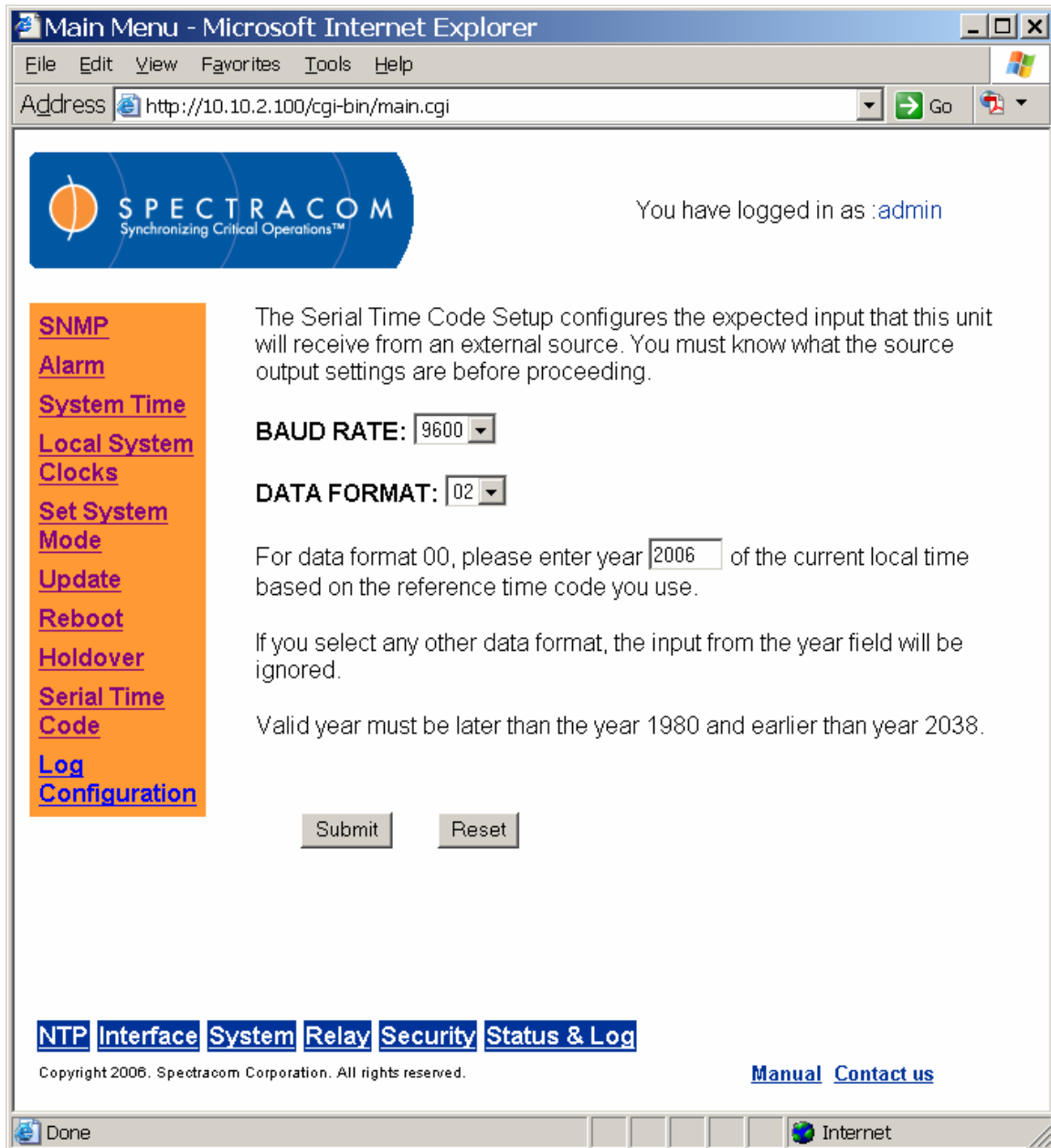


Figure 3-49: Serial Time Code Setup Screen

NOTE: When the year is updated, the NTP server must be restarted from the NTP Web UI page (or the NetClock rebooted) for the new year value to take effect.

3.4.12 Configuring System Logs

From the System Log Configuration screen (Figure 3-50), the user may configure remote Syslog servers with which the NetClock will communicate. Facilities and severities are defined by the Syslog server and must be set up in the NetClock to match. The IP addresses and host names of the Syslog servers are entered on the bottom portion of the screen.

Syslog Configuration:

Log Name	Enable Local Log	Facility	Severity	Local File Name
system	<input checked="" type="checkbox"/>	local7	emerg	/log/spectracom/system.log
events	<input checked="" type="checkbox"/>	local7	alert	/log/spectracom/events.log
alarms	<input checked="" type="checkbox"/>	local7	crit	/log/spectracom/alarms.log
operational	<input checked="" type="checkbox"/>	local7	warn	/log/spectracom/operational.log
journal	<input checked="" type="checkbox"/>	local7	debug	/log/spectracom/journal.log
update	<input checked="" type="checkbox"/>	local6	emerg	/log/spectracom/update.log
auth	<input checked="" type="checkbox"/>	local6	alert	/log/auth.log
ntp	<input checked="" type="checkbox"/>	local6	crit	/log/ntp.log

Remote Syslog Servers:

#	IPv4/Hostname
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006, Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-50: System Log Configuration Screen

NOTE: Any remote syslog server that is entered to receive log messages must be properly configured to accept incoming syslog messages.

3.4.13 Configuring and Testing Relays

The Relay menu groups the NetClock's relay functions (Figure 3-51). From this menu, the user may access screens configure, test, and reset the relay outputs and event timers.

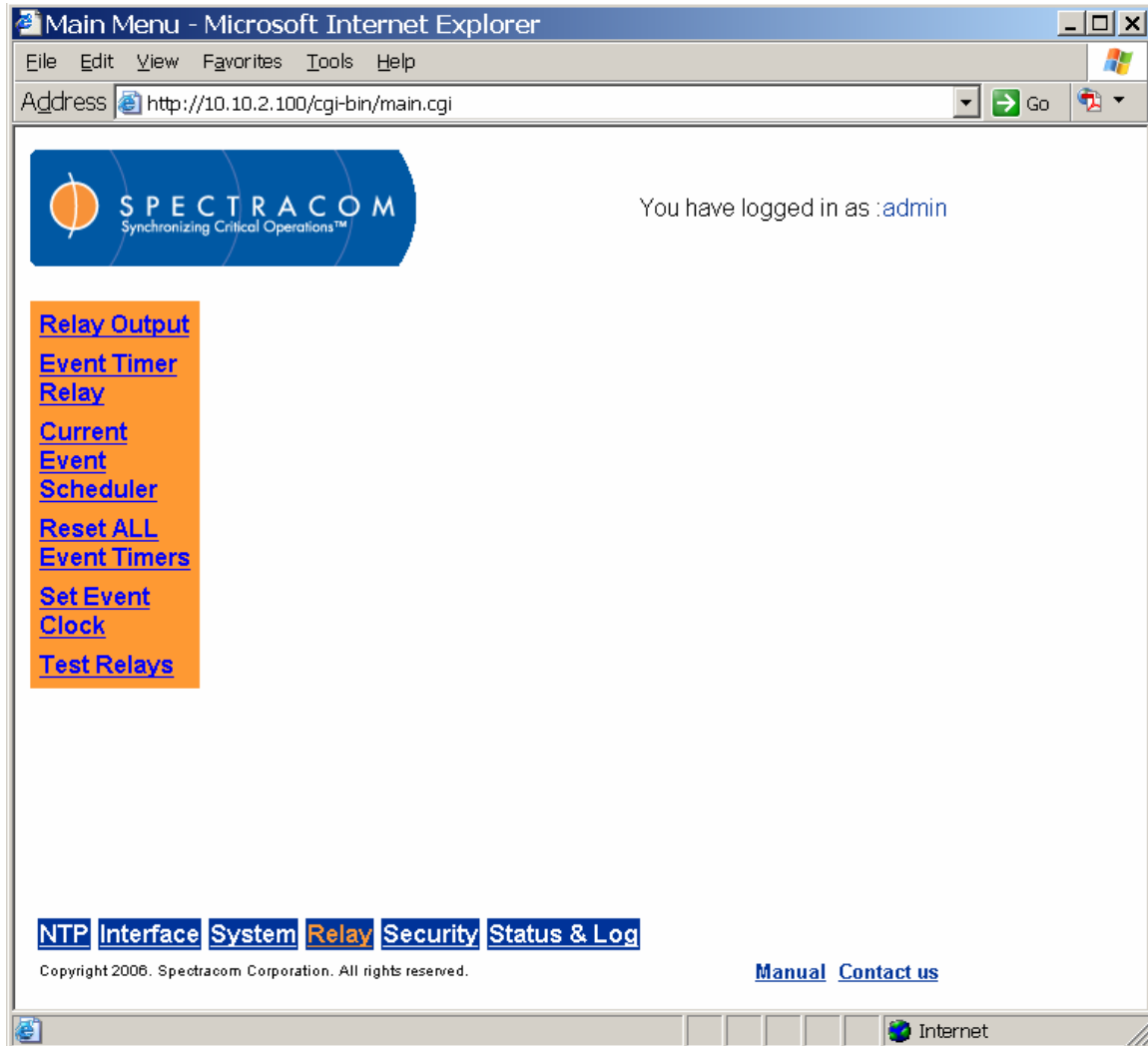


Figure 3-51: Relay Menu

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.

To assign a function to a relay, click the radio button that lines up with both the function and the relay. 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.

NOTE: 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.”

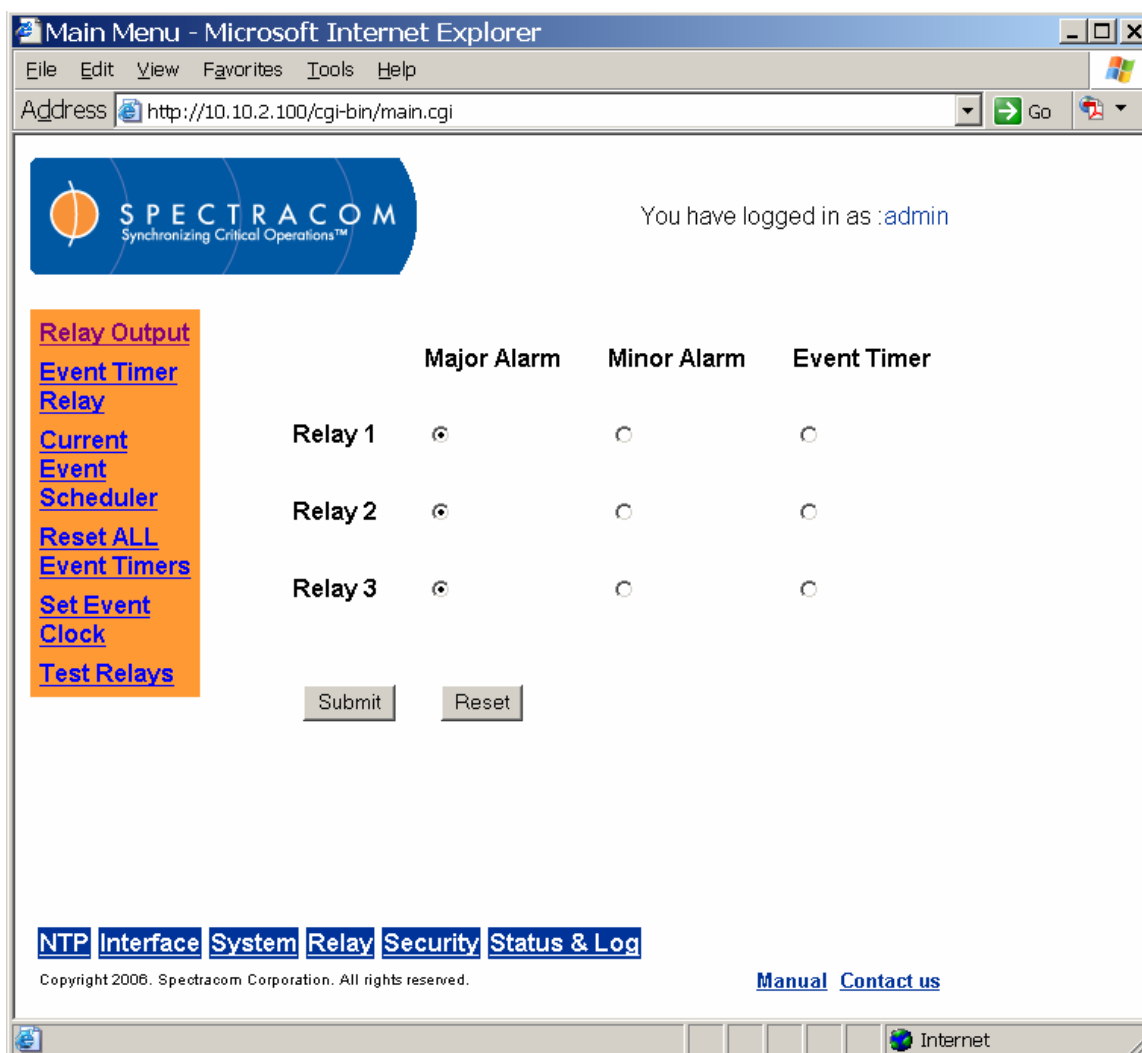


Figure 3-52: Relay Output Screen

The Event Timer Relay screen (Figure 3-53) and the Relay Current Event Scheduler screen (Figure 3-55) allow for the configuration of 128 events that can turn on or off any one of the event timer relays. 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.

If any events are already configured, they will be displayed by event number. 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.

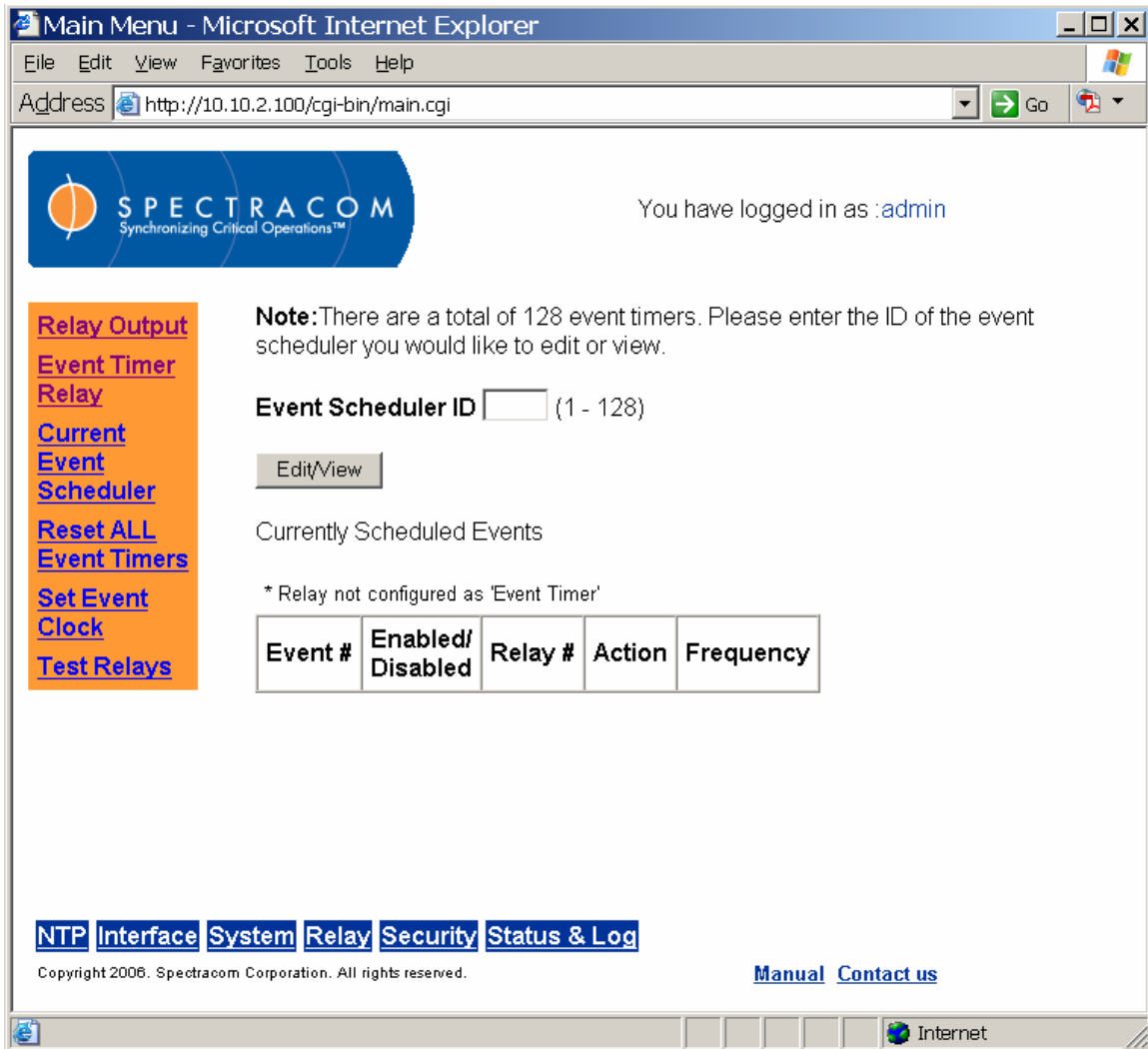


Figure 3-53: Event Timer Relay Screen

Main Menu - Microsoft Internet Explorer
 Address: http://10.10.2.100/cgi-bin/main.cgi

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as :admin

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
 Daily
 Weekly
 Monthly
 Yearly

Minute Second Millisecond
 Hour Minute Second Millisecond
 MON Day Hour Minute Second Millisecond
 1 Day Hour Minute Second Milliseconds
 Jan Month 1 Day 0 Hour 0 Minute 0 Second

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Manual](#) [Contact us](#)

Figure 3-54: Edit/View Event Timers

Choose a Time Zone

From the left menu, select "Set Event Clock." Choose an already defined Clock (Time Zone) or define a new one

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.

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

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

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

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

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

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

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

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

Yearly: The event will happen every year at the month, day of month, hour, minute, second, and millisecond specified (within 100 milliseconds). If the month and day of month are programmed for February 29th (this can only be done while currently in a leap year), the event will happen on March 1st on non-leap years and February 29th on leap years.

NOTE: The Current Event Schedule (Figure 3-55) is a list of ENABLE events only. The events are ordered by next occurrence.

SPECTRACOM
Synchronizing Critical Operations™

You have logged in as :admin

Next events as of 14:38:59 on Apr 24, 2006 'UTC' time

Current Relay States :

Relay #1 is OFF | Relay #2 is OFF | Relay #3 is OFF

* Relay not configured as 'Event Timer'

Event #	Relay #	Action	Next Event	Frequency
---------	---------	--------	------------	-----------

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Manual](#) [Contact us](#)

Figure 3-55: Relay Current Event Scheduler Screen

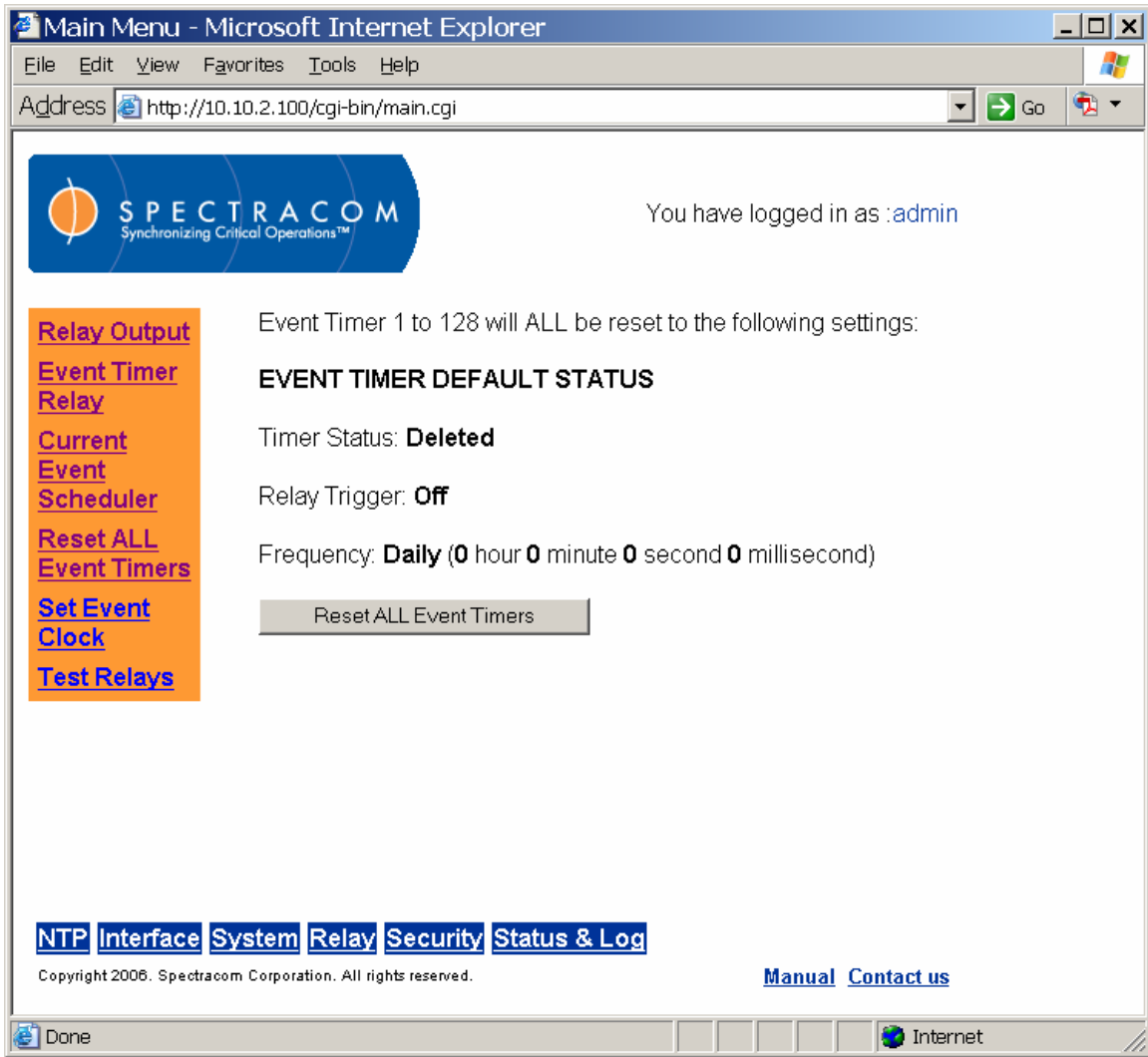


Figure 3-56: Relay Reset ALL Event Timers Screen

From the Reset ALL Event Timers screen (Figure 3-56), the user may clear any set event timers.

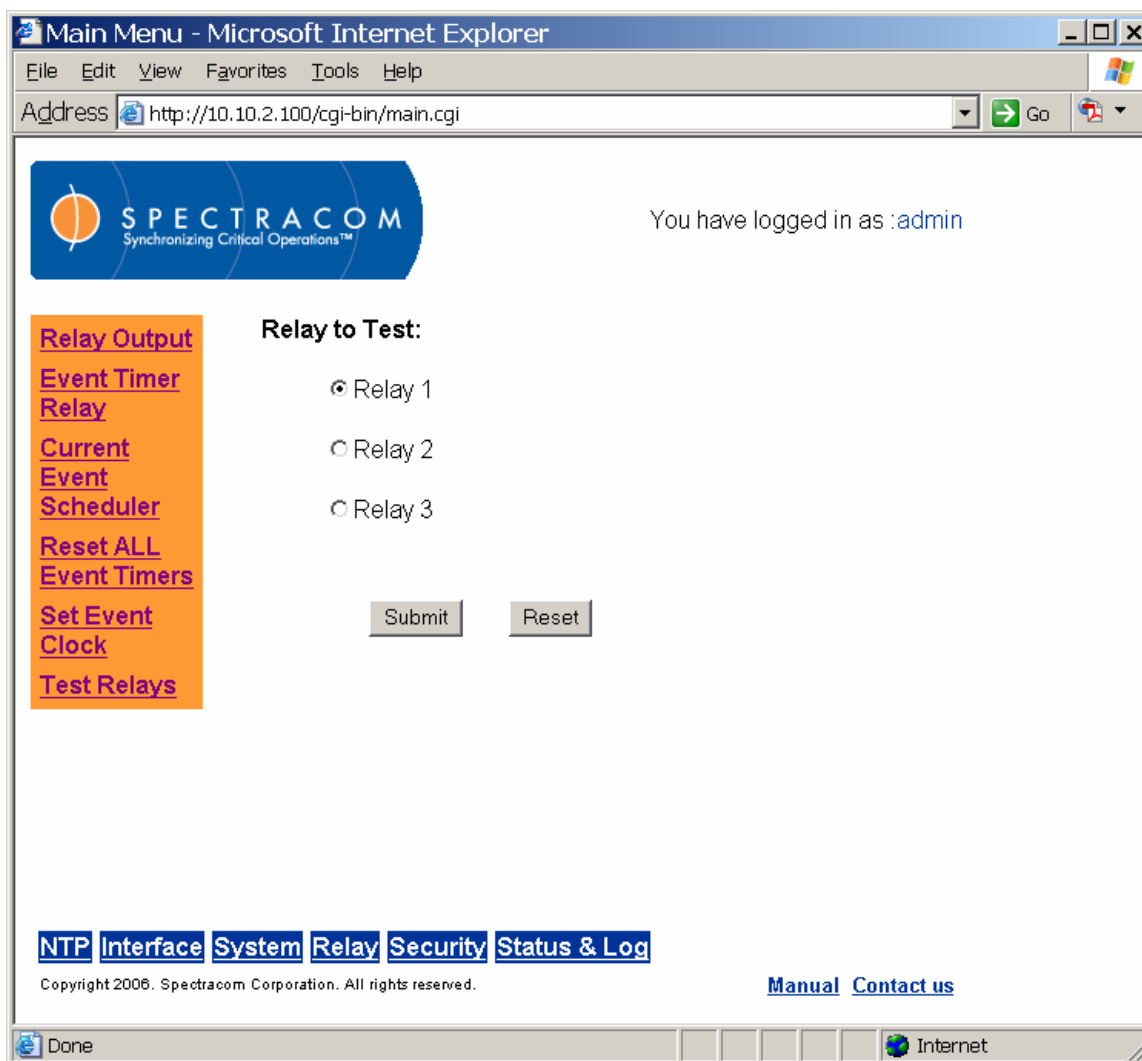


Figure 3-57: Test Relays Screen

Relay function can be tested from the Test Relays screen (Figure 3-57). Select one of the relays by clicking the radio button and test the selected relay by clicking Submit. If the relays are not connected to external devices, an audible clicking noise will emit from the NetClock. This noise indicates the relays are responding to the test. If external devices are connected to the relays, testing a relay should cause the connected device to actuate. When the test is complete, the Web UI will display the message, "Relay [number] test complete."

3.4.14 Configuring Network Security

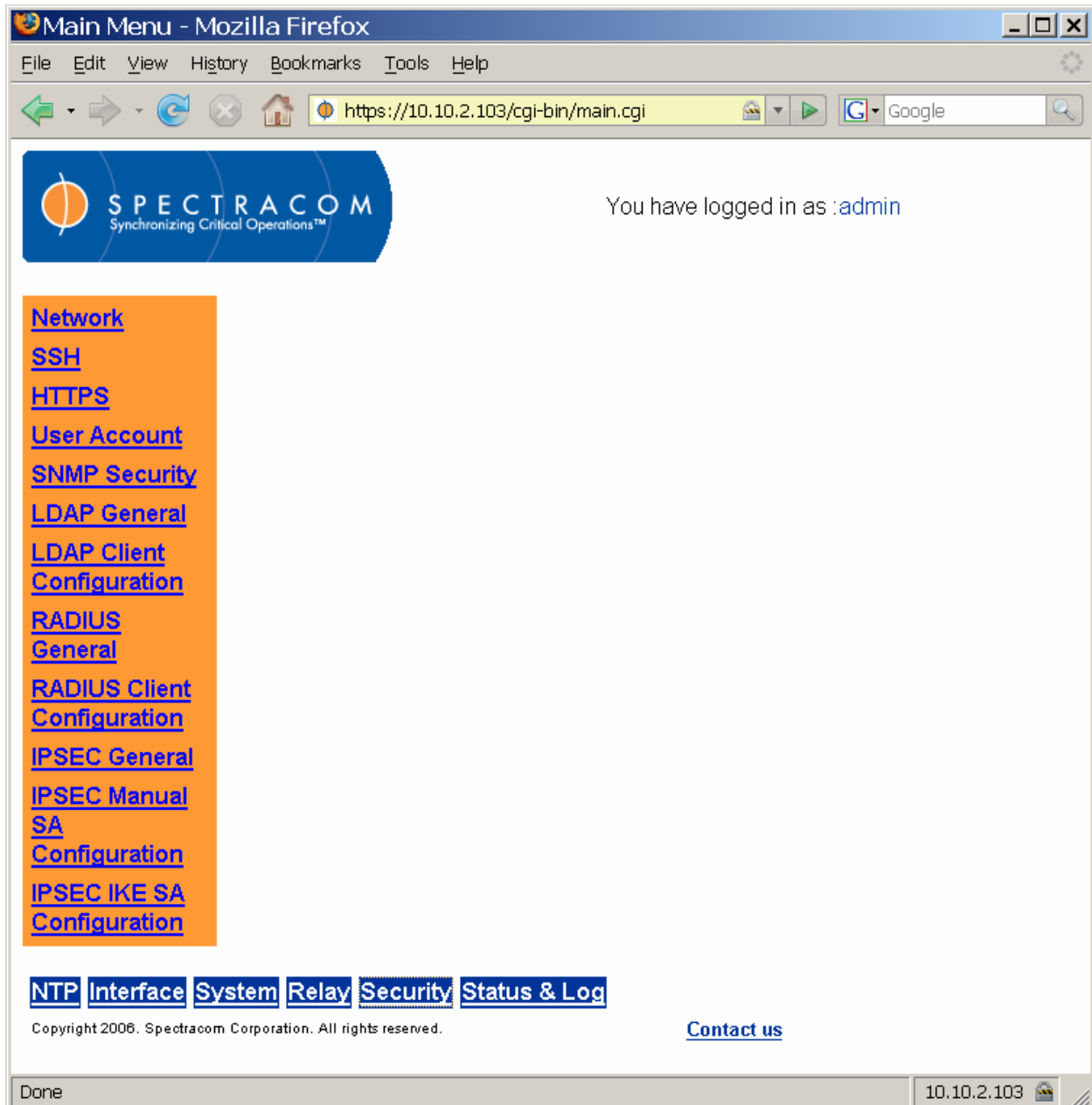


Figure 3-58: Security Menu

The Security menu groups the NetClock's security functions (Figure 3-58). From this menu, the user may access screens to configure network security, file transfers, user accounts, SNMP features, LDAP features, and RADIUS features.

Spectracom 9300 series products use OpenSSH and OpenSSL. OpenSSH is the Open Source version of the Secure Shell; which provides a set of server side tools allowing secure remote telnet like access and secure file transfer using remote copy like (RCP) and FTP like utilities.

OpenSSL is the Open Source version of Secure Sockets Library; which is used to provide the encryption libraries. Together OpenSSH and OpenSSL provide industrial strength encryption allowing for secure remote administration via command line, HTTPS web pages and secure file transfers.

The user is permitted to enable or disable HTTPS and SSH. 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.

Network
[SSH](#)
[HTTPS](#)
[User Account](#)
[SNMP Security](#)
[LDAP General](#)
[LDAP Client Configuration](#)
[RADIUS General](#)
[RADIUS Client Configuration](#)
[IPSEC General](#)
[IPSEC Manual SA Configuration](#)
[IPSEC IKE SA Configuration](#)

You have logged in as :admin

Hostname:

DNS Servers:

Primary DNS Server :

Secondary DNS Server :

IPv4 Configuration:

Enable DHCP

IP Address:

Subnet Mask:

Enable Gateway

Gateway Address:

IPv6 Configuration:

Enable DHCP6

IP Address	Prefix Length	Delete?
fe80::230:64ff:fe04:4aa3	64	<input type="checkbox"/>

Add a static IPv6 Address and Prefix Length:

IP Address:

Prefix Length:

Default Gateway:

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-59: Security Network Screen (1 of 2)

From the Security Network screen (Figure 3-59), the user may define the NetClock's host name. The DNS servers are set automatically if using DHCP and manually if not using DHCP. The same is true of the IP configuration. Certain information that must be entered on this screen should be obtained from your network administrator if it is not automatically filled in.



Figure 3-60: Security Network Screen (2 of 2)

3.4.14.1 Configuring SSH

SSH can be configured from the Security SSH screen (Figure 3-61). The tools supported are SSH – secure shell, SCP – secure copy, and SFTP – secure file transfer protocol. The NetClock implements the server components of SSH, SCP, and SFTP.

For more information on OpenSSH, refer to www.openSSH.org.

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

NOTE: Due to vulnerabilities in SSH1 protocol, it is not supported. Only SSH2 is supported.

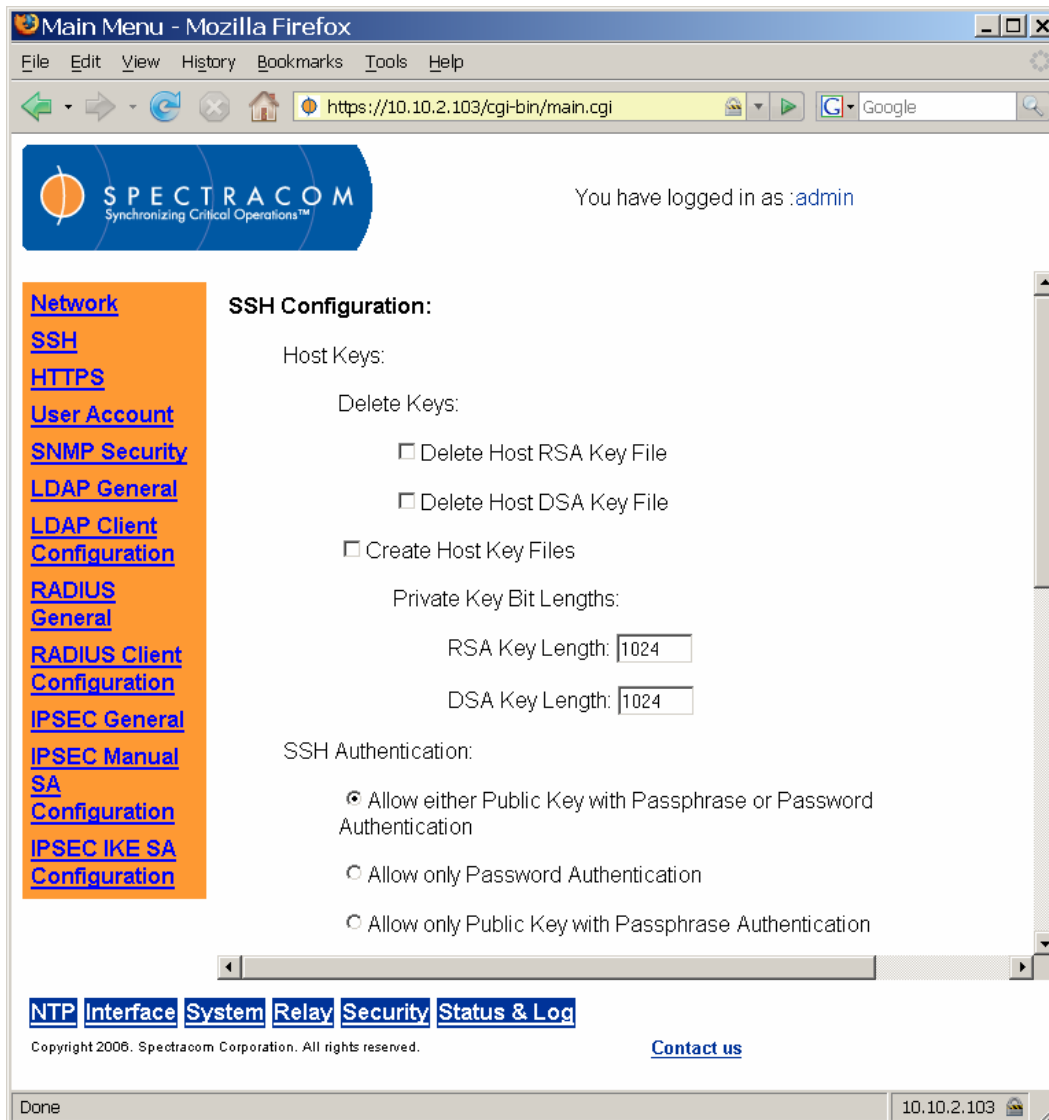


Figure 3-61: Security SSH Screen (1 of 2)

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.

If the user chooses to delete the RSA or DSA key, the SSH will function, but that form of server authentication will not be available. If the user chooses to delete both the RSA and 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, but it is often simpler to make these requests separately.



Figure 3-62: Security SSH Screen (2 of 2)

The user may create individual 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.

Spectracom secure products typically have their initial Host Keys created at the factory. The default key size for all key types is 1024. Host Key sizes can vary between 768 and 4096 bits. The recommended key size is 1024. Though many key sizes are supported, it is recommended that users select key sizes that are powers of 2 or divisible by 2. The most popular sizes are 768, 1024, and 2048. Large key sizes up to 4096 are supported, but may take ten minutes or more to generate.

Host Keys are generated in the background. Creating RSA and DSA keys, each with 1024 bits length, typically takes about 30 seconds. 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.

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 NetClock a copy of their public key. 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 NetClock. 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.

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 view and edit the `authorized_keys` file, to add Public Keys. Using FTP, SCP, or SFTP the user may also retrieve the `authorized_keys` file from the `.ssh` directory.

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

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 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 `.ssh` directory named `authorized_keys`. The file is to be formatted such that the key is followed by the optional comment with only one key per line. The file format, line terminations, and other EOL or EOF characters should correspond to UNIX conventions, not Windows.

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

If a user wants to completely control the public keys used for authentication, a correctly formatted `authorized_keys` file formatted as indicated in the OpenSSH web site can be loaded onto a secure Spectracom product. The user transfers a new public key file using an insecure FTP client or a secure SCP or SFTP client using only account password authentication. The user should place the new public key's file in the `.ssh` directory.

Secure shell sessions using an SSH client can be performed using the admin or a user-defined account. The user may use Account Password or Public Key with Passphrase authentication. The OpenSSH tool SSH-KEYGEN may be used to create 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 an SSH session.

Creating an SSH session with Password Authentication for the admin account:

```
ssh admin@10.10.200.5  
admin@10.10.200.5's password: admin123
```

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

Creating an SSH session using Public Key with Passphrase Authentication for the admin account:

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

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

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

3.4.14.2 Secure File Transfer

NetClocks 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, in which the admin or a user-defined account is 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 account 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 product file system 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 authorized_keys scp@10.10.200.5:~/.ssh
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 scp@10.10.200.5:~/.ssh
Enter passphrase for key './id_rsa': mysecretpassphrase
```

```
publickeys      100% |*****| 5 00:00
```

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

```
sftp 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.

NOTE: Use of SCP and SFTP is restricted to the administrator. To access SCP, enter the account name SCP with your administrator password. For SFTP, the account name is SCP.

3.4.14.3 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/)

3.4.14.4 Configuring HTTPS

The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS) (Figure 3-63). The OpenSSL package also provides tools and software, which is used to create x509 Certificate Requests, Self Signed Certificates and Private/Public Keys. The NetClock uses OpenSSL library with a simple GUI interface to create certificate Requests and self-signed certificates. Users can then send these certificate requests to an external Certificate Authority (CA) for the creation of a third party verifiable certificate or use an internal corporate CA. If a Certificate Authority is not available the user can simply use the self-signed certificate that comes with the unit until it expires or create their own self-signed certificates to allow the use of HTTPS.

Network
[SSH](#)
[HTTPS](#)
[User Account](#)
[SNMP Security](#)
[LDAP General](#)
[LDAP Client Configuration](#)
[RADIUS General](#)
[RADIUS Client Configuration](#)
[IPSEC General](#)
[IPSEC Manual SA Configuration](#)
[IPSEC IKE SA Configuration](#)

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:

*-Required Field

Create Certificate Request and Self Signed Certificate

Signature Algorithm: MD5

* Private Key Pass Phrase:

* RSA Private Key Bit Length: 1024

* 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): 7300

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-63: Security HTTPS Screen (1 of 2)

NOTE: If the IP Address or Common Name (Host Name) is changed, you may wish to regenerate the security certificate. Otherwise you may receive security warnings from your web browser.

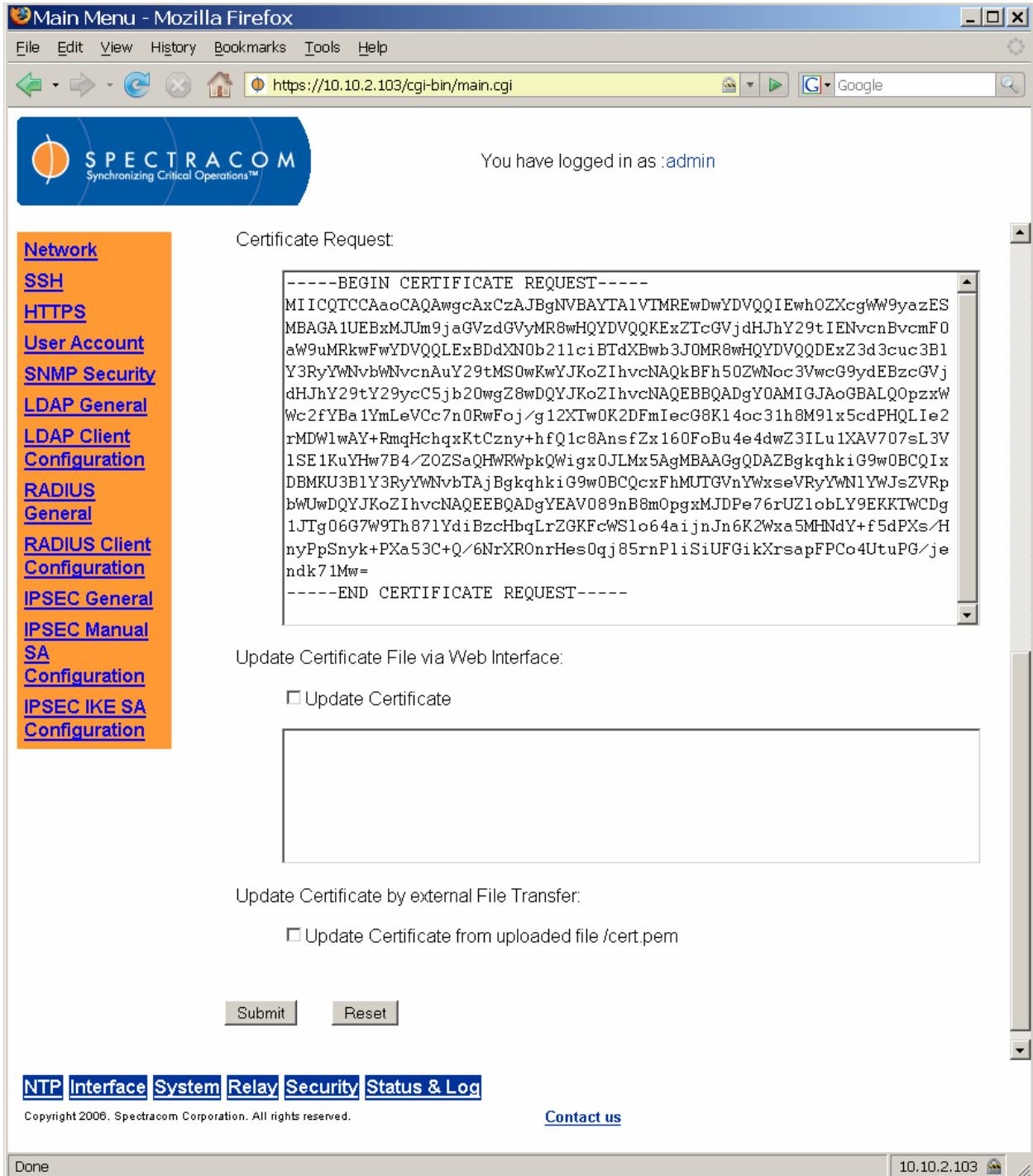


Figure 3-64: Security HTTPS Screen (2 of 2)

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.

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.

The Common Name field is the name of the host being authenticated. The Common Name field in the x509 certificate must match the hostname, IP address, or URL used to reach the host via HTTPS. This field should be filled with the hostname or IP address of the NetClock. Spectracom recommends using a static IP address, because DHCP-generated IP addresses can change. If the hostname or IP address changes, the x509 certificate must be regenerated. If using only self-signed certificates, the user should choose the fields based on the company's security policy.

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 root directory with the file name cert.csr. This file can be retrieved using FTP, SCP or SFTP. The certificate request can also be cut and paste from the certificate request text box on the web browser user interface.

3.4.14.5 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.

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

3.4.14.6 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 root directory using file transfer and installed using the web browser user interface.

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 root directory using any file name. The user then selects the “Update Certificate with file named” check box and enters the file name in the space. The user then enters submit at the bottom of the page and the current self-signed certificate is overwritten with the specified file name.

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

3.4.14.7 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.

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 root directory using either SCP or SFTP. Once the file is transferred, the user simply selects the “Update Certificate with file named” checkbox and provides the file names. The user then enters the submit button.

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

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

3.4.15 If You Cannot Access a Secure NetClock

Spectracom assumes that the customer is responsible for the physical security of the product. Spectracom secure products are required to be locked in a secure enclosure, cabinet or room. Unauthorized persons are not to be given access to the product nor should a serial cable and

terminal program be attached unless the system administrator is configuring or performing maintenance.

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

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

3.4.16 Configuring User Accounts

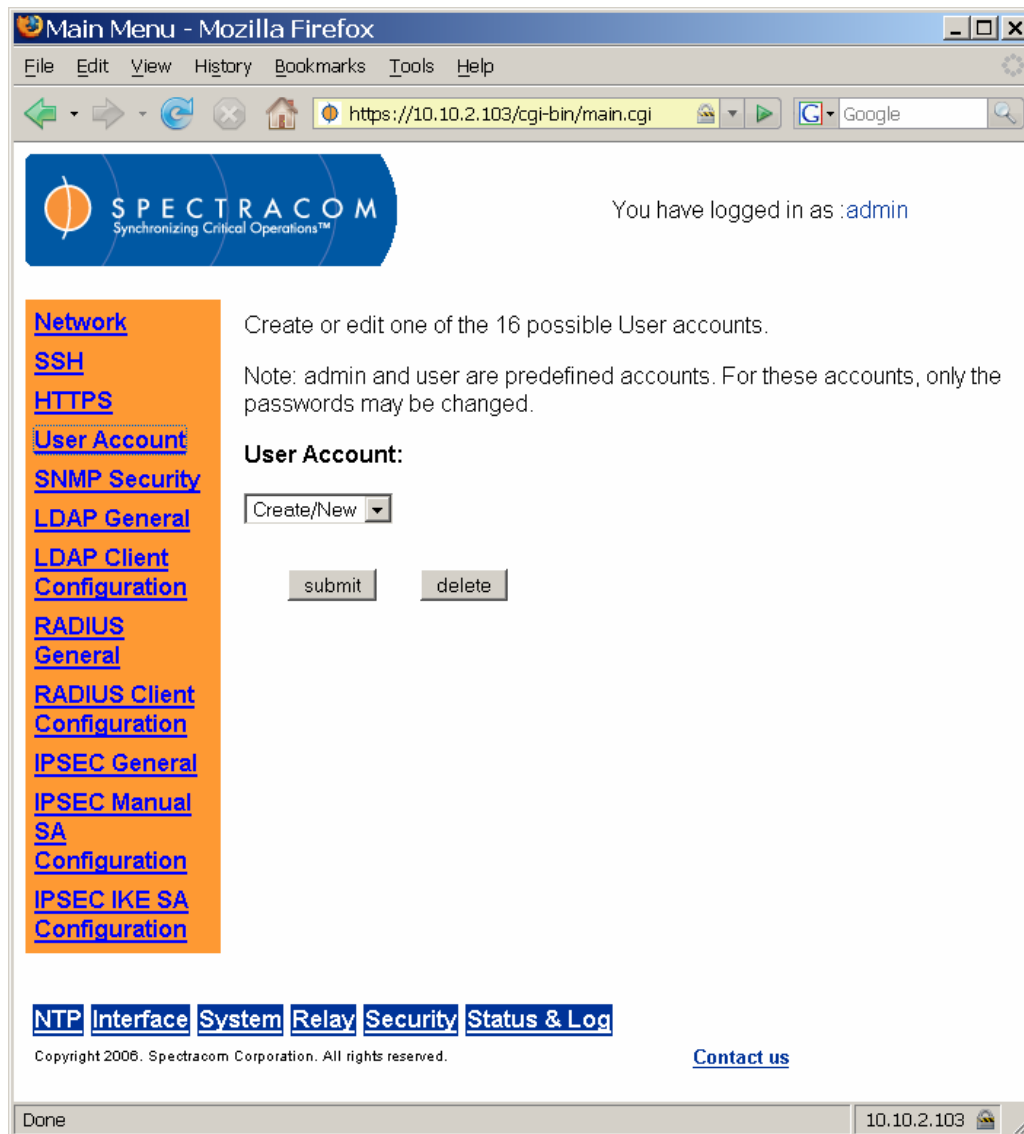


Figure 3-65: Security User Account Screen

From the Security User Account screen (Figure 3-65), the user may create and assign privileges to up to 16 local users. Click “Create/New” and “Submit” to create and assign privileges to users (Figure 3-66).

SPECTRACOM
Synchronizing Critical Operations™

You have logged in as :admin

[Network](#)
[SSH](#)
[HTTPS](#)
[User Account](#)
[SNMP Security](#)
[LDAP General](#)
[LDAP Client Configuration](#)
[RADIUS General](#)
[RADIUS Client Configuration](#)
[IPSEC General](#)
[IPSEC Manual SA Configuration](#)
[IPSEC IKE SA Configuration](#)

User Name (Required):
 Password (Required):
 Type Password Again (Required):

Group	None	Read	Write
System status and logs	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Local system clocks	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
User-defined alarms	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Network information and settings	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Security features (SSL, SSH, etc.)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
NTP configuration and statistics	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
NTP security configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SNMP configuration	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SNMP security configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Modem dialout configuration	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Relay configuration and status	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Oscillator monitoring and disciplining	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Done 10.10.2.103

Figure 3-66: Security User Account Screen (Assigning Privileges)

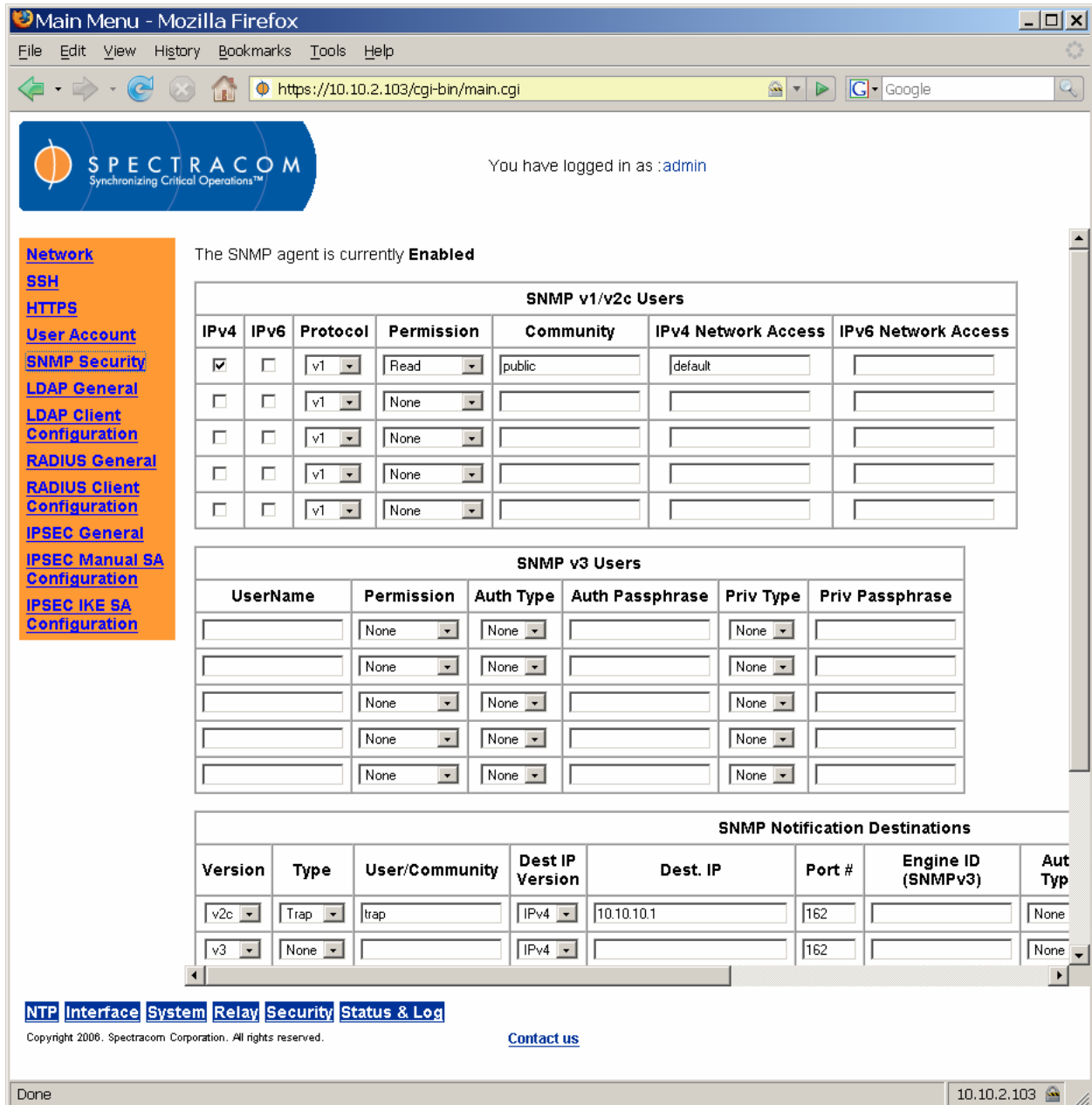


Figure 3-67: SNMP Security Screen (1 of 3)

3.4.17 Configuring SNMP v1, v2, and v3

From the SNMP Security screen (Figure 3-67), the user can define the network locations, hostnames, and protocols used in communicating with SNMP v1, v2, and v3 users. (SNMP v3 is secure SNMP.)

NOTE: Usernames are arbitrary. The username must be the same on the unit and on the management station.

Main Menu - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://10.10.2.103/cgi-bin/main.cgi

SPECTRACOM
Synchronizing Critical Operations™

You have logged in as :admin

v1 None

v1 None

v1 None

[Network](#)
[SSH](#)
[HTTPS](#)
[User Account](#)
[SNMP Security](#)
[LDAP General](#)
[LDAP Client Configuration](#)
[RADIUS General](#)
[RADIUS Client Configuration](#)
[IPSEC General](#)
[IPSEC Manual SA Configuration](#)
[IPSEC IKE SA Configuration](#)

SNMP v3 Users

UserName	Permission	Auth Type	Auth Passphrase	Priv Type	Priv Passphrase
<input type="text"/>	None	None	<input type="text"/>	None	<input type="text"/>
<input type="text"/>	None	None	<input type="text"/>	None	<input type="text"/>
<input type="text"/>	None	None	<input type="text"/>	None	<input type="text"/>
<input type="text"/>	None	None	<input type="text"/>	None	<input type="text"/>
<input type="text"/>	None	None	<input type="text"/>	None	<input type="text"/>

SNMP Notification Destinations

Version	Type	User/Community	Dest IP Version	Dest. IP	Port #	Engine ID (SNMPv3)	Aut Typ
v2c	Trap	trap	IPv4	10.10.10.1	162	<input type="text"/>	None
v3	None	<input type="text"/>	IPv4	<input type="text"/>	162	<input type="text"/>	None
v3	None	<input type="text"/>	IPv4	<input type="text"/>	162	<input type="text"/>	None
v3	None	<input type="text"/>	IPv4	<input type="text"/>	162	<input type="text"/>	None
v3	None	<input type="text"/>	IPv4	<input type="text"/>	162	<input type="text"/>	None

Submit

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

https://10.10.2.103/cgi-bin/showsnmpsecconf.cgi 10.10.2.103

Figure 3-68: SNMP Security Screen (2 of 3)

NOTE: When selecting an engine ID for SNMPv3, pick an arbitrary hexadecimal number (such as 0x1234).

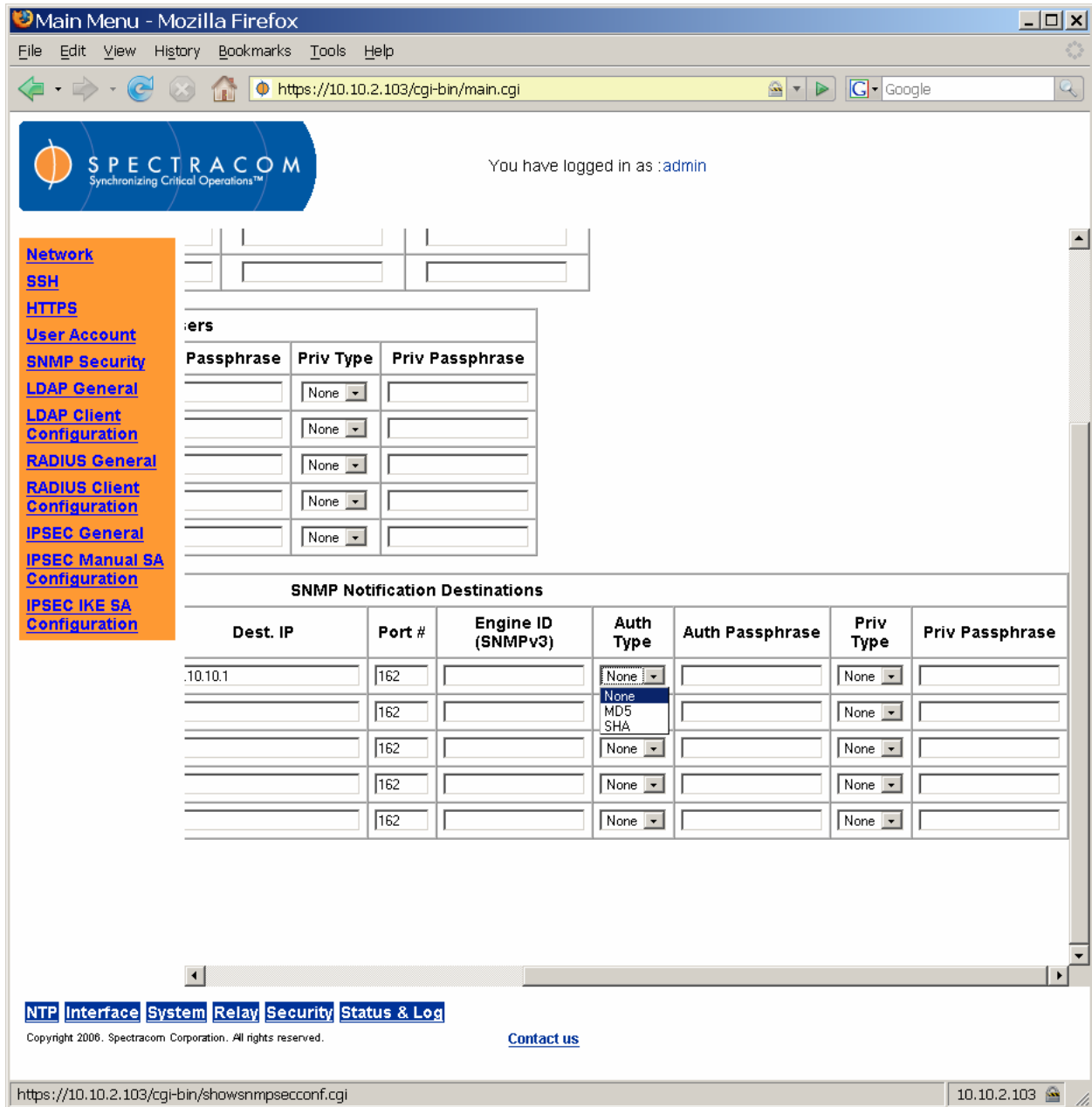


Figure 3-69: SNMP Security Screen (3 of 3)

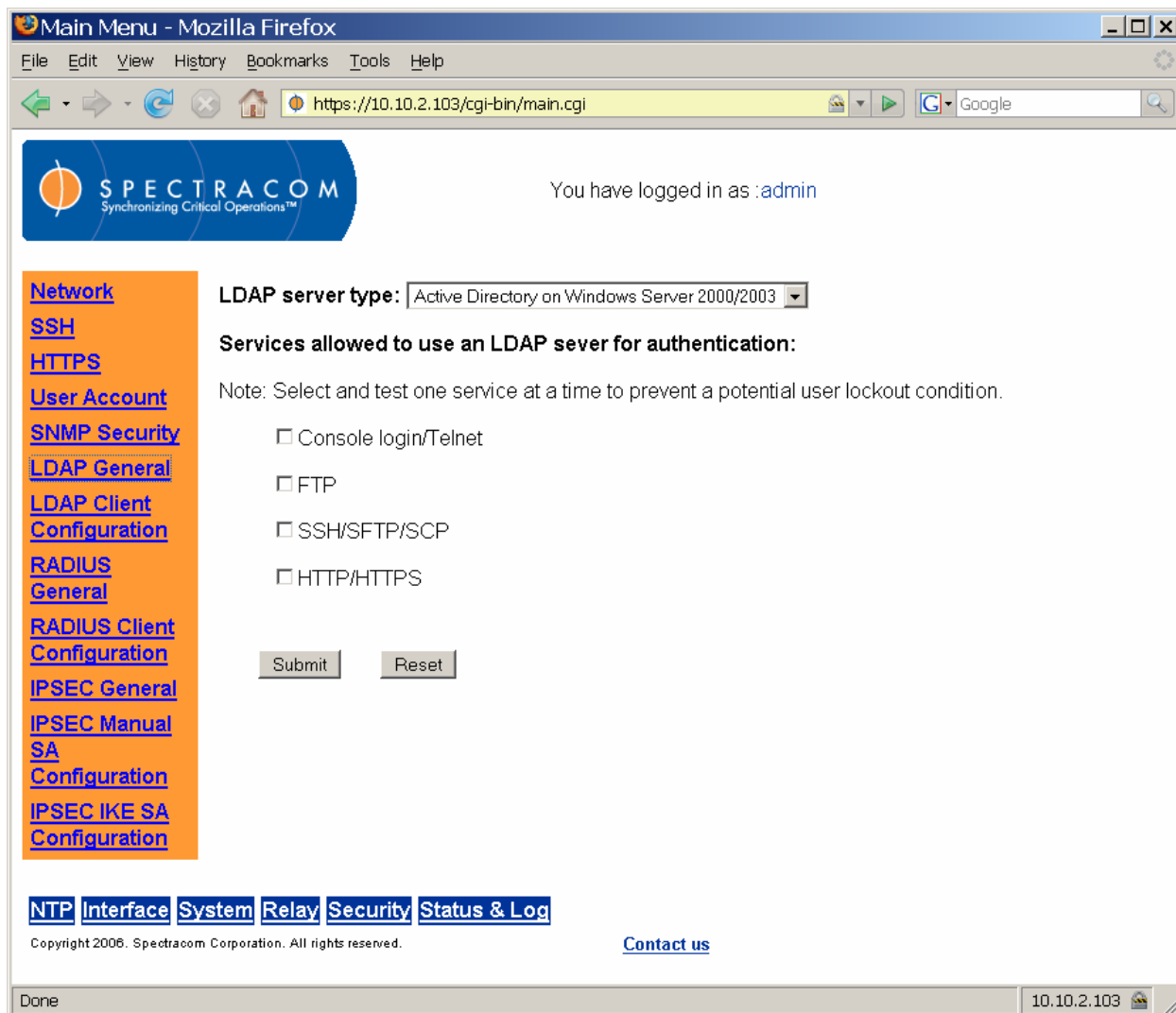


Figure 3-70: Security LDAP General Screen

3.4.18 Configuring LDAP and RADIUS

From the Security LDAP General screen (Figure 3-70), the user chooses the LDAP server type (it must be the correct one – check with your LDAP server administrator if you are not sure) and choose the types of services allowed to request authentication from the LDAP server.

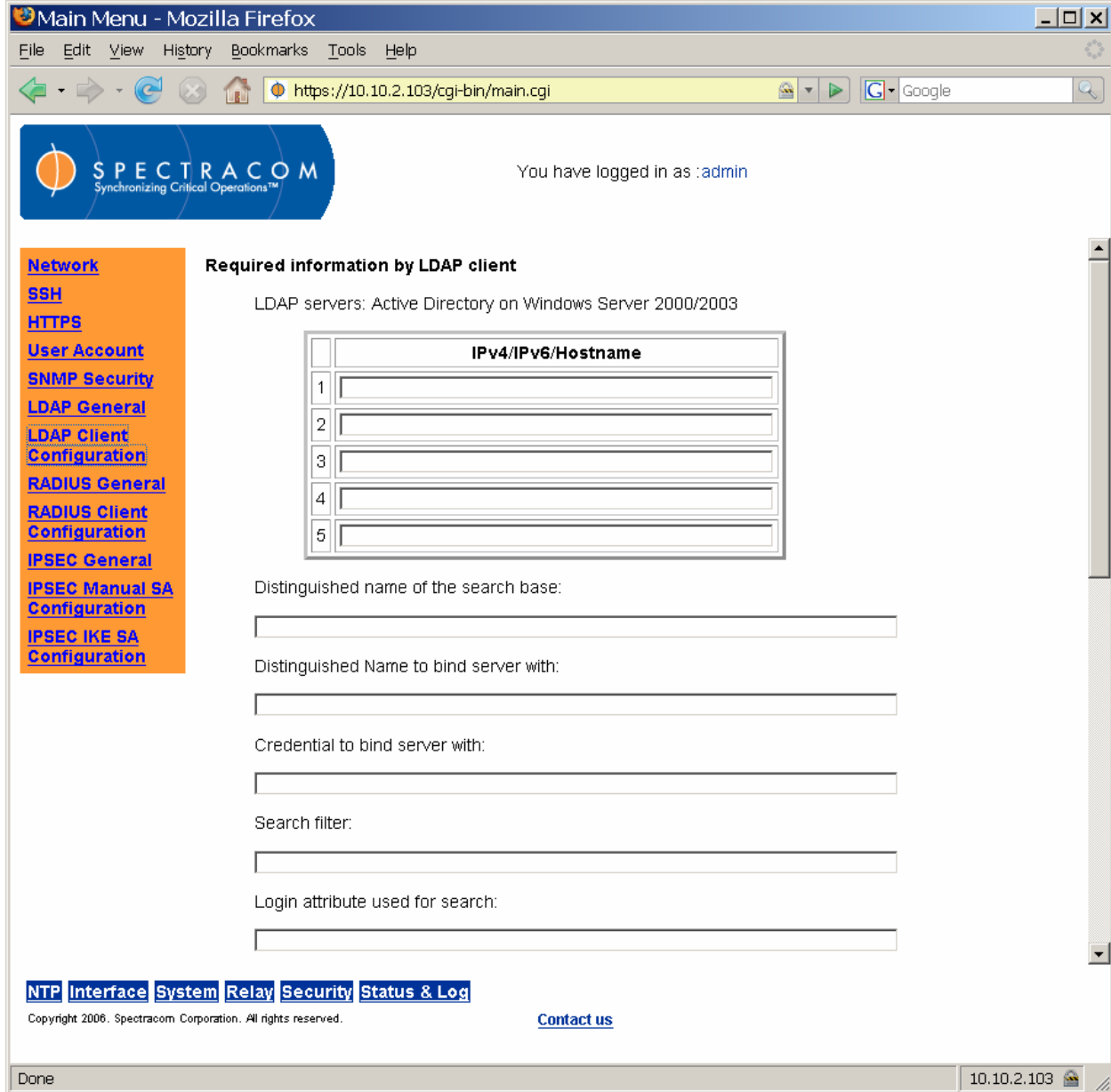


Figure 3-71: Security LDAP Client Configuration Screen (1 of 2)

From the LDAP Client Configuration screen, the user specifies the addresses or hostnames of the LDAP server(s) and inputs other fields that must be provided by the LDAP server administrator. One of the servers (and one only) must be defined as the main LDAP server. The other servers are replicas.

Main Menu - Mozilla Firefox
 File Edit View History Bookmarks Tools Help
 https://10.10.2.103/cgi-bin/main.cgi

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as :admin

Search base for password:

Enable SSL for simple authentication

Server CA certificate verification level:

CA certificate for server certificate verification:

Enable group based authentication

Group to enforce membership of:

Group member attribute:

General setting

Port for server binding: --Default: 389 for LDAP/636 for LDAPS
 Time limit for searching: --Default: 120 seconds
 Time limit for binding : --Default: 120 seconds
 LDAP protocol version --Default: LDAP V3
 Scope to search server with: --Default: sub

NTP Interface System Relay Security Status & Log

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

https://10.10.2.103/cgi-bin/showldapconfig.cgi 10.10.2.103

Figure 3-72: Security LDAP Client Configuration Screen (2 of 2)

If “Enable SSL for simple authentication” is not clicked, clear text is sent to the LDAP server. If SSL is checked, text sent to the LDAP server is encrypted.

A sample configuration for an OpenLDAP server would be as follows:

DN for search base	dc=spectracomcorp,dc=com
Bind DN	cn=manager,dc=spectracomcorp,dc=com
Bind password	test
Search filter	objectclass=posixaccount
Login attribute	uid
DN for password	ou=people,dc=spectracomcorp,dc=com?one
Group DN	cn=engineer,ou=group,dc=spectracomcorp,dc=com
Group member attribute	member

A sample configuration for Active Directory would be as follows:

DN for search base	dc=test,dc=spectracomcorp,dc=com
Bind DN	cn=administrator,cn=users,dc=test,dc=spectracomcorp,dc=com
Bind password	test
Search filter	objectclass=User
Login attribute	sAMAccountName
DN for password	ou=users,dc=test,dc=spectracomcorp,dc=com?one
Group DN	cn=engineer,cn=users,dc=test,dc=spectracomcorp,dc=com
Group member attribute	member

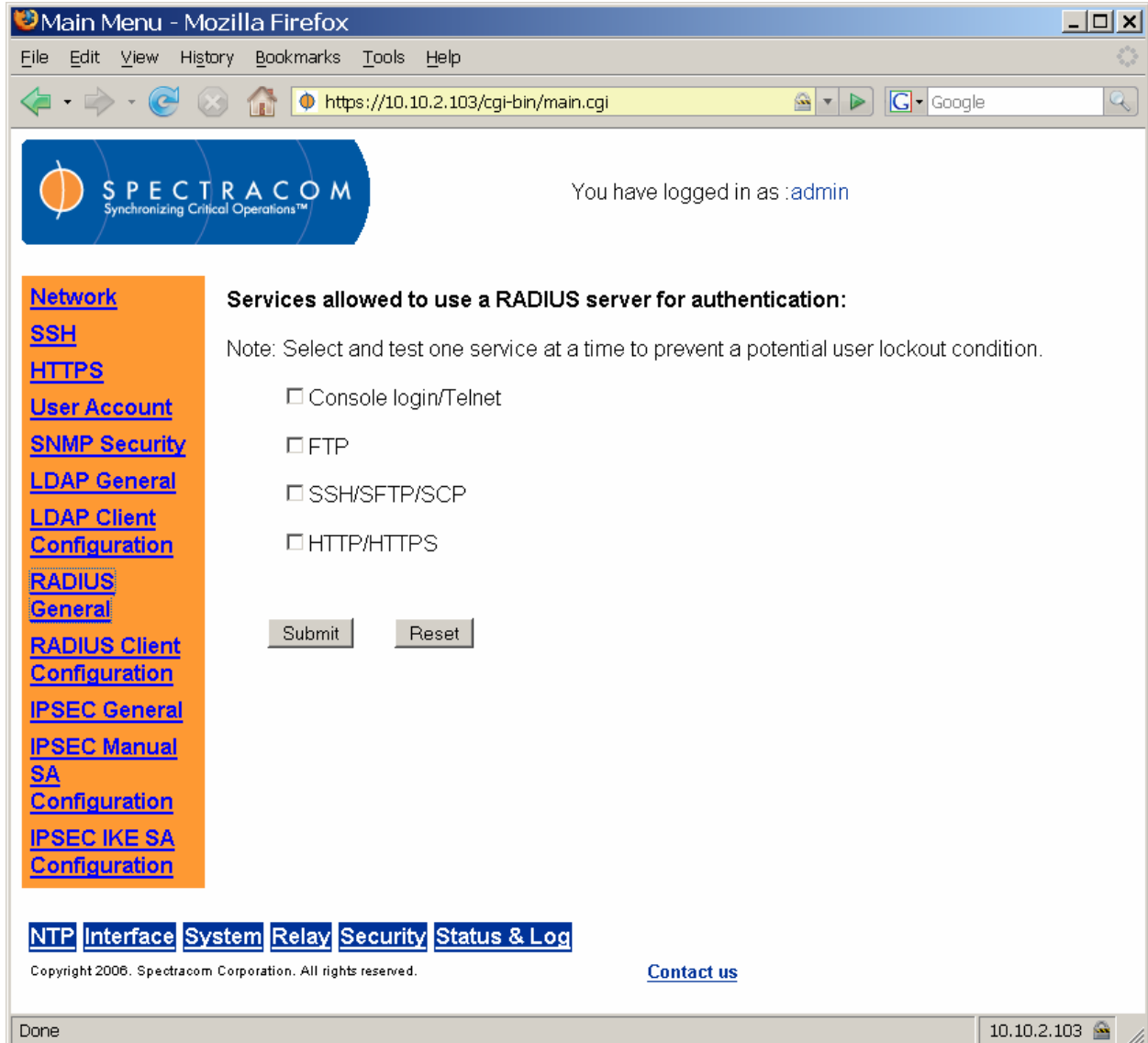


Figure 3-73: Security RADIUS General Screen

From the Security RADIUS General screen (Figure 3-73), the user selects the services that may use RADIUS for authentication.

The screenshot shows a web browser window titled "Main Menu - Mozilla Firefox" with the address bar displaying "https://10.10.2.103/cgi-bin/main.cgi". The page header includes the Spectracom logo and the text "You have logged in as : admin".

Network

- [SSH](#)
- [HTTPS](#)
- [User Account](#)
- [SNMP Security](#)
- [LDAP General](#)
- [LDAP Client Configuration](#)
- [RADIUS General](#)
- [RADIUS Client Configuration](#)
- [IPSEC General](#)
- [IPSEC Manual SA Configuration](#)
- [IPSEC IKE SA Configuration](#)

Radius server 1

HostName/IPV4/IPv6:
Secret Key:
Port:
Timeout:

Radius server 2

HostName/IPV4/IPv6:
Secret Key:
Port:
Timeout:

Radius server 3

HostName/IPV4/IPv6:
Secret Key:
Port:
Timeout:

Radius server 4

HostName/IPV4/IPv6:
Secret Key:
Port:
Timeout:

Radius server 5

HostName/IPV4/IPv6:
Secret Key:
Port:
Timeout:

General setting for all radius servers

Re-transmit Attempts: (0 to 3)

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright © 2005 Spectracom Corporation. All rights reserved. [Contact us](#)

Done 10.10.2.103

Figure 3-74: Security RADIUS Client Configuration Screen

From the Security RADIUS Client Configuration screen (Figure 3-74), the user identifies the addresses of the network's RADIUS servers. From this screen, the user also specifies the number of re-transmit attempts (0 to 3) that will be made in communicating with the RADIUS server.

3.4.19 Configuring IPsec

Internet Protocol Security (IPsec) is a suite of IP protocols that authenticates and encrypts network communications. IPsec supports IPv6 and IPv4 as of this writing.

IPsec defines a Security Association (SA), consisting of secured communications between two network devices. Configuring IPsec requires us to define SA Policy (SAP) and SA Descriptors (SAD). SAP determines what network traffic can or must be secured through IPsec. SAD describes actively secured conversations. All network traffic for an SA contains an identical Security Parameter Index (SPI).

3.4.19.1 AH vs. ESP

An Authentication Header (AH) and an Encapsulating Security Payload (ESP) are the primary protocols used by IPsec. They authenticate (AH) or authenticate and encrypt (ESP) the data across that connection. Typically, they are used independently, but it is possible to use them together. The NetClock supports both protocols.

3.4.19.2 Transport Mode vs. Tunnel Mode

Transport mode provides a secure connection between two endpoints by encapsulating the IP payload. Tunnel mode encapsulates the entire IP packet/

NOTE: Tunnel mode is used to form a traditional Virtual Private Network (VPN), in which the tunnel creates a secure path across a distrusted Internet connection. The NetClock supports *Transport mode ONLY*.

3.4.19.3 MD5 vs. SHA-1 vs. DES vs. 3DES vs. AES

An IPsec connection can use two or three encryption choices from among those available. Authentication calculates an Integrity Check Value (ICV) over the data packet's contents. It is usually built on a hash algorithm (for example, MD5 or SHA-1). It uses a secure key known to both endpoints, allowing the recipient to compute the ICV as the sender has computed it. If the recipient gets the same value, the sender has effectively authenticated itself.

3.4.19.4 IKE vs. Manual Keys

To communicate, the devices at both endpoints must possess the same secure keys. Keys can be entered manually. They may also be generated dynamically between two hosts through Internet Key Exchange (IKE). The NetClock supports both IKE and manual keys.

3.4.19.5 Main Mode vs. Aggressive Mode

The initial IKE exchange may be efficient or it may be secure. This tradeoff is governed by the exchange mode, Main or Aggressive. Main mode is completely secure and requires six packets to be sent between the two devices. Aggressive mode requires only three packets be sent between the two devices, but it is less secure.

NOTE: The NetClock supports both Main and Aggressive modes. Aggressive mode is NOT recommended because of the security risks involved.

3.4.19.6 Configuring IPsec (IKE SA)

To establish an IPsec connection between the Spectracom Netclock and an IPv4 addressed host ("A") using IKE SA configuration, we must first configure the IPsec IKE to communicate with host A. To do this, navigate to the IPSEC IKE SA Configuration screen (Figure 3-75).

The screenshot shows a web browser window titled "Main Menu - Mozilla Firefox" with the URL "https://10.10.2.103/cgi-bin/main.cgi". The page displays the Spectracom logo and a message "You have logged in as :admin". A navigation menu on the left lists various configuration options, with "IPSEC IKE SA Configuration" highlighted. The main content area is titled "IPsec Security Association Configuration" and shows the "Phase 1:" configuration options:

- Exchange Mode:**
 - Main
 - Aggressive
 - Base
- Life Time:**
 - Input: 0
 - Unit: Minutes
- DH group:**
 - Dropdown: Group 1 - Modp768
- Encryption Algorithm:**
 - Dropdown: DES
- Hash Algorithm:**
 - Dropdown: HMAC-MD5
- Authentication Method:**
 - Using Preshared key located in
 - Using x.509 certificate
 - Certificate Files Path:
 - Peer's Certificate File name:
 - Certificate and private keys on this machine
 - Generate certificate and private key
- Signature Algorithm:**
 - Dropdown: Md5
 - Dropdown: Sha1

At the bottom of the page, there are navigation links: "NTP", "Interface", "System", "Relay", "Security", "Status & Log", and "Contact us". The footer includes "Copyright 2006. Spectracom Corporation. All rights reserved." and the URL "https://10.10.2.103/cgi-bin/showipsecikesa.cgi".

Figure 3-75: IPSEC IKE SA Configuration Screen (1 of 2)

Main Menu - Mozilla Firefox
 File Edit View History Bookmarks Tools Help
 https://10.10.2.103/cgi-bin/main.cgi

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as :admin

Certificate and private keys on this machine

Generate certificate and private key

Signature Algorithm :

RSA Private Key Length:

Upload the certificate and private key

Certificate File Name:

Private Key File Name:

Phase 2:

Life Time:

Encryption Algorithm:
 DES 3DES AES NULL

Authentication Algorithm:
 HMAC-SHA1 HMAC-MD5

Compression Algorithm:
 Deflate

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

https://10.10.2.103/cgi-bin/showipsecikesa.cgi 10.10.2.103

Figure 3-76: IPSEC IKE SA Configuration Screen (2 of 2)

3.4.19.6.1 IKE Phase 1 Configuration

Exchange Mode defines the mode for Phase 1 (when the IKE daemon is the initiator). You may select all three options (meaning the NetClock supports Main, Aggressive, and Base exchange modes) or you may select one or two modes to support. The IKE daemon uses the Main exchange mode when it is the initiator.

Life Time defines the lifetime of the Phase 1 SA proposal.

DH group defines the group used for Diffie-Hellman exponentiations. This directive must be defined using one of the following:

Group 1 - Modp768
Group 2 - Modp1024
Group 5 - Modp1536
Group 14 - Modp2048

NOTE: When using Aggressive mode, the DH group defined for each proposal must be the same.

Encryption Algorithm specifies the algorithm used for Phase 1 negotiation. Choose DES, 3DES, or AES as desired (or as specified by your network administrator).

Hash Algorithm defines another algorithm used for Phase 1 negotiation. Select HMAC-MD5 or HMAC-SHA1 as desired or required.

Authentication Method defines the means of Phase 1 authentication used (preshared keys or X.509 certificates).

Preshared Keys

The easiest way to authenticate using the IKE daemon is through preshared keys. These keys must be defined in a file uploaded to the location specified in the *Using Preshared key located in* field.

NOTE: After the file is uploaded, its file privileges will be changed automatically to deny unauthorized users access to the preshared keys. This means you will not be able to access the file after uploading it. Always keep an extra copy of the file on hand in another location.

The preshared key file should have the following syntax:

```
192.168.2.100      password1
5.0.0.1           password2
3ffe:501:ffff::3  password3
```

This file is organized in columns. The first column holds the identity of the peer authenticated by the preshared key. The second column contains the keys.

X.509 Certificates

The IKE daemon supports the use of X.509 certificates for authentication. Spectram supplies two means of providing the public/private key pair to the Netclock.

The first approach is through the user interface on the IPsec IKE SA Configuration screen. Specify the Certificate Files Path and Peer's Certificate File name, then select Md5 or Sha1 to specify the Signature Algorithm. You must also specify the RSA Private Key Length to use when generating the key pair.

Alternatively, you may generate elsewhere and upload to the NetClock your key pair(s). Specify the directory and the name of the key pairs uploaded to it. Regardless of the method used, however, you must upload the peer's public key to the NetClock and provide the directory and file name to the NetClock in the IPsec IKE SA Configuration screen.

3.4.19.6.2 IKE Phase 2 Configuration

Life Time defines how long an IPsec SA will be used.

Encryption Algorithm defines the group used for Diffie-Hellman exponentiations. This directive must be defined using one of the following:

Group 1 - Modp768
Group 2 - Modp1024
Group 5 - Modp1536
Group 14 - Modp2048

NOTE: When using Aggressive mode, the DH group defined for each proposal must be the same.

Encryption Algorithm specifies the algorithm used for Phase 2. Select DES, 3DES, AES (used with ESP) or NULL as desired (or as required by your network administrator).

Authentication Algorithm defines another algorithm used for Phase 2. Select HMAC-SHA1 or HMAC-MD5 as desired or required.

Compression Algorithm defaults to "deflate." It is not configurable at this time.

NOTE: After completing and submitting changes in the IPsec IKE SA Configuration screen, check to make sure IPsec is enabled and IKE is selected for use with IPsec. The IKE Log (refer to *Logs and Status Reporting*) is helpful in troubleshooting this condition.

3.4.19.6.3 Configure IPsec Security Policy

Configure the IPsec security policy from the IPsec General screen (Figure 3-77).

NOTE: Always configure IKE BEFORE enabling the IKE option from the IPsec General screen. If IKE is not configured, the IKE daemon won't start correctly when the Security Association is enabled.

From the IPsec General screen (Figure 3-77), enable (or disable) the IPsec service and specify the Security Association (IKE if already configured, or Manually Configure). In the Security Policy table, input the NetClock's IP address as the Source IP and host A's address as the Destination IP.

Main Menu - Mozilla Firefox
 File Edit View History Bookmarks Tools Help
 https://10.10.2.103/cgi-bin/main.cgi

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as : admin

Network
[SSH](#)
[HTTPS](#)
[User Account](#)
[SNMP Security](#)
[LDAP General](#)
[LDAP Client Configuration](#)
[RADIUS General](#)
[RADIUS Client Configuration](#)
[IPSEC General](#)
[IPSEC Manual SA Configuration](#)
[IPSEC IKE SA Configuration](#)

IPsec Service:
 Enabled Disabled

Security Association:
 Using IKE Manually Configure

Security Policy:

Source IP	Destination IP	Protocol	Direction	Policy	AH	Level	ESP	Level
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright © 2006, Spectracom Corporation. All rights reserved. [Contact us](#)

Done 10.10.2.103

Figure 3-77: IPsec General Screen

Select *ANY* as the desired protocol to apply for IPsec security protection (unless a specific protocol is desired; these can be selected from the drop-down list).

Select *Both* for the Direction, which means IPsec security protection is required for both incoming and outgoing packets. Security protection may also be applied to incoming packets only, or to outgoing packets only (from the drop-down list).

Select *Ipsec* to use IPsec as the security policy. (You may also select *None* or *Discard*. Selecting *None* means that IPsec operation will not take place on the packet, while selecting *Discard* means the packet matching indexes will be discarded.

You may choose to check either or both AH and ESP to set them as *Require*, *Use*, *Default*, or *Unique*.

- *Default* means the kernel consults the system-wide default for the protocol specified.
- *Use* means the kernel uses an SA if it is available, while the kernel keeps normal operation otherwise.
- *Require* means an SA is required whenever the kernel sends a packet matched with the policy.
- *Unique* is the same as *Require*, but allows the policy to match the unique outbound SA.

3.4.19.7 Configuring IPsec (Manual SA)

To establish an IPsec connection between the NetClock and an IPv6 addressed host (“B”) using manual SA configuration, refer to the IPsec Manual SA Configuration screen (Figure 3-78).

3.4.19.7.1 Manual Security Associations

Input the NetClock IP address as the Source IP and host B’s IP address as the Destination IP.

Network

SSH

HTTPS

User Account

SNMP Security

LDAP General

LDAP Client Configuration

RADIUS General

RADIUS Client Configuration

IPSEC General

IPSEC Manual SA Configuration

IPSEC IKE SA Configuration

You have logged in as : admin

IPsec Security Association Configuration

Source IP	Destination IP	AH	SPI in Hex	Algorithm	key In ASCII	ESP
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	HMAC-MD5	<input type="text"/>	<input type="checkbox"/>

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Contact us](#)

Done 10.10.2.103

Figure 3-78: IPsec Manual SA Configuration (1 of 2)

The Security Parameter Index (SPI) must be a hexadecimal number without the “0x” prefix. Enter the desired values manually.

NOTE: SPI values between 0 and 255 are reserved and cannot be used at this time.

Make sure to check the AH or ESP boxes for the key configurations used. If the appropriate box is not checked, information following the AH or ESP inputs will be ignored by the update page.

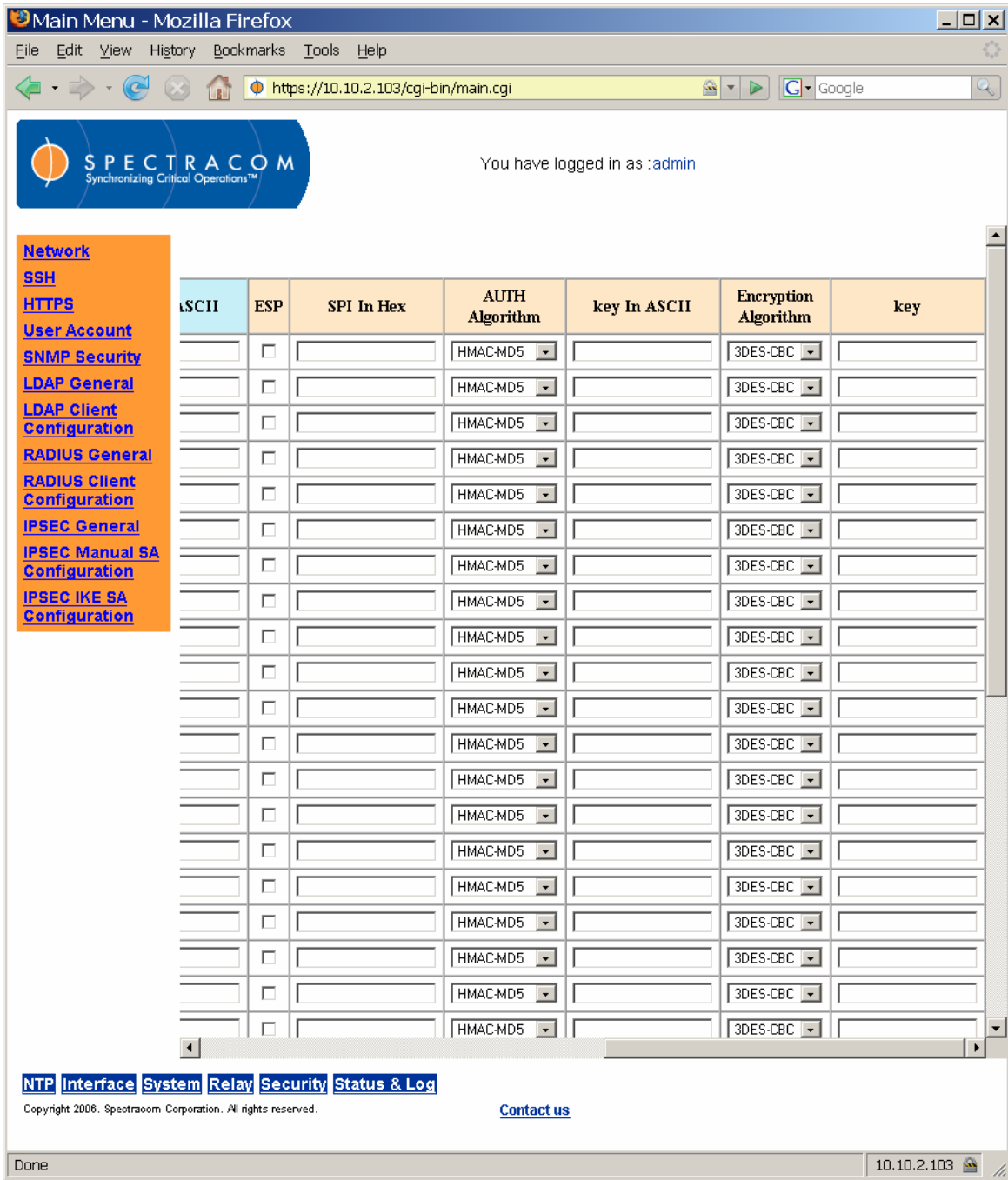


Figure 3-79: IPsec Manual SA Configuration (2 of 2)

3.4.19.7.2 Configure IPsec Security Policy

Configure the IPsec security policy from the IPsec General screen (Figure 3-80).

NOTE: The manual SA values must be configured BEFORE the manual SA option is enabled from the IPsec General screen (Figure 3-80). If the feature is enabled before it is configured from the IPsec Manual SA Configuration screen, the SA and SP tables will not update correctly.

The screenshot shows a web browser window titled "Main Menu - Mozilla Firefox" with the URL "https://10.10.2.103/cgi-bin/main.cgi". The page header includes the Spectracom logo and the text "You have logged in as :admin".

On the left side, there is a navigation menu with the following items:

- Network
- SSH
- HTTPS
- User Account
- SNMP Security
- LDAP General
- LDAP Client Configuration
- RADIUS General
- RADIUS Client Configuration
- IPSEC General
- IPSEC Manual SA Configuration
- IPSEC IKE SA Configuration

The main content area is titled "IPsec Service:" and contains the following options:

- Enabled Disabled
- Security Association:**
 - Using IKE Manually Configure
- Security Policy:**

The Security Policy table has the following columns: Source IP, Destination IP, Protocol, Direction, Policy, AH, Level, ESP, and Level. The table contains 15 rows, each with the following values:

Source IP	Destination IP	Protocol	Direction	Policy	AH	Level	ESP	Level
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require
		ANY	In	Ipsec	<input type="checkbox"/>	Require	<input type="checkbox"/>	Require

At the bottom of the page, there is a navigation bar with the following items:

- NTP
- Interface
- System
- Relay
- Security
- Status & Log

Copyright © 2006 Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-80: IPsec General Screen

Select *ANY* as the desired protocol to apply for IPSec security protection (unless a specific protocol is desired; these can be selected from the drop-down list).

NOTE: When using IKE over IPv6, do NOT select ANY. There are protocols that do not work well with IKE under IPv6 with IKE. Select one of the specific protocols listed in the dropdown menu, as desired or required.

Select *Both* for the Direction, which means IPSec security protection is required for both incoming and outgoing packets. Security protection may also be applied to incoming packets only, or to outgoing packets only (from the drop-down list).

Select *Ipssec* to use IPSec as the security policy. (You may also select *None* or *Discard*. Selecting *None* means that IPSec operation will not take place on the packet, while selecting *Discard* means the packet matching indexes will be discarded.

You may choose to check either or both AH and ESP to set them as *Require*, *Use*, *Default*, or *Unique*.

- *Default* means the kernel consults the system-wide default for the protocol specified.
- *Use* means the kernel uses an SA if it is available, while the kernel keeps normal operation otherwise.
- *Require* means an SA is required whenever the kernel sends a packet matched with the policy.

Unique is the same as *Require*, but allows the policy to match the unique outbound SA.

3.4.20 Logs and Status Reporting

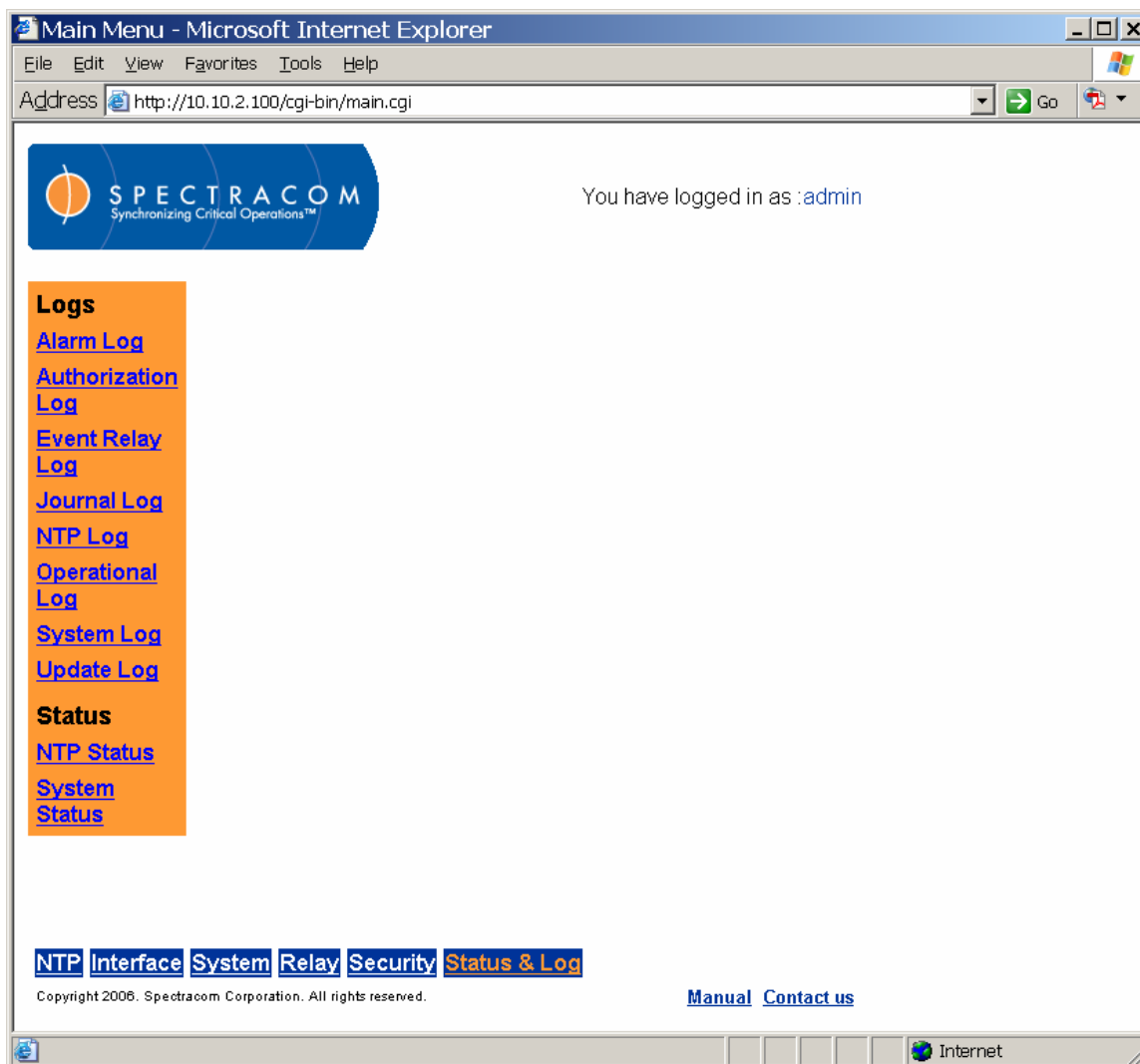


Figure 3-81: Status and Log Menu

The Status and Log menu groups the NetClock's status and log access screens. From this menu the user can view system logs and monitor that status of the NetClock's GPS signal. The user may also view system and NTP statuses from this menu.

NOTE: The times indicated in all log entries are UTC (no correction for local time or Daylight Saving Time). Four iterations of each log are kept locally on the NetClock, with the oldest rotated out (deleted) as a fifth log is generated. Logs can be up to 75K in size individually. This means that 300K of storage is devoted to each log.

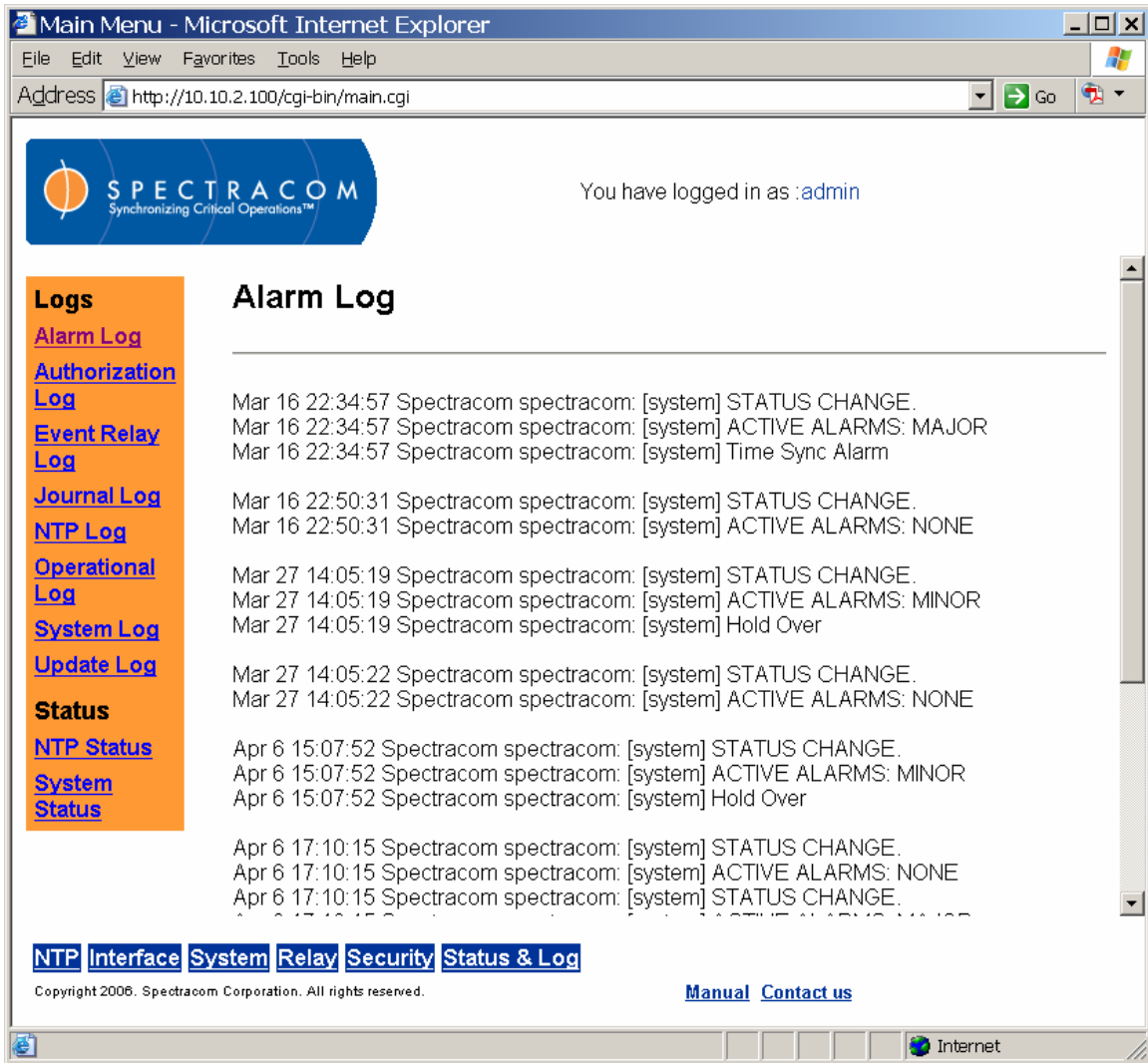


Figure 3-82: Alarm Log Screen

The Alarm Log (Figure 3-82) is a running list of the alarms (with descriptive information) experienced by the NetClock.

Main Menu - Microsoft Internet Explorer
 File Edit View Favorites Tools Help
 Address <http://10.10.2.100/cgi-bin/main.cgi> Go

SPECTRACOM
 Synchronizing Critical Operations™

You have logged in as :admin

Logs
[Alarm Log](#)
[Authorization Log](#)
[Event Relay Log](#)
[Journal Log](#)
[NTP Log](#)
[Operational Log](#)
[System Log](#)
[Update Log](#)

Status
[NTP Status](#)
[System Status](#)

Authorization Log

Mar 16 22:40:34 Spectracom login(pam_unix)[1373]: session opened for user admin by (uid=0)
 Mar 16 22:40:59 Spectracom login(pam_unix)[1373]: session closed for user admin
 Apr 5 17:30:35 Spectracom xinetd[1637]: START: telnet pid=13981 from=::ffff:10.10.128.10
 Apr 5 17:30:40 Spectracom login(pam_unix)[13982]: check pass; user unknown
 Apr 5 17:30:40 Spectracom login(pam_unix)[13982]: authentication failure; logname= uid=0 euid=0 tty=pts/0 ruser= rhost=eng_mg.miroge
 Apr 5 17:30:43 Spectracom login[13982]: FAILED LOGIN 1 FROM eng_mg.miroge FOR root^H, Authentication failure
 Apr 5 17:30:51 Spectracom login(pam_unix)[13982]: session opened for user admin by (uid=0)
 Apr 5 17:45:57 Spectracom login(pam_unix)[13982]: session closed for user admin
 Apr 5 17:45:57 Spectracom xinetd[1637]: EXIT: telnet pid=13981 duration=922(sec)

[NTP](#) [Interface](#) [System](#) [Relay](#) [Security](#) [Status & Log](#)

Copyright 2006. Spectracom Corporation. All rights reserved. [Manual](#) [Contact us](#)

Done Internet

Figure 3-83: Authorization Log Screen

The Authorization Log (Figure 3-83) is a running list of authenticated users who have accessed the NetClock.

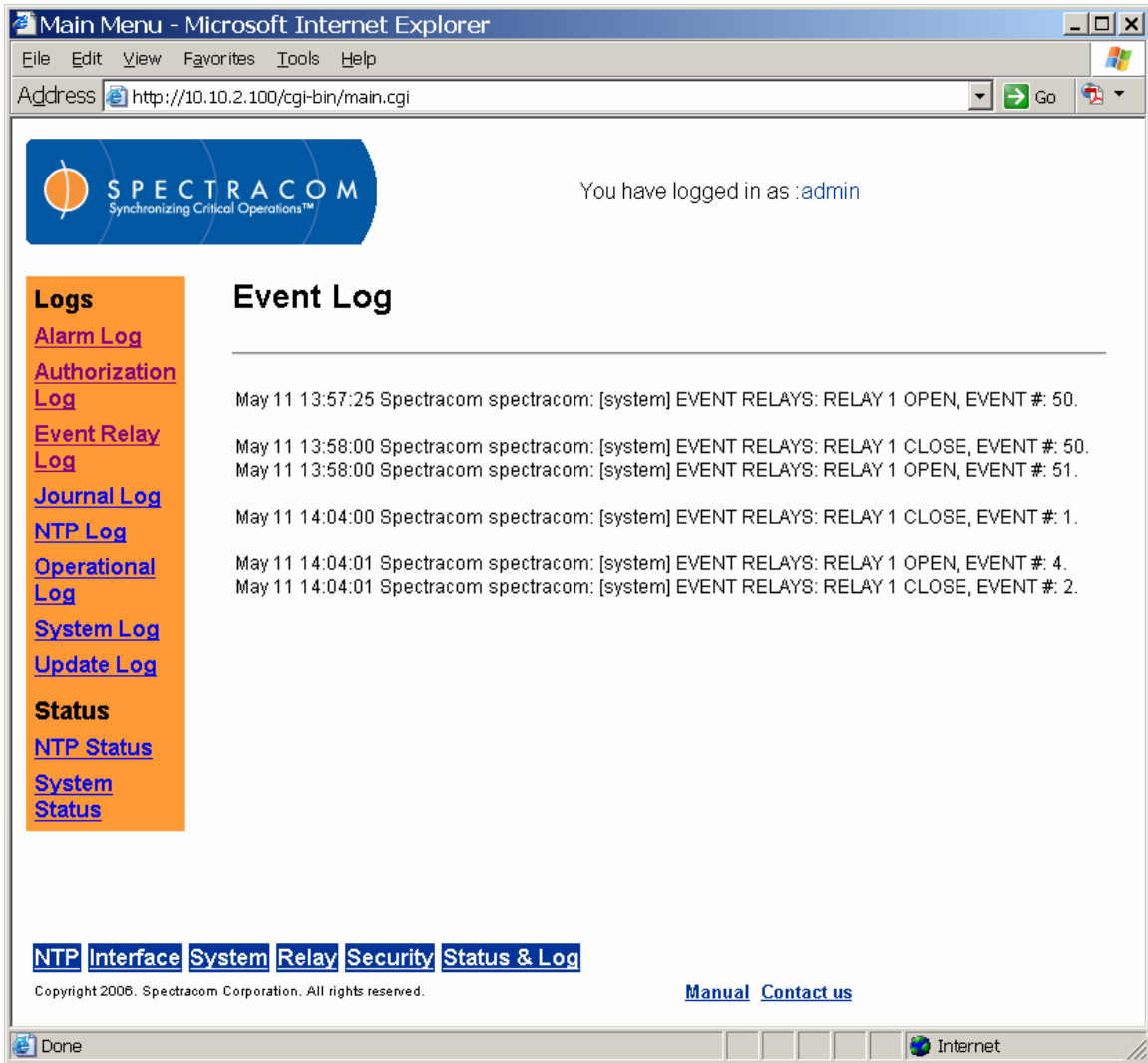


Figure 3-84: Event Log Screen

The Event Log (Figure 3-84) is a running list of the event timer relay activity.

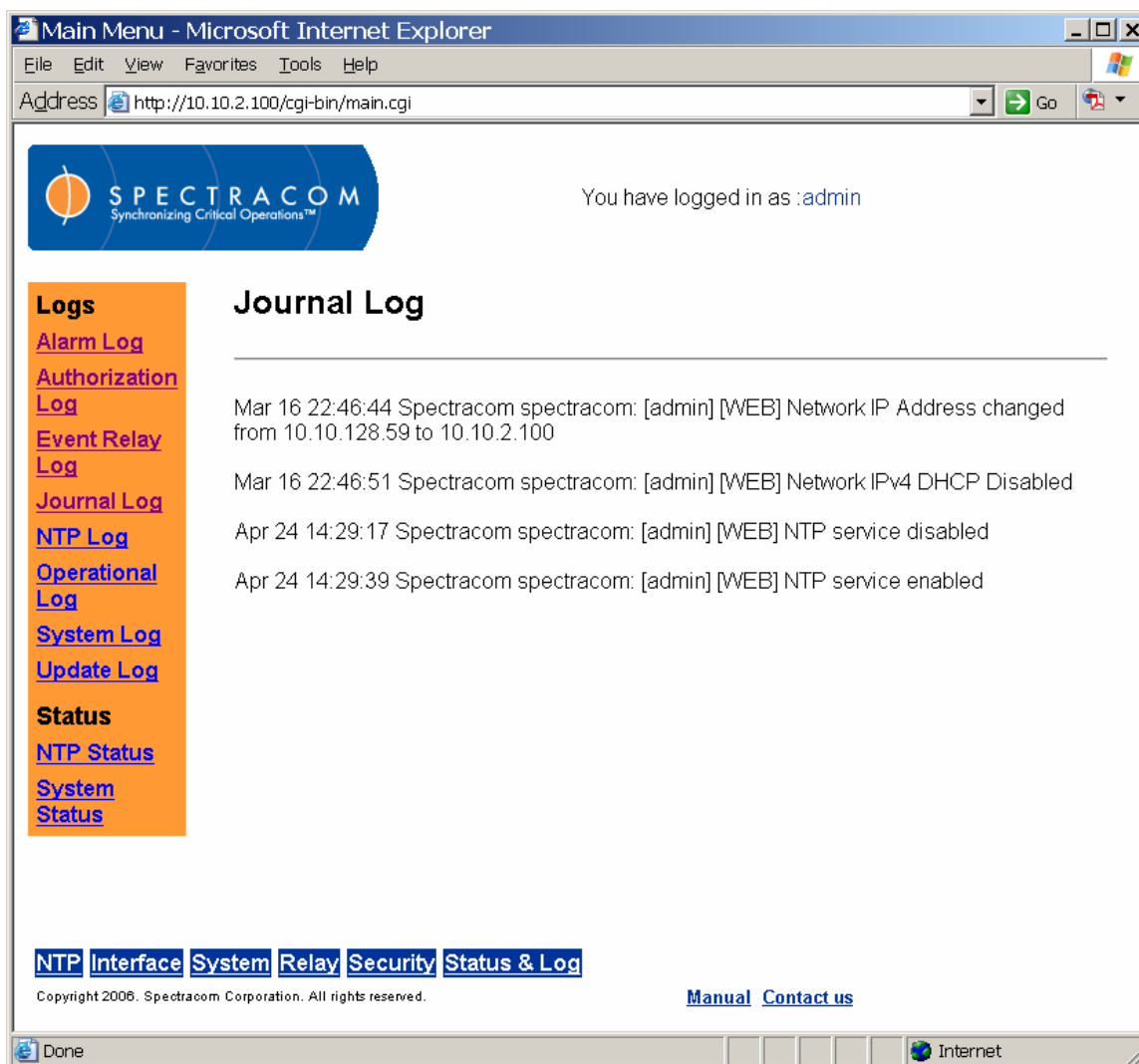


Figure 3-85: Journal Log Screen

Whenever a user changes the NetClock's configuration, the change (who performed it and what the change was) is recorded in the Journal Log (Figure 3-85).

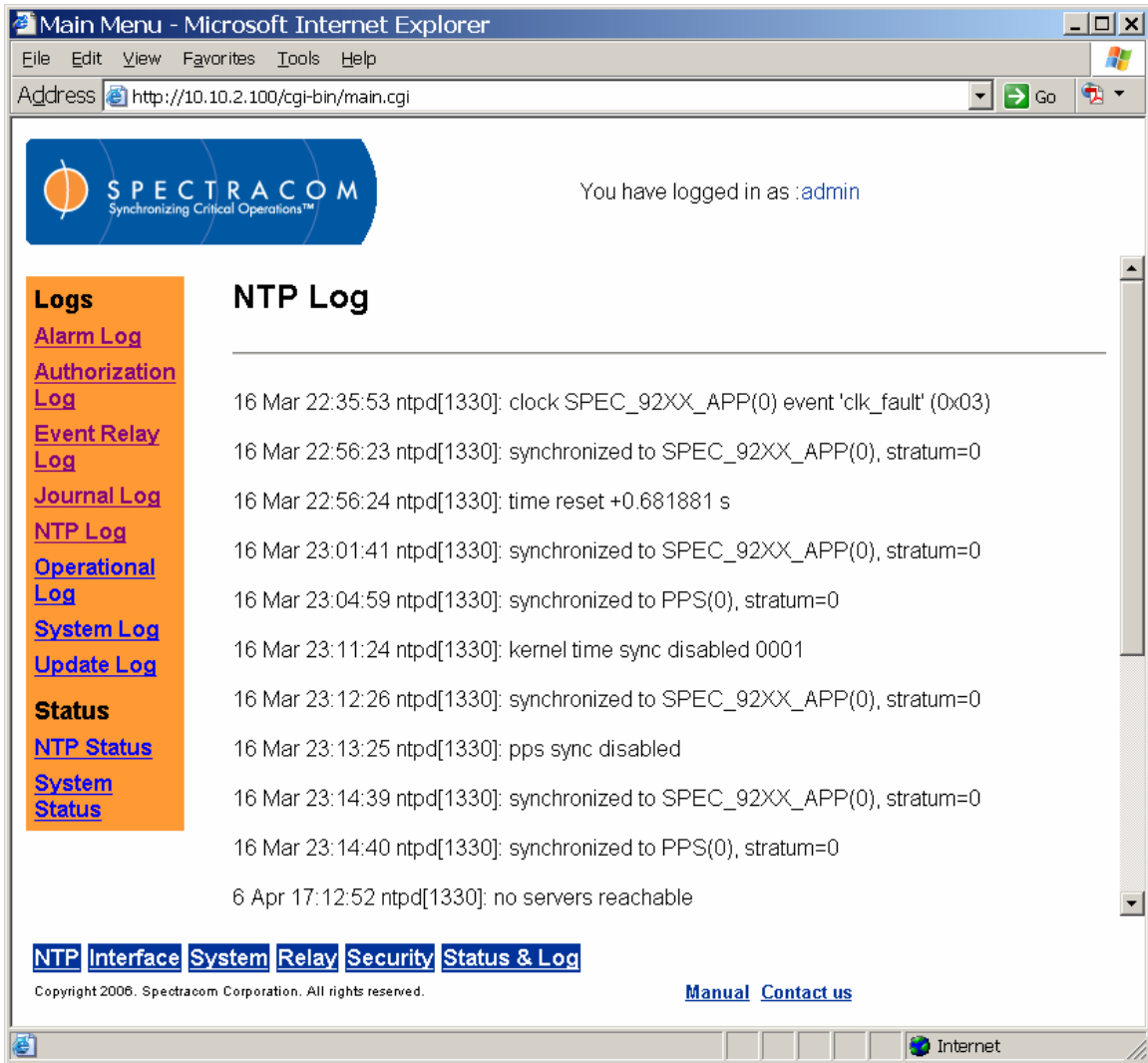


Figure 3-86: NTP Log Screen

The NTP Log (Figure 3-86) is a running list of NTP activity on the NetClock.

Logs

- [Alarm Log](#)
- [Authorization Log](#)
- [Dialout Log](#)
- [Event Relay Log](#)
- [GPS Qualification Log](#)
- [Journal Log](#)
- [NTP Log](#)
- [IKE Log](#)
- [Operational Log](#)
- [Oscillator Log](#)
- [System Log](#)
- [Update Log](#)

Status

- [GPS Signal Status](#)
- [NTP Status](#)
- [System Status](#)

IKE Log

```

2007-03-12 15:03:00: INFO: @(#)ipsec-tools 0.6.6 (http://ipsec-tools.sourceforge.net)
2007-03-12 15:03:00: INFO: @(#)This product linked OpenSSL 0.9.7i-fips 14 Oct 2005 (http://www.openssl.org)
2007-03-12 15:03:00: INFO: 127.0.0.1[500] used as isakmp port (fd=20)
2007-03-12 15:03:00: INFO: 10.10.128.8[500] used as isakmp port (fd=21)
2007-03-12 15:03:01: INFO: ::1[500] used as isakmp port (fd=22)
2007-03-12 15:03:01: INFO: fe80::230:64ff:fe04:4afd%eth0[500] used as isakmp port (fd=23)
2007-03-12 15:03:02: INFO: unsupported PF_KEY message REGISTER
2007-03-12 15:03:02: INFO: unsupported PF_KEY message 0
2007-03-12 15:03:02: INFO: unsupported PF_KEY message 0
2007-03-12 15:03:03: INFO: caught signal 15
2007-03-12 15:03:03: INFO: unsupported PF_KEY message 0
2007-03-12 15:03:04: INFO: racoon shutdown
2007-03-12 15:03:06: INFO: @(#)ipsec-tools 0.6.6 (http://ipsec-tools.sourceforge.net)
2007-03-12 15:03:06: INFO: @(#)This product linked OpenSSL 0.9.7i-fips 14 Oct 2005 (http://www.openssl.org)
2007-03-12 15:03:06: INFO: 127.0.0.1[500] used as isakmp port (fd=20)
2007-03-12 15:03:06: INFO: 10.10.128.8[500] used as isakmp port (fd=21)
2007-03-12 15:03:06: INFO: ::1[500] used as isakmp port (fd=22)
2007-03-12 15:03:06: INFO: fe80::230:64ff:fe04:4afd%eth0[500] used as isakmp port (fd=23)

```

NTP **Interface** **System** **Relay** **Security** **Status & Log**

Copyright 2006, Spectracom Corporation. All rights reserved. [Contact us](#)

Figure 3-87: IKE Log Screen

The IKE Log (Figure 3-87) is useful for troubleshooting the status of the IPSec IKE SA configuration.

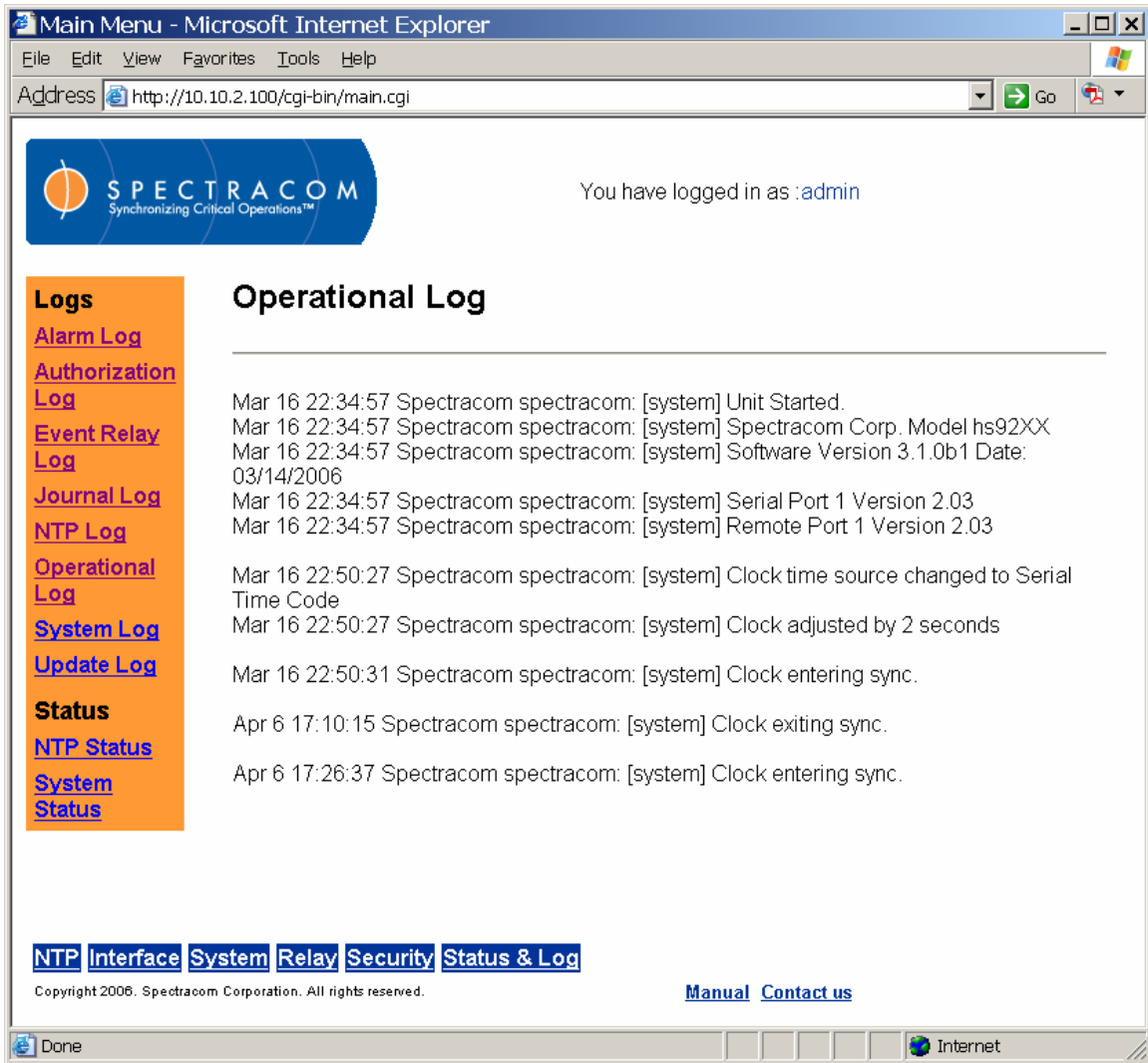


Figure 3-88: Operational Log Screen

The Operational Log (Figure 3-88) is a running list of NetClock operations, such as system updates and clock synchronizations.

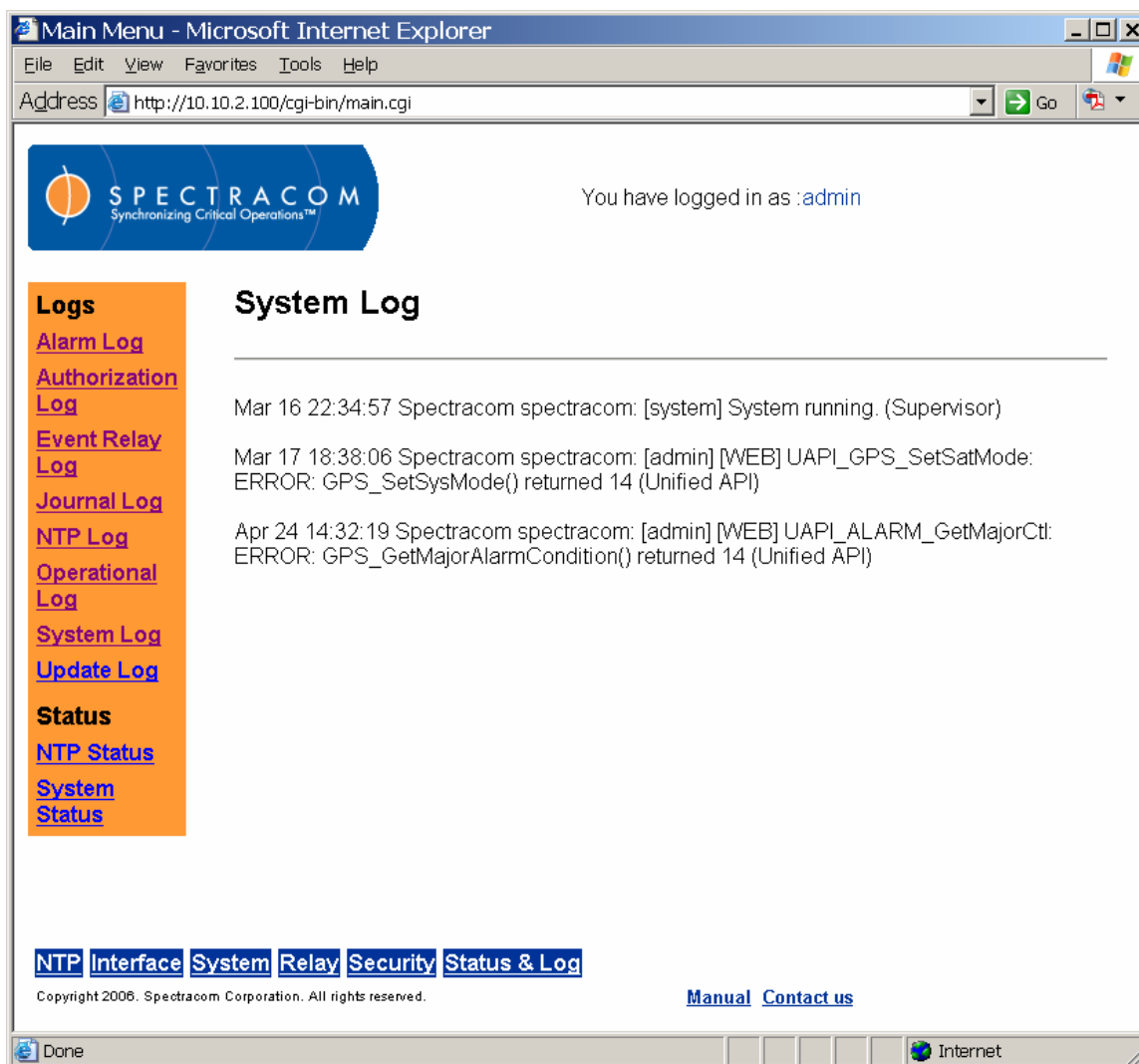


Figure 3-89: System Log Screen

The System Log (Figure 3-89) is a running list of system information and status messages that may be used by factory personnel for troubleshooting. This log records internal system information that is not intended for customer use.

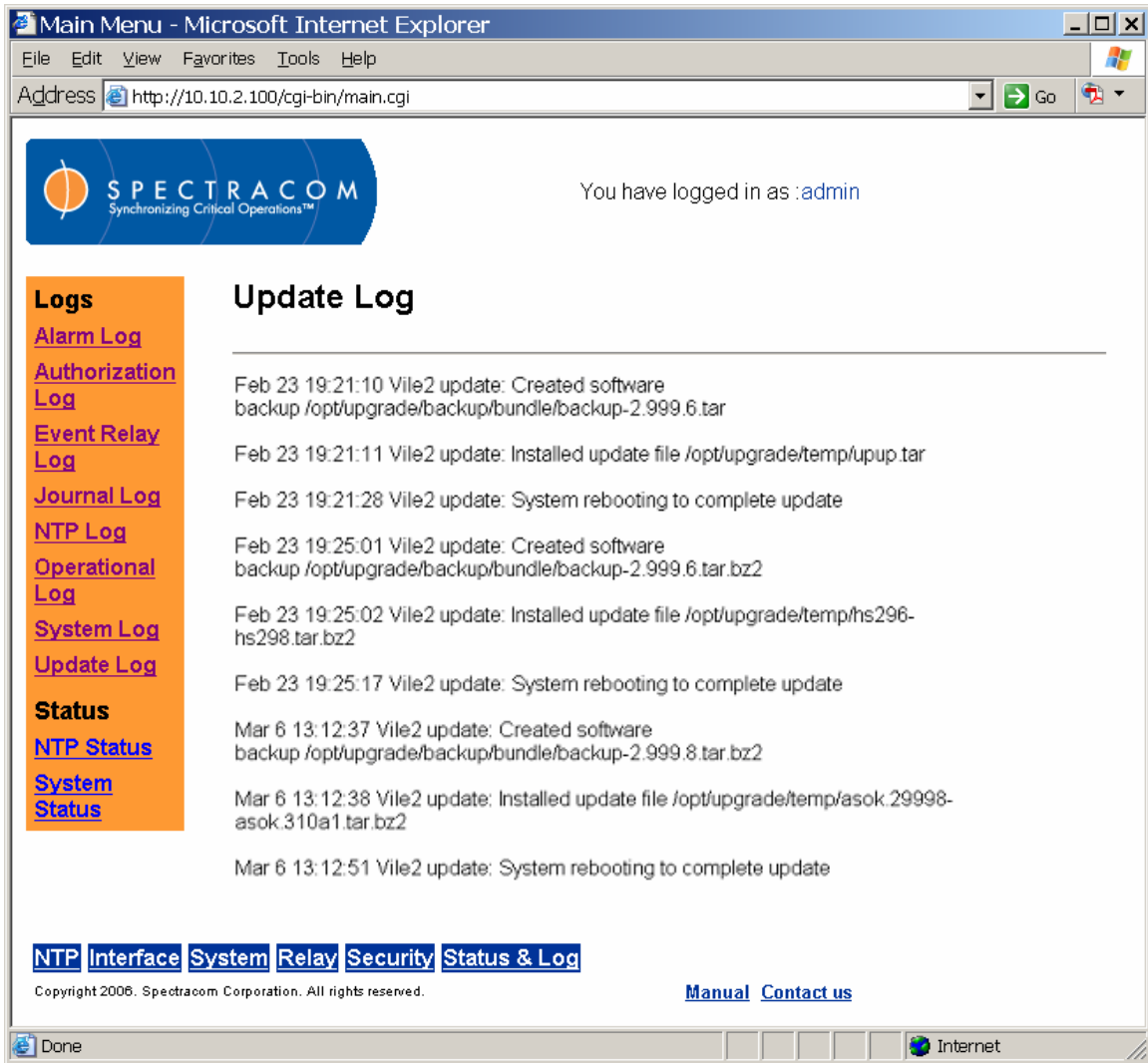


Figure 3-90: Update Log Screen

The Update Log (Figure 3-90) is a running list of software updates performed on the NetClock. Software updates are performed using a utility program provided by Spectracom.

The System Status screen (Figure 3-91) consists of four sections that provide the user with the software revision levels, the current time synchronization status, the results of internal unit testing, and the features and options that are currently enabled and disabled.

NOTE: The NTP Status screen is discussed in the *Configuring NTP* section of this manual.

Dynamic System Information

Uptime: 0 years, 38 days, 16 hours, 20 minutes, 13 seconds
Current internal temperature: 39.75 C (103.55 F)
Major Alarm is (OFF)
Minor Alarm is (OFF)
Time Sync status: In Sync
Time Source: Serial Time Code Input
NTP Service Status : In Sync (Stratum 1)

Static System Information

Product Name is Spectracom Corp. Model 9288
Application Name is hs92XX
Application Rev is 3.1.0b1
Application Date is 03/14/2006
SSH Rev is OpenSSH_4.1p1
SSL Rev is OpenSSL 0.9.7i-fips 14 Oct 2005
Unit's Serial Number: 115
MAC Address: 00:30:64:04:4a:85

System Test Results

PCB Test	PASSED (PCB rev. 0)
----------	---------------------

Navigation Menu: NTP | Interface | System | Relay | Security | Status & Log | Manual | Contact us

Copyright 2008. Spectracom Corporation. All rights reserved.

Figure 3-91: System Status Screen (1 of 2)

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 synchronization 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 Serial Time Code Input is the Primary Time Source for the Model 9288.

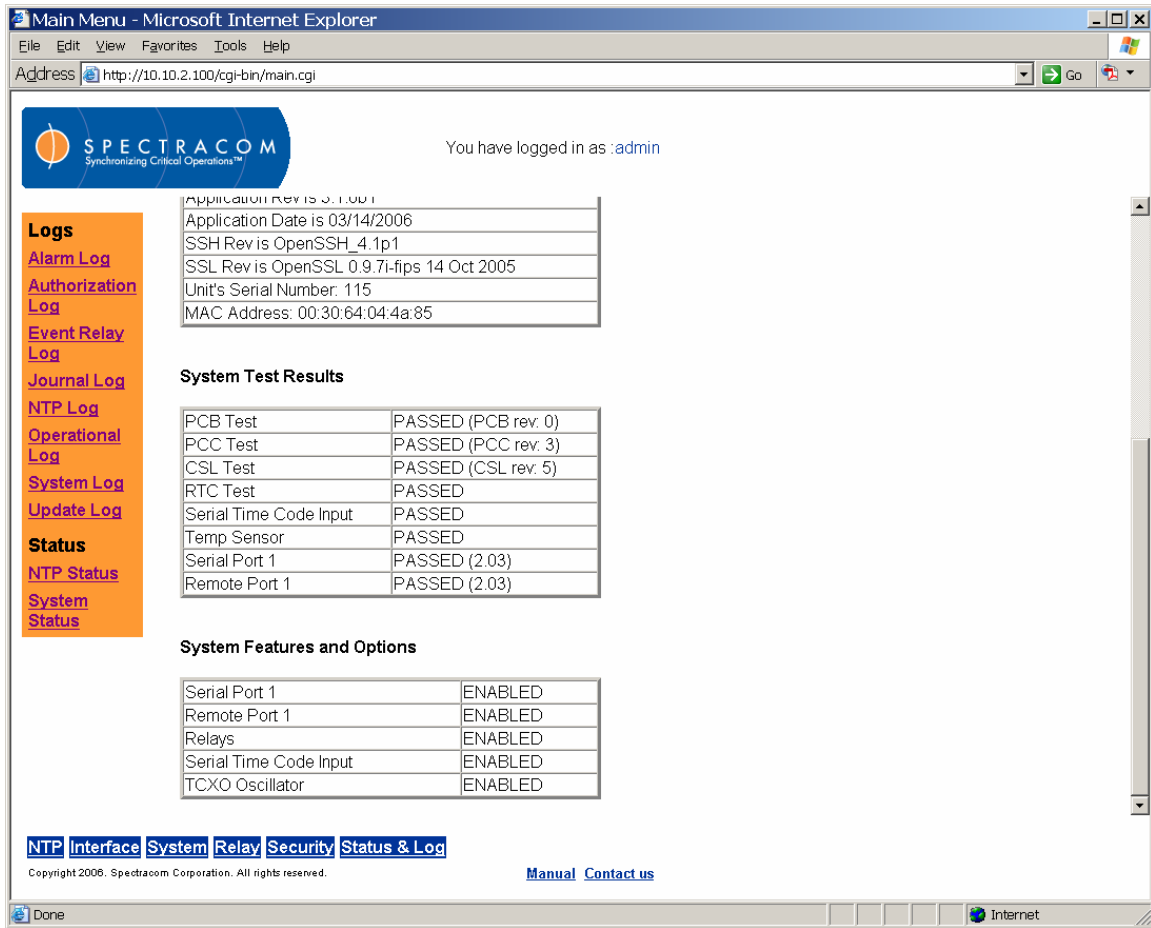


Figure 3-92: System Status Screen (2 of 2)

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.

The **Static System Information** section of the System Status screen provides the software revisions, the NetClock’s Serial Number, and the MAC address.

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

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

4 Operation

Operation of the 9200 series NetClock is relatively intuitive and requires little operator intervention during normal network operations.

4.1 Front Panel

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

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

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

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

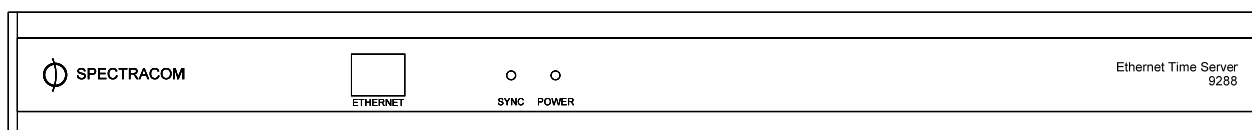


Figure 4-1: Front Panel

4.1.1 Status Indicator

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

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

Blink is defined as ½ second on, ½ second off

Flash is defined as 1/20 second on, 19/20 second off

LABEL	COLOR	ACTIVITY	DESCRIPTION
POWER	Green	On Off	Power is supplied to the NetClock. Power is disconnected.
SYNC	Multi	Off	No fault but not synchronized to GPS. Holdover spec has not been met.
		Green On	Synchronized to GPS. Time is valid and within the Locked to GPS accuracy specs.
		Blinking Green	Holdover mode. Not synchronized to GPS but time is still within Holdover accuracy specs. Also indicates the unit is synchronized with the optional dial-out modem (Option 03).
		Yellow On	No longer synchronized to GPS but no unit fault. Time accuracy may not be meeting holdover specs.
		Blinking Yellow	Unit is in power-up initialization mode. The unit is in this mode for the brief period between power on and when it is operationally ready to receive satellite data.
		Flashing Red	GPS antenna fault. This flash may occur over any of the other color conditions at runtime.
		Red On	Unit fault. Time may not be valid. Overrides all other indicators.
		Blinking Red	If the unit fails Power On Self Test (POST) then the indicator will blink in a sequence indicating the failure code (consult factory)
Ethernet (left)	Yellow	On Off	LAN Activity detected. No LAN traffic detected.
Ethernet (right)	Green	On Off	LAN Link established 10 or 100 Mb/s. No link established.

Table 4-1: Status Indicators

4.2 Rear Panel

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

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 add-on Model 9288 Ethernet Time Servers.

Remote Port 2 is an input port.

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

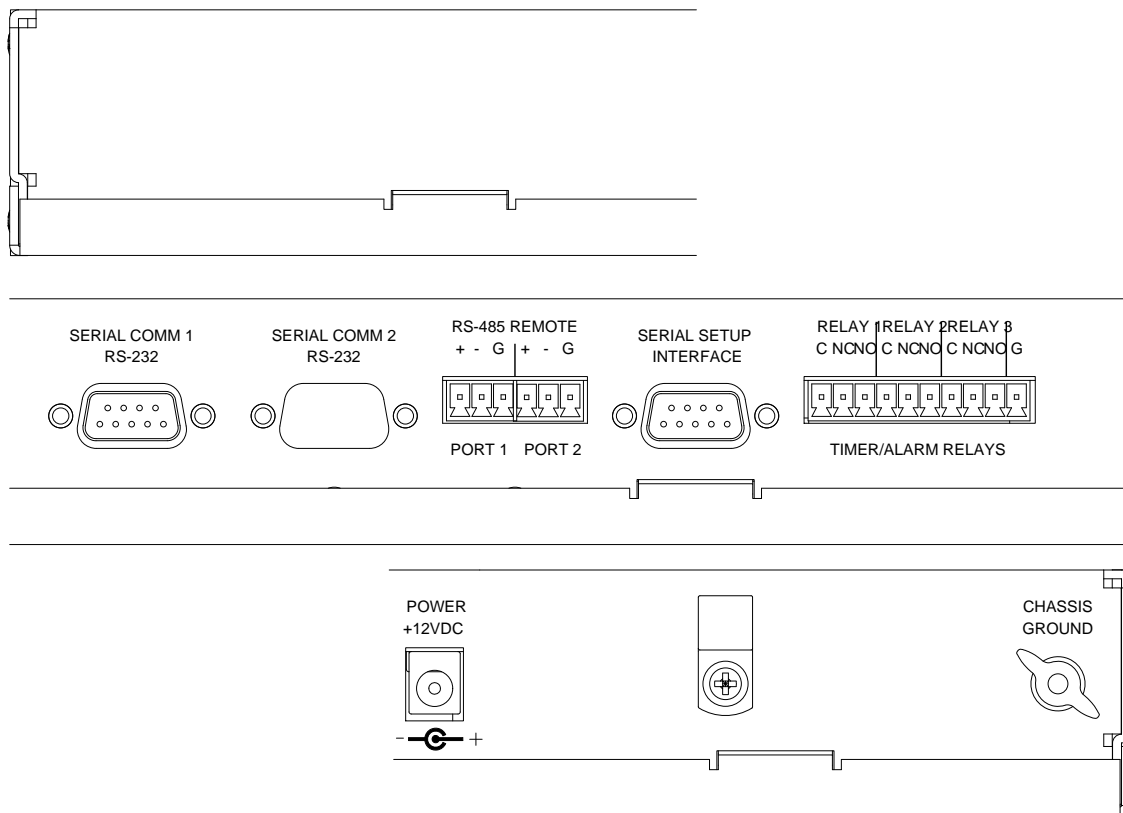


Figure 4-2: NetClock Rear Panel Detail

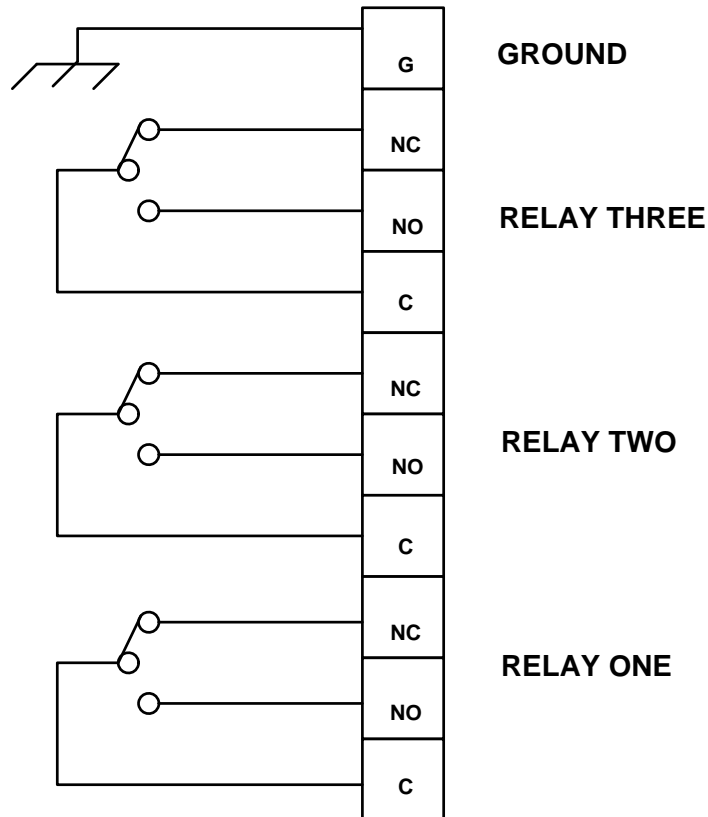
4.2.1 Event and Alarm Relay Outputs

The NetClock features three programmable relay outputs. The relays can be configured as major alarms, minor alarms, or events. They can control bells, whistles, sirens or other devices based on the event/alarm setup. Each event has an assigned start and stop time. An event can be scheduled for daily, monthly, or specific date occurrences.

An example of a daily event schedule is to sound the siren at the fire station at noon every day for five seconds. An example of a dated event is to schedule a test of the emergency evacuation horns on May 9th, 2007 from 10:00 AM to 10:05 AM.

The event timer is configured using the Web UI. Relays are configurable as events or alarm outputs. Refer to the appropriate configuration screens in Section 3 of this manual.

Event and alarm relay contacts are rated at 2.0 Amps, 30 VDC. The relays will be in the de-energized state (refer to Figure 4-3) when power is removed, when a major alarm is present and the relay is configured as a major alarm, or when an event is "on" and the relay is configured as an event output. The relay contacts can be referenced to ground by connecting to Pin G of the Alarm Outputs connector.



NOTE: Relays are shown in the de-energized state (event "off").

Figure 4-3: Event and Alarm Relay Contacts

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.

1. The NetClock can be alerted of impending leap seconds through the GPS receiver. The GPS satellite system transmits information regarding a Leap second adjustment at a specific Time and Date an arbitrary number of months in advance.

4.3.2 Leap Second Alert Notification

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

1. Data Formats 2 and 7 on the Serial and Remote Ports contain a Leap Second indicator. During the entire calendar month preceding a Leap Second adjustment, these Formats indicate that at the end of the current month a Leap Second Adjustment will be made by having a 'L' rather than a ' ' (space) character in the data stream. Note that 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 two Leap Indicator Bits. 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.

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

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

4.3.3 Sequence of a Leap Second Correction Being Applied

1. The following is the time output sequence that the Model 9288 will utilize to apply the Leap second at UTC midnight (Not local time midnight. The Local time at which the adjustment is made will depend on which Time Zone you are located in).

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

56, 57, 58, 59, 60, 0, 1, 2, 3, ...

B) Sequence of seconds output when removing Leap seconds:

56, 57, 58, 0, 1, 2, 3, 4, ...

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

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

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

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

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

5 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.

5.1 Format 0

Format 0 includes a time synchronization 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 Saving 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 synchronization status character I is defined as described below:

(Space) =	Whenever the front panel time synchronization lamp is green.
? =	When the receiver is unable to track any satellites and the time synchronization 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

5.2 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 synchronization 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 synchronization status character I is defined as described below:

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

Example: * FRI 20APR01 12:45:36

The example data stream provides the following information:

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

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

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

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

To change Data Format 1 output on a Serial port to a leading 0, type:

ser mod ser[1/2] 1 zero <enter>

(Where 1 or 2 is the desired Serial port number)

To change Data Format 1 output on a Remote RS-485 port to a leading 0, type:

rem mod rem[1/2] 1 zero <enter>

(Where 1 or 2 is the desired Remote port number).

To change Data Format 1 output on a Serial port back to a leading space, type:

Ser mod ser[1/2] none <enter>

(Where 1 or 2 is the desired Remote port number).

To change Data Format 1 output on a Remote RS-485 back to a leading space, type:

rem mod rem[1/2] none <enter>

(Where 1 or 2 is the desired Remote port number).

5.3 Format 2

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

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

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

where:

CR = Carriage Return
 LF = Line Feed
 I = Time Sync Status (space, ?, *)
 Q = Quality Indicator (space, A, B, C, D)

YY = Year without century (99, 00, 01 etc.)
 ^ = space separator
 DDD = Day of Year (001 - 366)
 HH = Hours (00-23 UTC time)
 : = Colon separator
 MM = Minutes (00-59)
 SS = Seconds (00-60)
 . = Decimal Separator
 SSS = Milliseconds (000-999)
 L = Leap Second Indicator (space, L)
 D = Daylight Saving Time Indicator (S,I,D,O)

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

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

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

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

Quality	Time (hours)	TCXO Error (Standard configuration) (milliseconds)
Space	Lock	<1
A	<10	<10
B	<100	<100
C	<500	<500
D	>500	>500

Table 5-1: 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.

5.4 Format 3

Format 3 provides a format identifier, time synchronization 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 synchronization status character I is defined as:

(Space) = Whenever the front panel time synchronization lamp is green.

? = When the receiver is unable to track any satellites and the time synchronization 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.

5.5 Format 4

Format 4 provides a format indicator, time synchronization 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 synchronization status character I is defined as:

(Space) = Whenever the front panel time synchronization lamp is green.

? = When the receiver is unable to track any satellites and the time synchronization 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.

5.6 Format 7

This format provides a time data stream with millisecond resolution. The Format 7 data stream consists of indicators for time synchronization 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:

NOTE: Format 7 cannot be configured for a Time Zone Offset or with automatic Daylight Saving Time adjustment. Attempting to configure a Local clock using Data Format 7 with either a Time Zone Offset or automatic DST rule will result in an error message.

CR LF I^YY^DDD^HH:MM:SS.SSSL^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 synchronization status character I is defined as described below:

(Space) = Whenever the front panel time synchronization lamp is green.
 ? = When the receiver is unable to track any satellites and the time synchronization 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.

5.7 Format 8

Format 8 includes a time synchronization 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 Saving 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 NetClock is synchronized to UTC source.

= * when the NetClock time is set manually.

= ? when the NetClock 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 Serial Setup Interface Commands

The NetClock can be configured using the serial setup interface port and a terminal emulation program as discussed in Section 3.2. At the Command Line Interface (CLI), the user can manage files and configure product settings.

The available CLI commands are as follows:

```
time      - time
reboot    - reboot [app]
log       - log COMMAND OBJECT [ HANDLE ]
option    - option COMMAND [OPTION | PRODUCT] [VALUE]
ltc       - ltc COMMAND [INDEX | NAME] [...]
net       - net COMMAND [Arguments]
sys       - sys COMMAND [Arguments]
ser       - ser COMMAND SERIAL [Arguments]
rem       - rem COMMAND REMOTE [Arguments]
frq       - frq COMMAND INDEX [Arguments]
```

One additional command, **help**, displays the available commands at the CLI. Typing **help** and a specific command (for example, **help time**, or **help option**) and then pressing the enter key displays detailed information about the command.

NOTE: Commands typed at the CLI are case-sensitive. All terms and commands entered must be lower-case.

6.1 time

```
help time
Use the 'time' command to read the current system date and time.
USAGE: time
```

6.2 reboot

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.

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/*.

```
help reboot
This command is used to immediately reboot a unit.
The 'app' option is used to restart the application. Normally the
unit reboots to the application, unless the optional parameter is
specified to 'bootloader' which it will reboot to the bootloader.
USAGE: reboot [app]
      app      - Reboot to application.
```

NOTE: 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.

6.3 log

help log

Use the 'log' command to access and manage the log system.

USAGE: log COMMAND OBJECT [HANDLE]

COMMAND

show - Shows the contents of a log.
get - Gets the record #[HANDLE] from a log.

OBJECT

j - Journal log
a - Alarm log
g - GPS qualification Log
o - Operational log
n - NTP log
r - Event relay log
t - Authorization log
u - Update log

HANDLE : Record number to access. The first record is 0.

6.4 option

help option

The 'option' commands provide a means to set, clear and display product configuration options.

USAGE: option COMMAND [OPTION | PRODUCT] [VALUE]

COMMAND

display - Displays current option settings.
enable - Enables options after verifying the hash value.

6.5 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.

help ltc

The 'ltc' group of commands are used to manage the local time clocks.

USAGE: ltc COMMAND [INDEX | NAME] [...]

COMMAND = {disp | create | delete | tz | dst}

disp - Displays information about the local clock.
create - Creates a new local clock. Multiple consecutive spaces in the name will be reduced to a single space
delete - Deletes a local clock at the specified index.
tz - Assigns a new time zone offset for the local clock.
dst - Assigns a new daylight saving rule to the clock.

6.6 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 admin level security in order to set or change them.

```
help net
```

The 'net' group of commands are used to manage network interface

```
USAGE: net COMMAND [Arguments]
```

```
COMMAND
```

```
    config    - Configure IP settings.
    show      - Displays network configurations.
    daytime   - Enable/disable Daytime.
    time      - Enable/disable UNIX time.
    telnet    - Enable/disable Telnet.
    ftp       - Enable/disable FTP
    http      - Enable/disable HTTP.
    https     - Enable/disable secure HTTP.
    ssh       - Enable/disable SSH.
```

6.7 sys

```
help sys
```

The sys group of commands are used to retrieve information about the system.

```
USAGE: sys COMMAND [Arguments]
```

```
COMMAND
```

```
    mem       - Display memory information. Use v for verbose mode.
```

6.8 ser

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

```
help ser
```

The ser group of commands are used to setup serial ports RS-232.

```
USAGE: ser COMMAND SERIAL [Arguments]
```

```
COMMAND
```

```
    disp      - Displays the current serial port settings.
    all       - Configures all settings of a serial port.
    fmt       - Configures the format of the serial port output.
    req       - Sets the request character on a serial port.
    ltc       - Sets the reference clock on the serial output.
               To add/configure local clocks, use command 'ltc'
    baud      - Configures the baud rate of a serial port.
```

6.9 rem

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

help rem

The rem group of commands are used to setup remote serial ports RS-485.

USAGE: rem COMMAND REMOTE [Arguments]

COMMAND

- disp - Displays the current remote serial port settings.
- all - Configures all settings of a remote serial port.
- fmt - Configures the format of the serial port output
- ltc - Sets the reference clock on the remote serial

output.

To add/configure local clocks, use command 'ltc'

- baud - Configures the baud rate of a remote serial port.

6.10 frq

help frq

The frq group of commands are used manage frequency interfaces.

USAGE: frq COMMAND INDEX [Arguments]

COMMAND

- mode - Sets the signature control mode.
- status - Displays the status of the selected frequency output.

7 Options

Spectracom offers no options for the Model 9288. Please contact our Sales department at US +1 585.321.5800 for information regarding additional features available in other Spectracom NetClock products.

Option	Description	9288
02	Front panel display & Second Serial Port/Remote Port	NO
03	Dial-Out Modem & ACTS Server	NO
04	Rb (Rubidium) Oscillator *	NO
05	OCXO Oscillator *	NO
06	IRIG Input	NO
08	SPS GPS Receiver	NO
09	TCXO Oscillator *	STANDARD

*Choose one oscillator only.

8 License Notices

This file is automatically generated from `html/copyright.htm`

Copyright Notice

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

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

```
*****
* Copyright (c) David L. Mills 1992-2001
*
* Permission to use, copy, modify, and distribute this software and
* its documentation for any purpose and without fee is hereby
* granted, provided that the above copyright notice appears in all
* copies and that both the copyright notice and this permission
* notice appear in supporting documentation, and that the name
* University of Delaware not be used in advertising or publicity
* pertaining to distribution of the software without specific,
* written prior permission. The University of Delaware makes no
* representations about the suitability this software for any
* purpose. It is provided "as is" without express or implied
* warranty.
*****
```

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

1. [1]Mark Andrews <marka@syd.dms.csiro.au> Leitch atomic clock controller
 2. [2]Bernd Altmeier <altmeier@atsoft.de> hopf Elektronik serial line and PCI-bus devices
 3. [3]Vira] Baiz <vbais@mailman1.intel.com> and [4]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
 4. [5]Michael Barone <michael.barone@lmco.com> GPSVME fixes
 5. [6]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
 6. [7]Greg Brackley <greg.brackley@bigfoot.com> Major rework of port. Clean up recvbuf and iosomal code into separate modules.
 7. [8]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
 8. [9]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
 9. [10]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
 10. [11]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
 11. [12]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
 12. [13]Sven Dietrich <sven.dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port
 13. [14]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
 14. [15]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
 15. [16]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
 16. [17]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
 17. [18]Mike Iglesias <mike@uuc.uuc.edu> DEC Alpha port
 18. [19]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
 19. [20]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
 20. [21]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [22]H.Lambermont@chello.nl> ntpswep
 21. [23]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
 22. [24]Frank Kardel [25]Frank.Kardel@informatik.uni-erlangen.de> PARSE <GENERIC> driver (14 reference clocks), STREAMS modules
- for
23. [26]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HP-UX modifications
 24. [27]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
 25. [28]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
 26. [29]George Lindholm <lindholm@uuc.ubc.ca> SunOS 5.1 port
 27. [30]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
 28. [31]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
 29. [32]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbitr, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
 30. [33]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
 31. [34]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
 32. [35]Tom Moore <tmoore@fievvel.daytonoh.ncr.com> 1386 svr4 port
 33. [36]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
 34. [37]Derek Mulcahy <derek@toybox.demon.co.uk> and [38]Damon Hart-Davis <dhd.org> ARCON MSF clock driver
 35. [39]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
 36. [40]Dirce Richards <dirce@z3k3.dec.com> Digital UNIX V4.0 port
 37. [41]Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
 38. [42]Nick Sayer <nrapple@quack.kfu.com> SunOS streams modules
 39. [43]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the `html/pic/` subdirectory
 40. [44]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
 41. [45]Michael Shields <shields@tembel.org> USNO clock driver
 42. [46]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
 43. [47]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the `ChangeLog`)
 44. [48]Kenneth Stone <ken@sdd.hp.com> HP-UX port

45. [49]Ajit Thyagarajan <ajit@ee.udel.edu> IP multicast/anycast support
46. [50]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp> TRAK clock driver
47. [51]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
48. [52]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

[53]gif

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

References

1. <mailto:marka@syd.dms.csiro.au>
2. <mailto:altmeier@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:Piete.Brooks@cl.cam.ac.uk>
10. <mailto:reg@dwf.com>
11. <mailto:clift@ml.csiro.au>
12. <mailto:casey@csc.co.za>
13. <mailto:Sven.Dietrich@trimble.COM>
14. <mailto:dundas@salt.jpl.nasa.gov>
15. <mailto:duwe@immd4.informatik.uni-erlangen.de>
16. <mailto:dennis@mrbill.canet.ca>
17. <mailto:glen@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@uuc.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@fievvel.daytonoh.ncr.com>
36. <mailto:kamal@whence.com>
37. <mailto:derek@toybox.demon.co.uk>
38. <mailto:dhd.org>
39. <mailto:Rainer.Pruy@informatik.uni-erlangen.de>
40. <mailto:dirce@z3k3.dec.com>
41. <mailto:wsanchez@apple.com>
42. <mailto:mrapple@quack.kfu.com>
43. <mailto:jack@innovativeinternet.com>
44. <mailto:schnitz@unipress.com>
45. <mailto:shields@tembel.org>
46. <mailto:pebbles.jpl.nasa.gov>
47. <mailto:harlan@pfcs.com>
48. <mailto:ken@sdd.hp.com>
49. <mailto:ajit@ee.udel.edu>
50. <mailto:tsuruoka@nc.fukuoka-u.ac.jp>
51. <mailto:vixie@vix.com>
52. <mailto:Ulrich.Windl@rz.uni-regensburg.de>
53. <file://localhost/backroom/ntp-stable/html/index.htm>
54. <mailto:mills@udel.edu>

This file is part of the OpenSSH software.

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

OpenSSH contains no GPL code.

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

[Tatu continues]

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

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

- RSA is no longer included, found in the OpenSSL library

```

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

[The licence continues]

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

The legal status of this program is some combination of all these
permissions and restrictions. Use only at your own responsibility.
You will be responsible for any legal consequences yourself; I am
not
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:

* 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

REVISION HISTORY

<i>Revision Level</i>	<i>ECN</i>	<i>Description</i>
A	—	Revision A was the first-generation manual for the 9200 series products.
B	—	<i>RS-485 Output</i> section changed to <i>RS-485 Input/Output</i> . Corrected labeling and language of RS-485 Remote Port. Corrected language in <i>Serial Comm Ports</i> section and removed references to Option 02, which is not available on 9288 units. Replaced <i>System Holdover</i> screen. Removed accuracy specification in <i>Protocols Supported</i> section. Replaced <i>System Time</i> screen. Removed <i>Format 90</i> section, which does not apply. Removed several other references to GPS and modem, which do not apply.
C	2027	Added note concerning screens shown in <i>Configuration</i> . Edited <i>Configuring Network Security</i> to correct for changes in SSH and remove references to SSH1 protocol (which is not supported). Added <i>Sysplex Timing</i> section before <i>Configuring the Interface: SNMP</i> . Updated System Log Configuration screen.
D	2081	Notable changes include statements for UL earthing in Installation, UL disclaimer after the Table of Contents, and some minor corrections to sections 5.2 and 5.6 for content errors. Added IPsec material, FTP Statistics material. "Log clear" command has been removed.
E	2156	Revision to bring manual current to 3.4.0 NetClock software. Changes include adding HALT information in System Configuration, revising NTP section, and adding product configuration/options table.
F	2210	Clarified regions for Australia-1 and Australia-2 DST rules. Added note concerning Serial Time Code Setup year change update.

Spectracom Corporation

95 Methodist Hill Drive

Rochester, NY 14623

www.spectracomcorp.com

Phone: US +1.585.321.5800

Fax: US +1.585.321.5219