NetClock® 9400 Series
INSTRUCTION MANUAL

1565 Jefferson Road
Rochester, NY 14623
Phone: US +1.585.321.5800
Fax: US +1.585.321.5219

spectracom

www.spectracomcorp.com
Part Number 1209-5000-0050
Rev. G
February 2014

SPECTRACOM LIMITED WARRANTY

Five Year Limited Warranty
Spectracom, a business of the Orolia Group, warrants each new standard product to be free from defects in material, and workmanship for five years after shipment in most countries where these products are sold, EXCEPT AS NOTED BELOW (the "Warranty Period" and "Country Variances").

Warranty Exceptions
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, or repairs or modifications not performed by Spectracom authorized personnel.

Items with a variance to the Five Year Warranty Period are as follows:

90 Days Warranty
TimeKeeper Software

One Year Limited Warranty
Timeview Analog Clock
Path Align-R Products
Bus-level Timing Boards
IRIG-B Distribution Amplifiers

Two Year Limited Warranty
Rubidium Oscillators
Epsilon Board EBO3
Epsilon Clock 1S, 2S/2T, 3S, 31M
Epsilon SSU
Power Adaptors
Digital and IP/POE Clocks
WiSync Wireless Clock Systems and IPSync IP Clocks
Rapco 1804, 2804, 186x, 187x, 188x, 189x, 2016, 900 series

Three Year Limited Warranty
Pendulum Test & Measurement Products GPS-12R, CNT-9x, 6688/6689, GPS-88/89, DA-35/36, GPS/GNSS Simulators

Country Variances
All Spectracom products sold in India have a one year warranty.

Warranty Exclusions
Batteries, fuses, or other material contained in a product normally consumed in operation Shipping and handling, labor & service fees EXCEPT FOR THE LIMITED WARRANTY STATED ABOVE, SPECTRACOM DISCLAIMS ALL WARRANTIES OF ANY KIND WITH REGARD TO SPECTRACOM PRODUCTS OR OTHER MATERIALS PROVIDED BY SPECTRACOM, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

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

Warranty Claims
Spectracom's obligation under this warranty is limited to the cost of in-factory repair or replacement, at Spectracom's option, of the defective product or the product's defective component. Spectracom's Warranty does not cover any costs for installation, reinstallation, removal or shipping and handling costs of any warranted product. If in Spectracom's sole judgment, the defect is not covered by the Spectracom Limited Warranty, unless notified to the contrary in advance by customer, Spectracom will make the repairs or replace components and charge its then current price, which the customer agrees to pay.

In all cases, the customer is responsible for all shipping and handling expenses in returning product to Spectracom for repair or evaluation. Spectracom will pay for standard return shipment via common carrier. Expediting or special delivery fees will be the responsibility of the customer.

Warranty Procedure
Spectracom highly recommends that prior to returning equipment for service work, our technical support department be contacted to provide troubleshooting 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.

Spectracom shall not have any warranty obligations if the procedure for warranty claims is not followed. Customer must notify Spectracom of a claim, with complete information regarding the claimed defect. A Return Authorization (RMA) Number issued by Spectracom is required for all returns.

Returned products must be returned with a description of the claimed defect, the RMA number, and the name and contact information of the individual to be contacted if additional information is required by Spectracom. Products being returned on an RMA must be properly packaged with transportation charges prepaid.

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

Contents

List of Figures

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.

Section 1: NetClock 9400 Series

The NetClock® 9400 Series combines Spectracom's precision Time Server / master clock technology and secure network-centric approach with a compact modular hardware design to bring you a powerful time & frequency reference and synchronization system at the lowest cost of ownership.

1.1 Introduction

The NetClock 9400 product series is ideally suited for a variety of communications applications such as Emergency Communications Centers that require extremely accurate timing and frequency synchronization for their mission-critical systems, networks, and devices. The NetClock 9400 product series consists of two variants: the model 9483 is fully compliant with the National Emergency Number Association (NENA) master clock standard, and the model 9489.

1.2 NetClock 9483

The NetClock 9483 has been designed specifically for these environments, and when using GPS as its timing reference, the UTC (Coordinated Universal Time) time standard is employed, thus allowing the NetClock 9483 to provide legally traceable time and frequency synchronization services for various related environments and equipment, such as the following:

- 9-1-1 and PSAP communication center telephony
- Computer network synchronization
- VOIP / voice and video recording
- CAD
- ANI / ALI controllers
- Radio consoles and communications equipment
- Display clocks
- Security & building access systems, fire alarm systems

The NetClock 9483 also includes backwards-compatibility support with all previous generation NetClock products; thus providing a bridge from legacy devices and equipment to network-based systems.

The NetClock 9483 series is a truly flexible Time Server / master clock, which in addition to providing highly accurate network time synchronization, also supports a variety of timecodes (including all NENA formats) and signals to synchronize specific devices. The built-in network port can be supplemented to include 3 additional Gigabit Ethernet (10/100/1000Base-T) ports for synchronizing isolated networks, or for restricting administration to a specific management network. Precise 10 MHz and 1 Pulse-per second (1PPS) signals are standard features, and additional optional features include support for T1/E1 signals are available for synchronizing telecom systems and equipment, and Precision Timing Protocol (PTP) I/O support.

The unit is housed in a 19" rack unit chassis and offers an integrated power supply. DC power is available as back-up to AC power, or as the primary input power source.

NOTE: *All features described are not available on all NetClock 9400 Series variants.*

Initial setup of the NetClock 9483 can be performed via its front panel serial port interface, and further management and configuration can be performed via the NetClock's Web-based user interface.

1.2.1 NENA Standards Compliance & Support

The NetClock Model 9483 is designed to meet or exceed the following NENA standards and criteria:

- NENA PSAP Master Clock Standard #04-002
- NENA Security for Next-Generation 9-1-1 Standard (NG-SEC) #75-001

NOTE: Information regarding the configuration of the NetClock's NENA module can be found in Section *8.1*: *NENA-Compliant Option Module*.

1.2.2 Security Enhancements

In addition to fully supporting the NENA Security Standard #75-001, the NetClock 9400 series are security-hardened network appliances designed to meet rigorous network security standards and best practices. They ensure accurate timing through multiple references, tamper-proof management, and include extensive logging capabilities for auditing purposes. All features, interfaces, ports, and protocols can be enabled or disabled based on your network policies.

1.3 NetClock 9489

Spectracom's NetClock Model 9489 delivers the same high precision timing benefits of the NetClock 9483, and is ideally suited for delivering highly precise NTP timing for synchronizing systems, devices, and other communications equipment and devices.

In addition to providing a secure, high precision NTP platform, the NetClock 9489 also provides a (1) 1PPS output, and two RS-485 outputs.

NOTE: There are a number of commonly shared features between both the NetClock 9483 and 9489 models. However, the NetClock Model 9489 is designed to function primarily as an NTP server, and therefore is somewhat less complex than the NetClock Model 9483. As such, a majority of this document applies to the NetClock Model 9483, except where otherwise noted.

1.4 Inputs and Outputs: What Can NetClock Do for You?

Spectracom NetClock provides multiple outputs for use in networked systems and devices. GPS-equipped NetClocks can track up to thirty-two GPS satellites simultaneously and synchronize to the satellite's atomic clocks. This enables NetClock-equipped computer networks to synchronize all elements of network hardware and software over LANs or WANs – anywhere on the planet.

1.4.1 NetClock 9483 Standard Outputs

Standard outputs include the following:

Type	Connector
(1) Ethernet 10/100Base-T	RJ-45 (auto-sensing)
(1) RS-232 Serial Connector	DB9 female
(1) RS-485 Once-per-Second	3.81mm Terminal Block
(1) IRIG B/E, IEEE 1344/C37.118-2005 (AM/TTL) output	BNC
(1) 1 Pulse Per Second (1PPS) output	BNC
(1) 10 MHz Frequency output	BNC
(2) Relay / Alarm Outputs	3.81mm Terminal Block

1.4.2 NetClock 9483 Optional Outputs

Several additional option modules are available to provide specific or enhanced functionality for your NetClock product:

Type	Connector
(3) 10/100/1000Base-T Multi-Ethernet	RJ-45 (auto-sensing)
T1/E1 Balanced (1) 1.544 or 2.048 MHz (2) 1.544 or 2.048 MHz	3.81mm Terminal Block
(1) PTP (Precision Timing Protocol / IEEE 1588)	RJ-45

For more information, refer to *Section 8:* "*NetClock 9483 Option Modules*".

1.4.3 NetClock 9489 Standard Outputs

Standard outputs include the following:

Type	Connector
(1) Ethernet 10/100Base-T	RJ-45 (auto-sensing)
(1) 1 Pulse Per Second (1PPS) output	BNC
(2) RS-485 Once-per-Second	3.81mm Terminal Block

1.5 NetClock 9400 Series Front Panels

1.5.1 NetClock 9483 Front Panel

The front panel of the NetClock 9483 unit consists of the following:

- Three status LED indicator lights (“Power”, “Sync” and “Fault”). Refer to Section 1.7: “NetClock 9400 Series Front Panel LED Status Indicator Lights” for additional information.
- Keypad buttons, for performing operations from the front panel.
- LCD display, showing status information or currently selected menu items (display options are configurable via the product web interface, such as position information, time and date, Day of Year, GPS information, network settings, etc.).
- LED time display.
- An RS-232 serial port interface for serial cable connections.

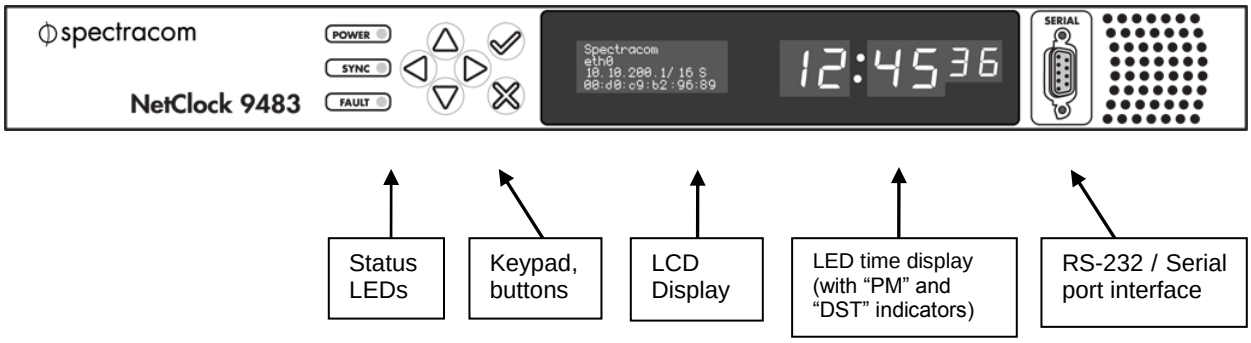


Figure 1-1: NetClock 9483 Series Front Panel Display

1.5.2 NetClock 9489 Front Panel

The front panel of the NetClock 9489 unit consists of the following:

- Three status LED indicator lights (“Power”, “Sync” and “Fault”). Refer to Section 1.7: “NetClock 9400 Series Front Panel LED Status Indicator Lights” for additional information.
- An RS-232 Serial port interface connection.

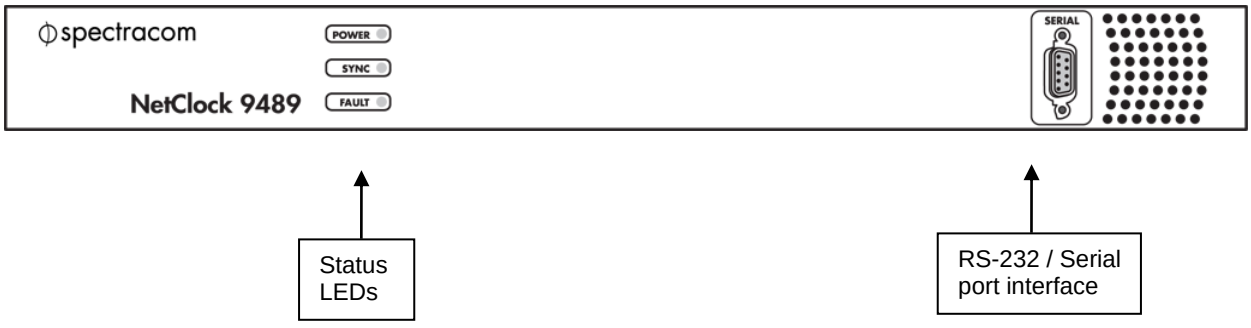


Figure 1-2: NetClock 9489 Front Panel

1.6 NetClock 9400 Series Rear Panels

1.6.1 NetClock 9483 Rear Panel

The NetClock 9483 rear panel provides several different outputs for interfacing the unit to various systems. The rear panel has an AC connection for power input (DC Power optional), Ethernet and USB connections, 1PPS and 10MHz outputs, IRIG and Relay / Alarm outputs, and GPS Antenna connector. Additional details are provided in this section.

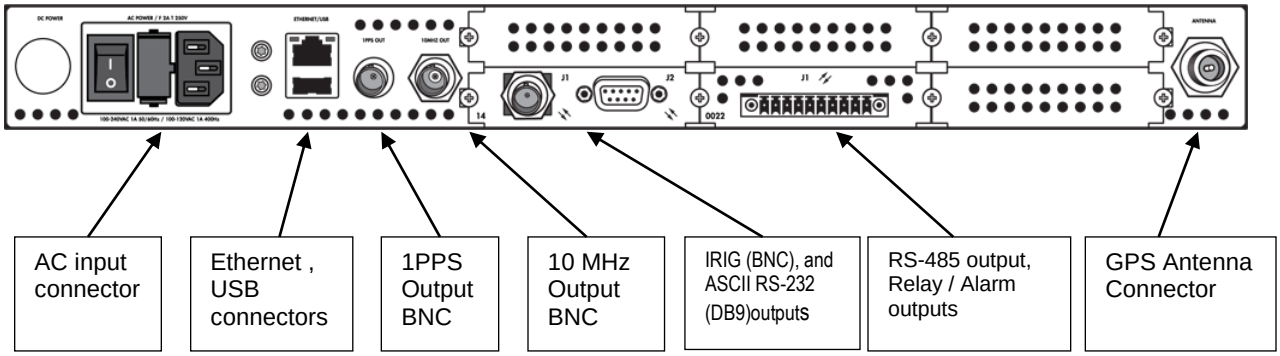


Figure 1-3: NetClock 9483 Rear Panel

- **AC Power** connector: Input for the AC power and provides and AC power ON/OFF switch. This connector is only installed if NetClock was ordered with AC input power option.
- **DC Power** port connector: Only installed if the NetClock was ordered with DC input power option. Note: DC input power does not have an ON/OFF switch.
- **Ethernet** connector: Provides an interface to the network for NTP synchronization and to obtain access to the NetClock product web interface for system management. It has two small indicator lamps, “Good Link” (green LED), and “Activity” (orange LED). The “Good Link” link light indicates a connection to the network is present. The “Activity” link light will illuminate when network traffic is detected.

Ethernet	Yellow	On Off	LAN Activity detected. No LAN traffic detected.
Ethernet	Green	On Off	LAN Link established, 10 or 100 Mb/s. No link established.

Table 1-1: Status Indicators, Rear Panel

- **USB connector** is reserved for future expansion.
- **1PPS Output**: Provides a once-per-second square-wave output via BNC output connector. The 1PPS output can be configured to have either the rising or falling edge of the signal to be coincident with the system’s on-time point.
- **10 MHz Output**: Provides a 10 MHz sine-wave output via BNC output connector.
- **IRIG Output**: Supports IRIG A/B/G/E, IEEE 1344/C37.118-2005 (AM/TTL).
- **RS-232 Output**: for serial connections.
- **Relay / Alarm** outputs.
- **RS-485** output for serial connection.

- **GPS Antenna** connector: GPS input for GPS antenna and coax cabling (type "N" connector).

The **four option module bays** are designated as **Slot 1** - **Slot 4**, as displayed in the following figure:

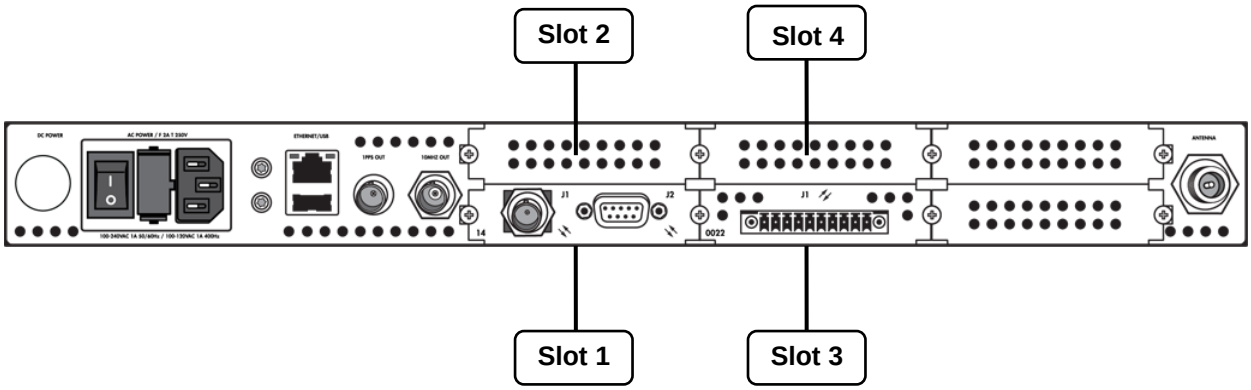
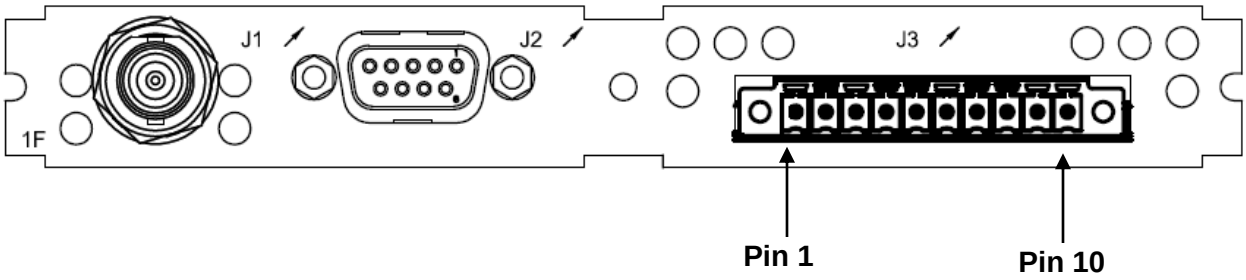


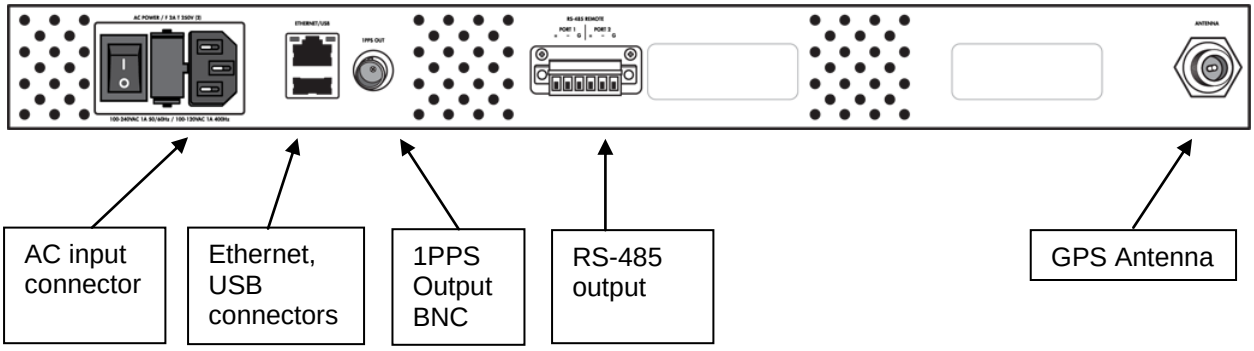
Figure 1-4: NetClock 9483 Rear Panel

NOTE: Pin numbers for the RS-485 outputs are defined starting with Pin 1 to Pin 10, arranged from left to right, as shown below:



1.6.2 NetClock 9489 Rear Panel

The NetClock 9489 rear panel provides an AC connection for power input, an Ethernet port, (1) 1PPS output, (2) RS-485 outputs, and GPS Antenna connector.



NOTE: Details on these features are identical to the NetClock 9483; therefore you may refer to the NetClock 9483 Rear Panel section for additional information if needed.

1.7 NetClock 9400 Series Front Panel LED Status Indicator Lights

Power: Green, always on.
Sync: Tri-color LED indicates the time data accuracy.
Fault: Indicates equipment fault.

The front panel LED status lights ("Power", "Sync", and "Fault") indicate whether the NetClock is synchronized, whether power is applied to the unit, and if any alarms are currently asserted. At power up, a quick LED test is run which illuminates all three LEDs. The Power LED light will not be lit if power is not applied. It will indicate green if power is applied. The Sync and Fault lights have multiple states.

Refer to the following table for an overview of the LED status indicator lights:

Label	Activity / Color	Description
Power	Off	Both AC and DC Input Power are disconnected. Or, NetClock's AC input switch is turned off and DC input is not present.
	On / Solid Green	AC and/or DC Power are supplied, NetClock detects all power inputs as present
	Orange	NetClock 9483 detecting only one of its possible power inputs, NetClock 9489 detecting a power configuration error.
	Green, but blinking Orange once per second	Indicates power error condition; general power configuration fault.
Sync	Red	Time Sync alarm. 1) NetClock has powered up and has not yet achieved synchronization with its inputs. 2) NetClock was synchronized to its selected input references, but has since lost all available inputs (or the inputs were declared invalid) and the Holdover period has since expired.
	Solid green	NetClock has valid time and 1PPS reference inputs present and is synchronized to its reference.
	Orange	In Holdover mode. NetClock was synchronized to its selected input references, but has since lost all available inputs (or the inputs are not declared valid). NetClock's outputs will remain useable until at least the Holdover period expires.
Fault	Off	No alarm conditions are currently active.
	Blinking orange	GPS antenna problem alarm has been asserted and is currently active. A short or open has been detected in the GPS antenna cable. The light will automatically turn off when the alarm condition clears (Refer to Section *10.1* for troubleshooting this condition).
	Solid orange	A Minor alarm condition (other than an antenna problem alarm) has been asserted and is currently active (Refer to Section *10.1.2*:"*Fault light - Minor Alarm*" for troubleshooting this condition). Possible causes include NetClock 9483 detects only one of its possible power inputs.

	Red	A Major alarm condition has been asserted and is currently active (Refer to Section *10.1.1*:"*Fault Light - Major Alarm*" for troubleshooting this condition).

Table 1-2: NetClock Front Panel LED Status Indicator Lights

1.8 Technical and Customer Support

If you require assistance with the configuration or operation of your product, or have questions or issues that cannot be resolved using the information in this document, please contact Spectracom Technical & Customer Support at either our North American or European service centers, or visit the Spectracom website at www.spectracomcorp.com.

NOTE: Premium Support Customers can refer to their service contracts for emergency 24-hour support.

North America		
Phone	+1 585.321.5800	
email	techsupport@spectracom.orolia.com	
Europe		
France		**United Kingdom**
Phone	+33 (0)1 6453 3980	44 (0)1256 303630
email	techsupport-france@spectracom.orolia.com	techsupport@spectracom.co.uk

Also visit Spectracom's website for general product information, Application and Technical Notes, notices regarding the availability of software updates for your products, and more.

1.8.1 Return Shipments

Please contact Customer Service before returning any equipment to 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.

1.9 Specifications

NOTE: The specifications listed herein are for the "base" NetClock 9483 unit (not including option modules or other options chosen at the time of purchase), except where otherwise noted, and are based on "standard" operation, with NetClock synchronized to valid Time and 1PPS input references (in the case of GPS input, this is with the GPS receiver operating in Stationary mode). Specifications for the available option modules are provided in Section **1.10*: "*NetClock 9483 Available Option Modules***".

1.9.1 GNSS Receiver

Standard Receiver:	GPS L1 C/A Code transmitted at 1575.42 MHz GLONASS L1 transmitted centered at 1602.0 MHz
Satellites Tracked:	Up to 32 simultaneously.
Acquisition Time:	Typically <4 minutes from a cold start.
Antenna Requirements:	Active antenna module, +5V, powered by the NetClock unit, 16 dB gain minimum.
Antenna Connector:	Type N, female.

1.9.2 RS-232 Serial Port (NetClock 9483 Only)

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

1.9.3 RS-485 Serial Port

Output:	(1) Output
Signal Type and Connector:	(1) RS-485 terminal block
Accuracy:	+/- 100-1000 microseconds (format dependant)

1.9.4 10/100 Ethernet Port

Function:	10/100 Base-T auto-sensing LAN connection for NTP / SNTP and remote monitoring, diagnostics, configuration and upgrade.
Connector:	RJ-45, Network IEEE 802.3.

1.9.5 IRIG Output (NetClock 9483 Only)

Outputs:	(1) IRIG Output
Signal Type and Connector:	IRIG A, B, G, E, NASA 36, Amplitude Modulated (0v to 5v peak to peak into 50 Ω on BNC) or DC Level Shift (unmodulated), user selectable.
Accuracy:	+/- 2 to 200 microseconds (IRIG Format dependant)

1.9.6 Protocols Supported

NTP:	NTP v4.2.6p5. Provides MD5 and Autokey, Stratum 1 or higher (RFCs 5905).
Loading:	~7,000 NTP 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:	For browser-based administration, configuration and monitoring using Internet Explorer 7 or higher with JavaScript support, Mozilla Firefox 3 or higher (per RFCs 1945 and 2068), with JavaScript support.
FTP / SFTP:	For secure remote upload of system logs and files (RFC 959).
Syslog:	Provides remote log storage (RFCs 3164 and 5424).
SNMP:	Supports v1, v2c, and v3.
Telnet / SSH:	For limited remote configuration.
Security Features:	Up to 32-character password, Telnet Disable, FTP Disable, Secure SNMP, SNMP Disable, HTTP/HTTPS Disable, SCP, SSH, SFTP.
Authentication:	LDAP v2 and v3, RADIUS, MD5 Passwords, NTP Autokey Protocol.

1.9.7 1PPS Output

Signal:	One pulse-per-second square wave.
Signal Level:	TTL compatible, 4.3 V minimum, base-to-peak into 50 Ω.
Pulse Width:	Configurable Pulse Width (200 milliseconds by default).
Pulse Width Range:	20 – 900 nanoseconds
Rise Time:	<10ns
Accuracy:	Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference.
Connector:	BNC Female
Signature Control:	Positive edge within ± 50 nanoseconds of UTC when locked to a valid 1PPS input reference.

1.9.8 10 MHz Output (NetClock 9483 Only)

Signal:	10 MHz sinewave.
Signal Level:	+13 dBm +/- 2dB into 50 Ω.
Harmonics:	-40 dBc minimum.
Spurious:	-70 dBc minimum TCXO
Oscillator Types & Accuracy:	**TCXO:** $1x10^{-11}$ over 24 hours to GPS, $1x10^{-8}$ aging/day, 450 usec 1PPS holdover in 24 hours
	OCXO: $2x10^{-12}$ over 24 hours to GPS, $5x10^{-10}$ aging/day, 25 usec 1PPS holdover in 30 days
	Rb (Rubidium): $1x1^{-12}$ over 24 hours to GPS, $5x10^{-11}$ aging/month, ($3x10^{-11}$ aging/month typical), 2 usec 1PPS holdover in 24 hours, 100 usec 1PPS holdover in 30 days, 10 msec 1PPS holdover in 1 year
Connector:	BNC Female
Signature Control:	This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output is restored when the fault condition is corrected.

1.9.9 Input Power

AC Power Source:	100 to 240 VAC, 50/60 Hz, +/- 10% and 100-120 VAC 400 Hz, +/- 10% via an IEC 60320 connector (power cord included).
DC Input (Option):	12-17VDC -15%, +20% or 21-60 VDC -15%, +20%, secure locking device. **Note:** No DC power option is available for the NetClock Model 9489.
Maximum Power Draw:	OCXO oscillator installed - 40W normal (50W start-up) Rubidium (Rb) oscillator installed - 50W normal (80W start-up)

1.9.10 Mechanical and Environmental

Dimensions:	Designed for EIA 19” rack mount 16.75” W x 1.72” H [1U] x 14.00” D actual (425 mm W x 44 mm H x 356 mm D) actual
Weight:	6.0 lbs (2.72 kg) 6.5 lbs. (2.95 kg) with Rubidium Oscillator option
Temperature:	0°C to 50°C operating range + 55°C for Rubidium option (NetClock 9483 only) -40° to 85°C storage range
Humidity:	10% - 95% relative humidity, non-condensing @ 40°C
Altitude:	100-240VAC - 6,560 ft (2000 m) operating range 100-120VAC - 13,123 ft (4000 m) operating range 45000ft (13700 m) storage range
Shock:	15g/0.53 oz, 11ms, half sine wave operating range 50g/1.76 oz, 11ms, half sine storage range
Vibration:	10-55Hz/0.07g, 55-500Hz/1.0g operating range 10-55Hz/0.15g, 55-500Hz/2.0g storage range
MIL-STD-810F:	501.4, 502.4, 507.4, 500.4, 516.5, 514.5

1.10 NetClock 9483 Available Option Modules

The NetClock 9483 product can be customized and enhanced via the addition of up to two (2) additional option modules, detailed in this section.

NOTE: In some cases, the number of option modules of any one type that can be installed may be limited (see "Maximum number of cards" for each type of module).

For additional information on available option modules, including configuration and usage with your product, refer to *Section 8:* "*NetClock 9483 Option Modules*".

1.10.1 T1 (1.544MHz) and E1 (2.048MHz) Module

Outputs:	T1 mode:
	• 1.544MHz (square wave) frequency output
	• (2) 1.544 Mb/sec data rate outputs:
	  ○ Outputs are DS1 framed all ones.
	  ○ Supports Super Frame (SF or D4) and Extended Super Frame (ESF).
	  ○ SSM support
	E1 mode:
	• 2.048MHz (square wave) frequency output
	• (2) 2.048 Mb/sec data rate outputs:
	  ○ Outputs are E1 frame all ones.
	  ○ Supports CRC4 and CAS Multiframe.
	  ○ SSM support

Maximum Number of Cards:	1
Ordering Information:	Option 13: T1/E1 Balanced (1) E1 (75 Ω) module (2) T1 and E1 (100 / 120 Ω) module

1.10.2 Multi-Port Gigabit Ethernet Module

Inputs / Outputs:	(3) Gigabit Ethernet (10/100/1000 Base-T)
Signal Type and Connector:	RJ-45
Management:	Enabled or Disabled (NTP server only)
Maximum Number of Cards:	1
Ordering Information:	Option 16: Multi-port Ethernet (3X) Module

1.10.3 PTP I/O Module

Inputs / Outputs:	(1) PTP

Signal Type and Connector:	RJ-45
Maximum Number of Cards:	1
Ordering Information:	Option 12: PTP I/O

Section 2: Installation

To begin the installation of your product, follow the steps and information outlined in this section.

2.1 Safety

Before beginning, carefully read the following important safety statements. Always ensure that you adhere to any and all applicable safety warnings, guidelines, or precautions during installation and operation of your product.

	**WARNING** *Installation of this product is to be done by authorized service personnel only. This product is not to be installed by the user/operator.* *Installation of the equipment must comply with local and national electrical codes.* *DO NOT OPERATE THIS EQUIPMENT WITH THE COVER OR BLANK PLATES COVERING UNUSED OPTION CARD SLOTS REMOVED.*
	**CAUTION** *Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.*
	**WARNING** ***The interior of this equipment does not have any user serviceable parts. Contact Spectracom Technical Support if this equipment needs to be serviced.*** *This unit will contain more than one power source if both the AC and DC power options are present. Turning off the rear panel power switch will not remove all power sources.* *Ensure all power sources are removed from the unit prior to installing any option cards by removing both the AC and DC power cords connected to the equipment.* *Never remove the cover or blank option card plates with power applied to this equipment.* *This equipment has Double Pole/Neutral Line Fusing on AC power.*
	**WARNING** *This equipment must be earth grounded. Never defeat the ground connector or operate the equipment in the absence of a suitably installed earth ground connection. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.* *The AC and DC power connectors of this equipment have a connection to the earthed conductor of the AC and DC supply earthing conductor through the AC and DC power cords. The AC source outlet must contain a protective earthing connection.*

	This equipment shall be connected directly to the AC power outlet earthing pin or DC supply system earthing electrode conductor. *This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection to the earthing conductor of the same AC or DC supply circuit earthing conductor, and also the point of earthing of the AC or DC system. The AC or DC system shall not be earthed elsewhere.* *The DC supply source is to be located within the same premises as this equipment.* *Switches or other disconnection devices shall not be in the earthed circuit conductor between the AC and DC source and the point of the connection of the earthing electrode conductor to NetClock's AC and DC input power connectors earthing pin.*
	**CAUTION** *For continued protection against risk of fire, replace fuses only with same type and rating of fuse.* *There is a danger of a new battery exploding if it is incorrectly installed. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.*

NOTE: The following sections assume setup and configuration of a NetClock 9483 and may refer to options or features specific to that model. For information specific to the setup and configuration of a NetClock 9489, refer to Section *3.3* : "*NetClock 9489 Network Setup*"

Unpack and inspect the unit and accessories. The following items are included with your NetClock:

- NetClock 9400 Series Unit
- QuickStart Guide
- Purchased Optional Equipment
- Ancillary kit (except for rack mounting items, contents of this kit, such as an AC line cord, will vary based on equipment configuration)

Any options on the original purchase order have been pre-installed.

NOTE: Retain all original packaging for use in return shipments if necessary.

2.2 Required Tools and Cables for Installation

1. Phillips screwdriver to install the unit's rack-mount ears.
2. Screwdriver to mount the unit in a standard 19-inch rack.
3. Ethernet cables (refer to Section *2.11*: "*Ethernet Network Cabling*").

2.3 Installation 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.

If installing the unit in a rack, install the rack-mount ears on the two sides of the front panel and mount the unit in a standard 19 inch rack cabinet. The unit is intended to be installed in one orientation only. The unit should be mounted so the front panel interface keys are to the left of the display area.

Depending on the equipment configuration at time of purchase, NetClock can be powered from an AC input, a DC input or with both AC and DC input (DC input is an option only for the NetClock 9483). Supplying both AC and DC input power provides redundant and automatic power switchover in case one or the other input power sources is lost.

2.4 Rack Mounting

The NetClock will install into any EIA standard 19 inch rack. The NetClock occupies one rack unit of space for installation, however, it is recommended to leave empty space of at least one rack unit above and below the NetClock for best ventilation of the NetClock.

- The NetClock maximum ambient operating temperature must be kept to the maximum value specified in Section *1.9* for the oscillator option purchased. If the NetClock is to be installed in a closed rack, or a rack with large amounts of other equipment, a rack cooling fan or fans should be part of the rack mount installation.
- Installation of the NetClock in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- Mounting of the NetClock in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Consideration should be given to the connection of the NetClock to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of NetClock nameplate ratings should be used when addressing this concern.
- Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

The NetClock ancillary kit will contain the following parts needed for rack mounting:

- 2 each 1165-1000-0714 Rack mounting brackets
- 2 each MP09-0003-0030 equipment rack handles
- 4 each H020-0832-0406 #8-32 flat head Phillips screws
- 6 each HM20R-04R7-0010 M4 flat head Phillips screws
- CA0R-1513-0001 AC POWER CORD

The following customer supplied items are also needed:

- 4 each #10-32 pan head rack mount screws
- 1 each #2 Phillips head screwdriver

- 1 each 3/32", Straight screwdriver

To rack mount the NetClock:

1. Attach an MP09-0003-0030 equipment rack handle to the front of each 1165-1000-0714 rack mounting bracket, using the holes nearest the right angle bend of the 1165-1000-0714 rack mounting bracket, with the #2 size Phillips screwdriver, using 2 each of the H020-0832-0406 #8-32 flat head Phillips screws.

2. Attach the 1165-1000-0714 rack mount brackets to the sides of the NetClock with the rack mounts ears facing outward, aligned with the front edge of the NetClock front panel. Use the #2 Phillips screwdrivers, using 3 each of the HM20R-04R7-0010 M4 flat head Phillips screws.

3. Secure the rack mount brackets to the rack using the #10-32 rack mount screws and #2 Phillips head screwdriver, 2 each per side of the rack.

NOTE: For safety purposes, the NetClock is intended to be operated in the upright position only, with the keypad to the left side and the LCD and time displays on the right side.

2.5 Power Connection

This section includes details on the NetClock's AC and / or DC power systems (*Note: DC power available with NetClock 9483 systems only*).

NOTE: Be sure that you have read all safety warnings detailed in "*Section 2: Installation"* while operating your equipment.

2.5.1 Input Power Selection:

As long as the AC input power is present, AC power will be selected.

- If AC and DC power are both applied, AC power is used.
- If DC power is applied, but AC power is not, the DC power will be used.
- If AC and DC power are both present, but AC power is subsequently lost, NetClock will automatically switch to using the DC power input.

The following sections discuss AC and DC power input. Connect AC and/or DC power, as desired.

2.5.2 If AC Input Power is Desired:

Connect the AC power cord supplied in the NetClock ancillary kit to the AC input on the rear panel and the AC power source outlet. The AC input is fuse-protected with two fuses located in the AC power entry module (line and neutral inputs are fused). The AC power entry module also contains the main power switch for the AC power applied to the equipment.

WARNING: This equipment has Double Pole/Neutral Line Fusing on AC power.

NOTE: ***Important!*** NetClock is earth grounded through the AC power connector. Ensure NetClock is connected to an AC outlet that is connected to earth ground via the grounding prong (do not use a two prong to three prong adapter to apply AC power to NetClock).

2.5.3 If DC Input Power is Desired (NetClock 9483 Only):

If the rear panel DC port is present, connect DC power, per the voltage and current as called out on the label that resides above the DC power connector.

NOTE: DC power is an option chosen at time of purchase. The rear panel DC input port connector is only installed if the DC input option is available. Different DC power input options are available (12vdc with a voltage range of 12-17V at 7A maximum or 24/48vdc input with a voltage range of 21-60V at 3A maximum). Review the DC power requirement chosen, prior to connecting DC power (when the DC port is installed, a label will be placed over the connector indicating the allowable DC input voltage range and the required current).

NOTE: ***Important!*** NetClock is earth grounded through the DC power connector. Ensure that the NetClock is connected to a DC power source that is connected to earth ground via the grounding pin C of the NetClock DC power plug supplied in the ancillary kit.

NOTE: The DC input port is both fuse and reverse polarity protected. Reversing polarity with the 24/48vdc option will not blow the fuse, but the equipment will not power-up. Reversing polarity with the 12vdc option will likely blow the internal fuse.

A DC power connector to attach DC power to NetClock is included in the ancillary kit provided with the equipment. A cable of 6 feet or less, using 16AWG wire, with adequate insulation for the DC voltage source should be used with this connector. The cable clamp provided with the DC power plug for strain relief of the DC power input cable should be used when DC power is connected to NetClock.

DC power connector pin-out:

Pin B goes to the most positive DC voltage of the DC source. For +12V or +24/48V this would be the positive output from the DC source. For a -12V or -24/48V DC source this would be the ground or return of the DC source.

Pin A goes to the most negative voltage of the DC source. For +12V or +24/48V this would be the ground or return output from the DC source. For a -12V or -24/48V DC source this would be the negative output from the DC source.

Pin C goes to the Earth ground of the DC source.

2.5.4 NetClock Power-up

If AC input is connected, turn the rear panel AC power switch on (DC input power is not switched, so NetClock will be powered up with DC input connected) and observe that all of the front panel LEDs momentarily illuminate (the Power LED will then stay lit) and that the LCD display backlight illuminates. The LED time display will reset and then start incrementing the

time. About 10 seconds after power-up, "Starting up NetClock" will be displayed in the LCD window. After approximately 2 minutes, the LCD will then display the current network settings.

NOTE: As the front panel cooling fan is internal temperature controlled, the fan may not always be in operation. However, the fan will momentarily turn on each time NetClock is power cycled.

2.6 Power and Ground Connection Safety

<table>
<tr><td rowspan="2">  </td><td>WARNING</td></tr>
<tr><td>The interior of this equipment does not have any user serviceable parts. Contact Spectracom Technical Support if this equipment needs to be serviced.

This unit will contain more than one power source if both the AC and DC power options are present. Turning off the rear panel power switch will not remove all power sources.

Ensure all power sources are removed from the unit prior to installing any option cards by removing both the AC and DC power cords connected to the equipment.

Never remove the cover or blank option card plates with power applied to this equipment.

This equipment has Double Pole/Neutral Line Fusing on AC power.</td></tr>
<tr><td rowspan="2">  </td><td>WARNING</td></tr>
<tr><td>This equipment must be earth grounded. Never defeat the ground connector or operate the equipment in the absence of a suitably installed earth ground connection. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

The AC and DC power connectors of this equipment have a connection to the earthed conductor of the AC and DC supply earthing conductor through the AC and DC power cords. The AC source outlet must contain a protective earthing connection.

This equipment shall be connected directly to the AC power outlet earthing pin or DC supply system earthing electrode conductor.

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

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

Switches or other disconnection devices shall not be in the earthed circuit conductor between the AC and DC source and the point of the connection of the earthing electrode conductor to NetClock's AC and DC input power connectors earthing pin.</td></tr>
</table>

2.7 Common Post-Installation Configuration Scenarios

There are commonly desired installation configuration scenarios. Refer to the following Sections if desired or applicable for your environment:

Common / Desired Configuration Scenario	**Refer to Section:**
Displaying Local Time on the Front Panel (instead of UTC time) – **NetClock 9483 only**	*3.13.6: "Example - Applying Local Clock to Front Panel"*
Interfacing a NetClock with Spectracom TimeView Display Clocks	*2.73.13.7: Example Configuration for Spectracom TimeView Displays Clocks*

2.8 Connecting Reference Inputs and Network Interface

NetClock 9400 can synchronize to various external inputs (Such as GPS, NTP, PTP, and/or a user set time). Depending on the desired operation and specific NetClock configuration, connect the GPS, or other external references (NTP input reference and "user set time" are software configurations that require no additional physical connection to NetClock. These two reference inputs are discussed later in this manual).

1. **GPS Reference Input:** Typical installations include GPS as an external reference input. If the GPS receiver is not installed or if the GPS will not be used as a NetClock reference, just disregard the steps to install the GPS antenna and associated cabling.

Install the GPS antenna, surge suppressor, antenna cabling, and GPS preamplifier (if required). Refer to the documentation included with the Model 8225 GPS antenna for additional information regarding GPS antenna installation.

Connect the GPS cable to the rear panel antenna input jack (refer to Figure 1-3). Until the GPS antenna is connected to the rear panel jack, the Antenna Problem alarm is asserted, causing the front panel "Fault" light to be blinking orange (the Antenna Problem alarm indicates an open or short exists in the antenna cable). Unless there is an open or short in the antenna cable, the Fault light should stop flashing orange once the GPS antenna and coax cable are connected to the rear panel. If the Fault light does not stop flashing after connecting the antenna, refer to Section *10.4*: "*Troubleshooting GPS Reception Issues (Holdover and/or Time Sync Alarms Occurring):*".

2. **PTP Reference input:** With the available PTP option card configured as a slave synchronizing via Ethernet / RJ-45 to a PTP master.

3. **Network interface to LAN:** Obtain the following network information from your network administrator before continuing:

Available static IP Address	This is the unique address assigned to the NetClock unit by the network administrator. The default static IP address of the NetClock unit is 10.10.201.1.
Subnet mask (for the network)	The subnet mask defines the number of bits

	taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.
Gateway address	The gateway (default router) address is needed if communication to the NetClock is made outside of the local network. By default, the gateway is disabled.

Table 2-1: Required Network information

If your network does not support DHCP, use the front panel LCD and keypad (refer to Section *2.9*: "*Front Panel Keypad/LCD Operation*") to input the desired static IP, subnet mask, and gateway address.

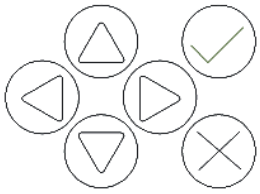
Network Bits	Equivalent Netmask	Network Bits	Equivalent Netmask
30	255.255.255.252	18	255.255.192.0
29	255.255.255.248	17	255.255.128.0
28	255.255.255.240	16	255.255.0.0
27	255.255.255.224	15	255.254.0.0
26	255.255.255.192	14	255.252.0.0
25	255.255.255.128	13	255.248.0.0
24	255.255.255.0	12	255.240.0.0
23	255.255.254.0	11	255.224.0.0
22	255.255.252.0	10	255.192.0.0
21	255.255.248.0	9	255.128.0.0
20	255.255.240.0	8	255.0.0.0
19	255.255.224.0		

Table 2-2: Subnet Mask Values

2.9 Front Panel Keypad/LCD Operation (NetClock Model 9483)

To simplify operation and to allow “local” access to the NetClock, a keypad and LCD display are provided on the front panel of the unit.

2.9.1 Keypad Description



The NetClock front panel keypad has six buttons for making certain configuration changes or viewing status information on the LCD display. The functions of each are as follows:

ENTER (✓): Select a menu item or load a parameter when editing

BACK (✕): Return to previous display or abort an edit process

LEFT arrow (←): Select a new item to the left

RIGHT arrow (→): Select a new item to the right

DOWN arrow (↓): Scroll through parameter values in edit displays

UP arrow (↑): Scroll through parameter values in edit displays

2.9.2 Navigating the Keypad Display

After power initialization, press any key to go to the "Home" display. As illustrated in Figure 2-1, several status and setup displays are accessible from the main "Home" menu. To navigate through the menus, use the arrow keys to highlight a selection and then press the ENTER button (✓).

The main menu options and their primary functions are as follows:

Display: Used to configure the LCD display.
Clock: Displaying and setting of the current date and time.
System: Displaying version info, system halt and reboot, reset **`spadmin`** password.
Netv4: Network interface configuration.
Lock: Locks the front panel keypad to prevent inadvertent operation.

2.9.3 Unlocking the Front Panel Keypad

If the front panel keypad is locked, the following sequence will locally unlock the keypad for use (note that the front panel can also be locked / unlocked via the NetClock web user interface.

↑ ↓ ↑ ↓ ← → ← → ✓ x ✓

2.9.4 Editing Options from the Keypad

To modify an option, highlight the menu option and press the ENTER button (✓). The "O" data is the current old setting and the "N" data is the new setting. You can only change the "N" setting in all menus. Use the UP and DOWN arrow keys to scroll through all possible parameter values.

When editing a sequence of numbers, use the LEFT and RIGHT arrow keys to select other digits. When the parameter is correct, press ENTER to load the new value. You will be asked to confirm the setting change. Press ENTER to accept or BACK to cancel the parameter change. All entered values are stored in memory and restored after a power cycle.

The following figure displays the keypad/LCD operation navigation tree.

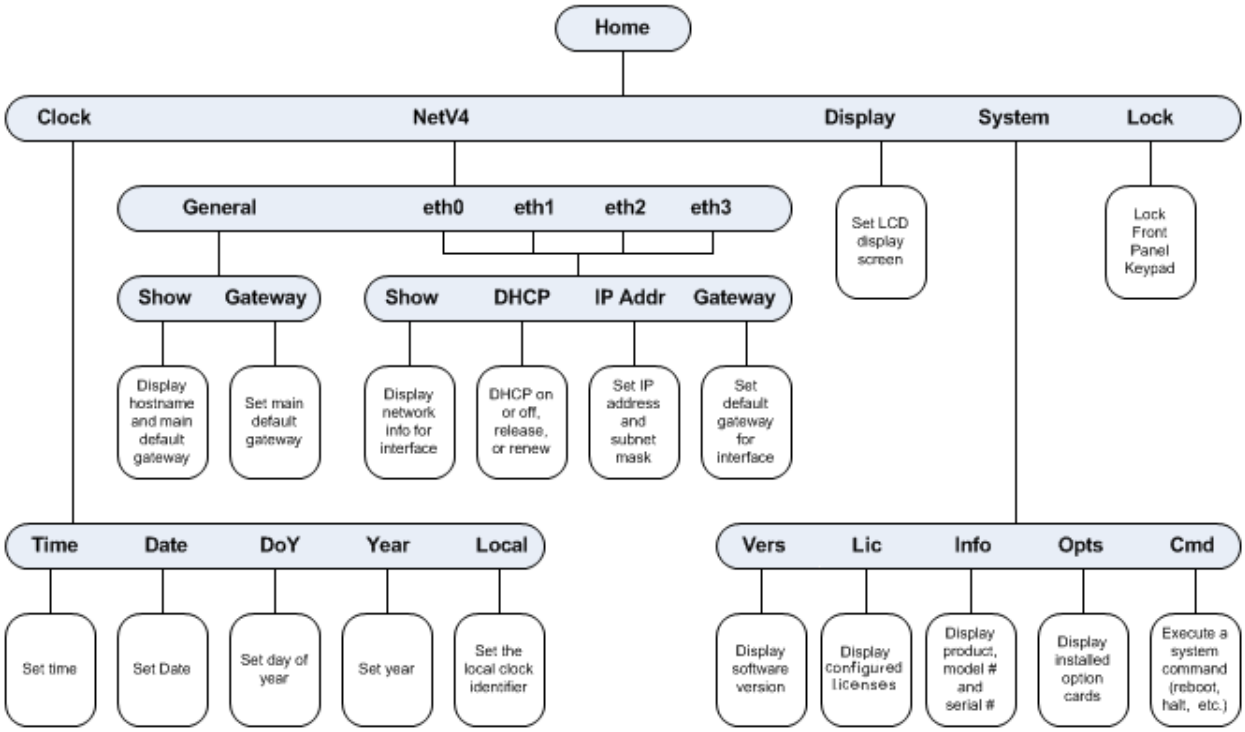


Figure 2-1: Keypad/LCD Navigation Tree

Using the keypad, the LCD display window can be configured to display various indications, including the network settings, System Status, GPS position, GPS signal information or the current date and time (Or, it can even be configured to remain blank, if desired).

2.10 Front Panel Serial Port

In addition to the available front panel keypad and LCD display, the front panel also contains a DB9 serial port that can be used to communicate with NetClock. The serial port connector is a standard DB9 Female connector. Communication with the serial port can be performed using a terminal emulator program (such as HyperTerminal or Procomm) using a pinned straight-thru standard DB9M to DB9F serial cable.

The serial port can be used to make configuration changes (such as network settings), retrieve operational data (such as the GPS receiver information), or to perform operational processes (such as resetting the admin password).

The serial port is account and password protected. Login via the serial port using the same user names and passwords as would be used to log into the NetClock web interface. Users with "administrative rights" can perform all available commands. Users with "user" permissions only can perform "**`get`**" commands that retrieve data, but cannot perform any "**`set`**" commands or change / reset any passwords.

Refer to Section 11: "*Using HyperTerminal to Connect to NetClock*" for more information on serial port connections, and Section 12: "*NetClock 9400 Series Commands*" for a list and description of the available serial port commands that can be issued.

2.10.1 To Disable DHCP using Front Panel

1. Press the ✓ key.
2. Using the arrow keys, select **Netv4** from the menu.

NOTE: *To select a menu item, highlight it using the arrow keys and press the ✓ key.*

3. Select the Ethernet interface for which DHCP is to be disabled, such as "**eth0**".
4. Select "**DHCP**" from the next menu.
   The display will show "**State=Enabled**" and "**Action=Disabled**".

NOTE: *The State is the current DHCP setting and the Action is the action to take. You can only change the Action setting.*

5. Press the ✓ key once to select the action, then again to apply it.

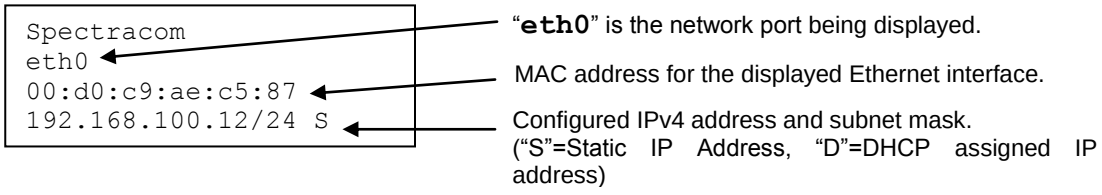
2.10.2 To Enter IP Address and Subnet Mask

1. Still on the **Home / Netv4 / eth[0-3]** menu, select **IP Address**, and change "**N=010.010.201.001/16**" to the value of the static IP address and subnet mask / network bits to be assigned.
2. Press the ✓ key once to enter the setting, then again to apply the new setting.

2.10.3 To Enter the Gateway Address (if Required)

1. Still on the **Home / Netv4 / eth[0-3]** menu, select **Gateway**, and change the "**N=010.010.201.254**" to the value of the default gateway to be assigned to this interface.
2. Press the ✓ key once to enter the setting, then again to apply the new setting.

After all addresses are entered, press the front panel ✕ key three times to return to the main display. It should now resemble the following example:



DNS: The Primary and Secondary DNS servers are set automatically if using DHCP. If DHCP is not available, they can be configured manually from the **Network / General Setup** page of the NetClock web interface.

NOTE: The remainder of the configuration settings will be performed through the NetClock web-based user interface, herein referred to as the "web interface" or "web UI".

Determine whether configuration will be done on a computer attached to the network or a computer connected directly to the NetClock unit. For a network computer, connect a shielded CAT 5, Cat 5E or CAT 6 cable with RJ-45 connectors to the Ethernet port on the NetClock rear panel (refer to Figure 1-3). Connect the opposite end of the cable to a network hub or switch. For connection with a stand-alone computer, this cable should be pinned as a network-crossover cable and should be connected to the NIC card of the computer. Verify the green link light on the Ethernet port is illuminated. The amber "Activity" link light may periodically illuminate when network traffic is present.

Connect to the NetClock unit using a web browser (such as Internet Explorer or Mozilla Firefox) directed to either the static IP address or the address assigned by DHCP, as displayed on the front panel LCD. If the network supports DNS, the hostname may also be entered instead (the default hostname is "Spectracom"). You can now manage and configure your product through the NetClock product web interface. Refer to Section *3.4* for additional information.

NOTE: *The factory-default user name and password are:*

Username: `spadmin`
Password: `admin123`

With input references connected, verify the NetClock's front panel Sync lamp is green. Initial synchronization with GPS input may take up to 35 minutes (approximately) when used in the default stationary GPS operating mode. If using GPS, verify that GPS is the sync source by navigating to the **Status / Time and Frequency Status** page of the web UI and viewing the "Selected Time Reference Source" in the table. The Selected Time Reference Source for GPS is "GPS 0".

Unless you are using DNS in conjunction with DHCP (with the client configured using NetClock's hostname instead of IP address), DHCP must be disabled and the IP address must be changed to a static address once 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 NetClock. Verify your setup before synchronizing the network PCs via NTP.

Synchronize the network PCs via NTP using the Ethernet port as desired. For a more description of synchronizing Windows PC's, please visit the Spectracom website (www.spectracomcorp.com), and from the main site navigation menu select **Support > Library > Installation and Troubleshooting Guides**, and download / review the document titled *Synchronizing Windows Computers*. This document also contains information and details about using the Spectracom PresenTense NTP client software.

During configuration of the various options it may be necessary to power down or restart the unit. In this case a 'Halt' command should be issued prior to removing power from the unit. Failure to do so may cause the NetClock unit to take longer to boot on the next power up cycle. After the 'halt' command is issued via the web interface or front panel, wait until the LCD reads 'Power off NetClock' before removing power (refer to Section *3.9* for additional information).

2.11 Ethernet Network Cabling

Spectracom NetClock provides a base 10/100 Ethernet port for full NTP functionality, as well as a full web-based user interface for configuration, monitoring and diagnostic support. Additional network ports are available with the Gigabit Ethernet option module (refer to Section 8: for additional information).

The Ethernet port is provided on the back panel for easy connection to routers, switches, or hubs.

Use shielded CAT 5 or CAT 6 cable with RJ-45 connectors.

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

When connecting directly to a Windows PC, use a crossover wired network cable. Since no DHCP server is available in this configuration, both NetClock and the Windows PC must be configured with static IP addresses that are on the same subnet (`10.1.100.1` and `10.1.100.2` with a subnet value of `255.255.255.0` on both devices, for example). For more information on configuring static IP addresses, please refer to the product documentation for the version of the Windows operating system that you are using.

2.12 Product Registration

Spectracom periodically releases important software updates for our products. If you would like to be notified of these updates as they become available, the Spectracom website provides a product registration page. To register your email address for automatic notifications of software updates, please visit http://www.spectracomcorp.com. Product registration can be accessed from the "**Support**" menu.

NOTE: If NetClock has access to the Internet, the **Tools / "Contact/Register**" page of the NetClock web interface provides a direct link to register your product & contact information.

Section 3: Product Configuration

NOTE: Screens displayed in this document are for illustrative purposes. Actual screens may vary depending upon your particular NetClock configuration (e.g., whether or not certain options were chosen at the time of purchase, etc). After installing NetClock, verify that power is connected and wait for the device to boot up.

3.1 Overview

Regardless of which NetClock 9400 Series product you may have (9483, or 9489), the following general steps are necessary during initial setup and configuration:

- Determine if your NetClock unit will use DHCP to obtain an IP configuration, or be configured with a static IP address.
- Set up the IP network settings for the NetClock product (IP address, etc).
- Perform further configuration via the NetClock's web-based user interface.

NOTE: The default IP address for both NetClock Model 9400 products is **`10.10.201.1`**, with subnet mask **`255.255.255.0`**.

The following sections cover network setup for both NetClock Models (9483, 9489).

3.2 NetClock 9483 Network Setup

The front panel display provides certain configuration data on start-up. The LED window displays the current time (UTC, TAI, GPS or local timescale, as configured. Current time will be displayed in UTC by default). The LCD window displays the unit's hostname, IPv4 address, mask, and gateway.

NOTE: If using DHCP, the IP address will be assigned automatically and displayed on the front panel. You may use a web browser to connect to this IP address and configure the NetClock through the web user interface (Figure 3-1). Refer to the *"Network Configuration with DHCP"* section.

When configuring a NetClock without DHCP, or to configure a NetClock that has not been assigned an IP address, refer to Section *3.2.2*., *"Network Configuration without DHCP"*.

3.2.1 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 are 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 NetClock'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.

NOTE: Unless the user opens the web interface using the default DNS name of "Spectracom" (instead of using the IP address to access NetClock), the SSL certificate / security pop-up window will continue to be displayed each time the user opens the web interface. To prevent the security pop-up window from opening each time, a new SSL certificate needs to be created using the assigned IP address of NetClock during the certificate generation.

3.2.2 Network Configuration without DHCP

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 automatically assign an IP address for the NetClock.

To configure a NetClock without a DHCP server available on the network or to configure a NetClock that has not been assigned an IP address; you can use either the front panel keypad and LCD display or a serial cable to connect a PC or laptop computer to the serial port on the front of the NetClock. The keypad is the simplest method to configure the network settings. Refer to Section *2.9* for information on using the keypad. Refer to Sections *2.10.1*, *2.10.2* and *2.10.3* for the steps to disable DHCP and to configure the IP address, Subnet Mask and Gateway address.

If you desire to use the front panel serial port instead of the keypad, after making this connection, use a terminal emulator 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. Refer to Section 11: for more information on the serial port connection and Section 12: for a list and description of the available serial port commands that can be issued.

A) To configure NetClock's network settings using the front panel serial port:
   1) Connect a serial cable to a PC running HyperTerminal and the NetClock.
   2) Log in to NetClock with a user account that has "admin" group rights, such as the default spadmin account (the default password for spadmin is "admin123").
   3) To disable DHCP, type: **`dhcp4set 0 off`** <Enter>. ***Note:*** If your NetClock is configured with an Ethernet option card, use **`0`**, **`1`**, **`2`**, **`3`** for **`eth0`** – **`eth3`**.
   4) To configure the IP address and subnet mask, type: **`ip4set 0 xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy`** <Enter> (where **`0`** is the desired interface, "**`xxx.xxx.xxx.xxx`**" is the desired IP address for NetClock, and "**`yyy.yyy.yyy.yyy`**" is the full subnet mask for the network (refer to Table 2-2 for a list of subnet mask values).
   5) Type **`gw4set 0 zzz.zzz.zzz.zzz`** <Enter> (where where **`0`** indicates which interface routing table to add the default gateway for, and "**`zzz.zzz.zzz.zzz`**" is the default gateway address). ***Note:*** If your NetClock is configured with an Ethernet option card, use **`0`**, **`1`**, **`2`**, **`3`** for **`eth0`** – **`eth3`**.

NetClock is now configured with a static IP address, subnet mask and gateway address. From this point forward, further product configuration can be performed by logging in to the product web interface. Refer to Section 3.4: Product Configuration Using the Web Interface

3.3 NetClock 9489 Network Setup

NOTE: By default, DHCP is disabled on the NetClock 9489 unit, and it ships with a default IP address of **`10.10.201.1`** with subnet mask **`255.255.255.0`**. As the NetClock 9489 does not include a front panel LED or LCD that can display status information, it is important to read the following sections carefully in order to successfully determine or configure a NetClock 9489's network settings. This can be achieved via one of the following methods:

- Configuration via serial cable connection
- Configuration via crossover cable
- Configuring a temporary IP address remotely

3.3.1 Network Configuration using Serial Cable Connection

Connect a serial cable from your PC to the input on the front panel of the NetClock 9489. Open a terminal emulator program (such as HyperTerminal, or equivalent), and use the following values to establish a connection to the NetClock:

- **Bits per second:** 9600
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** None

Once a serial connection has been established, log in to the NetClock as an administrator. Once logged in, you may use the command line interface commands to configure network settings.

To setup a static IP address, netmask, and gateway, perform the following steps:

1. Enter "**`ip4set 0 address mask`**", using your static IP4 address and net mask.
2. Enter "**`gw4set 0 gw_address`**", using your gateway address **`gw_address`**.

For additional details regarding available commands, refer to *Section 12:* "*NetClock 9400 Series Commands"*. Once you've determined or set the IP address, you can then also login to the product web interface by entering the IP address into a web browser's address bar and logging into the NetClock as an administrator.

3.3.2 Network Configuration using a Crossover Cable

Turn on the NetClock 9489 with NO crossover cable plugged into the Ethernet port (note: once you apply power, it may take up to two minutes for the system to fully boot). Configure your PC's network interface card (NIC) with an IP address on the same network as the NetClock 9489's default IP address (**`10.10.201.1`**). For example, configure the IP address of your PC's network interface card as **`10.10.201.10`**, with a subnet mask of **`255.255.255.0`**.
Connect a crossover cable from your PC to the Ethernet port of the NetClock unit. Once connected via crossover cable, open a web browser and enter the NetClock's default IP address (**`10.10.201.1`**) into the browser's address bar and login to the NetClock's web

interface as an administrator. Once logged in, network settings for the NetClock can be configured from **Network → General Setup**.

3.3.3 Network Configuration via Setting a Temporary IP Address Remotely

If your network supports DHCP, your NetClock 9489 may have automatically been assigned an IP address by a DHCP server (if DHCP had been enabled on the unit after initial setup and configuration). In this scenario, you can perform remote commands for initial network setup by using the MAC address information of your NetClock 9489. This method also applies to statically configured IP networks.

NOTE: Before beginning, ensure the following prerequisites are met:

- If it is desired to configure the NetClock 9489 with a static IP address, it must be a unique IP address not already assigned to another device via DHCP, or that has not already been statically assigned to another device.
- Ensure that the operator or administrator's PC and the NetClock 9489 are on the same subnet, and that the **`arp`** and **`ping`** commands can be issued from the workstation.

Complete the following steps:

1. From the rear panel of your NetClock 9489, locate the label displaying the MAC address of your unit. Write down or record the MAC address information.
2. Login to the operator's workstation and open a command prompt window.
3. Install the NetClock 9489 on your network and the same subnet as the workstation.
4. Power on the NetClock 9489 (wait for 2 minutes for the system to fully boot).
5. From the command prompt, issue the following commands:

From a Windows Operating System

NOTE: On Windows operating systems, you will need to elevated privileges to execute these commands. This can be accomplished using the "**`runas`**" command line program, or by holding CTRL + Right-clicking the command prompt icon, and selecting "Run as Administrator".

```
arp -s IP_ADDRESS MAC_ADDRESS
ping -l 408 IP_ADDRESS
```

Where "**`IP_ADDRESS`**" is the desired static IP address, and "**`MAC_ADDRESS`**" MAC address of your NetClock 9489. For example:

```
arp -s 192.168.0.10 00-AA-11-BB-22-CC
ping -l 408 192.168.0.10
```

From a UNIX or GNU/Linux Operating System:

NOTE: You must have administrative / root privileges to execute these commands.

```
sudo arp -s IP_ADDRESS MAC_ADDRESS
```

```
sudo ping -s 408 IP_ADDRESS
```

Where "**IP_ADDRESS**" is the desired static IP address, and "**MAC_ADDRESS**" is the MAC address of your NetClock 9489. For example:

```
arp -s 192.168.0.10 00:AA:11:BB:22:CC
ping -s 408 192.168.0.10
```

NOTE: You must complete this process within 5 minutes of the system booting, or else you will need to restart the NetClock system, and then restart from step 4. This is also a temporary IP address that will not persist through power cycles.

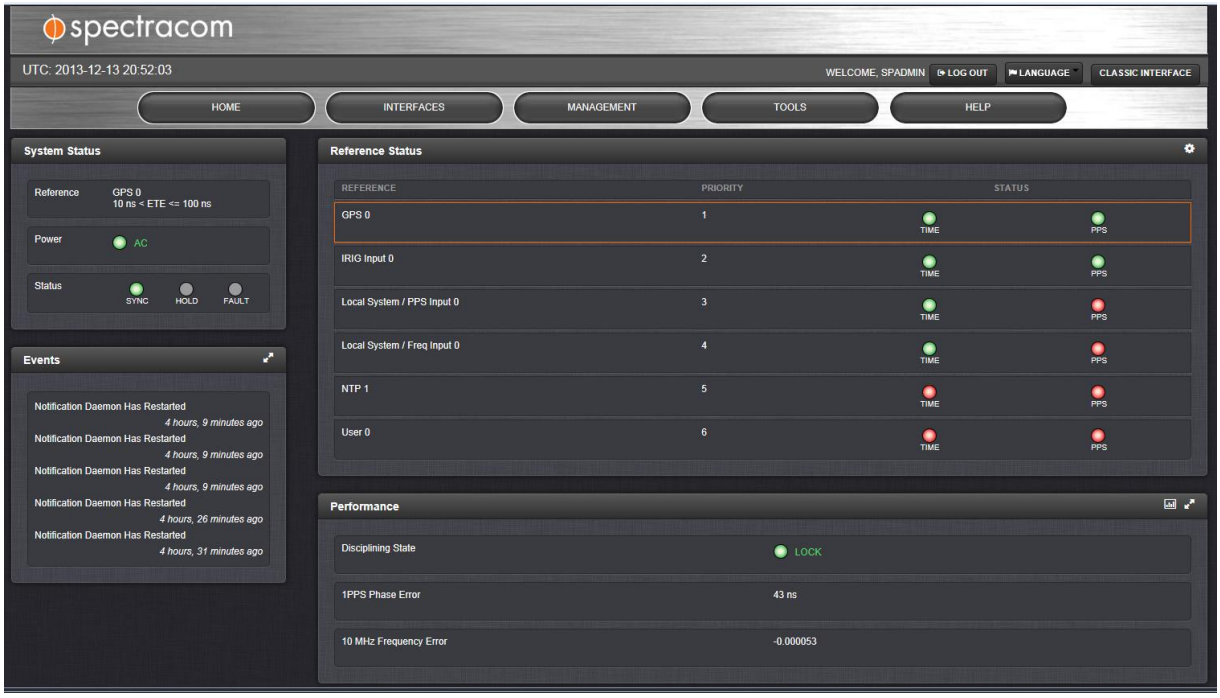
6. Open a web browser and enter the NetClock's IP address into the browser's address bar to access the NetClock web interface. Login as an administrator. Navigate to **Network → General Setup** and set your permanent IP configuration and network settings.

3.4 Product Configuration Using the Web Interface

Once the NetClock has been configured with the appropriate network settings and connected to the network, you may configure it, change its operating settings, check its status, and generate reports from the web interface (or "web UI") as needed. All web interface screens are accessible through the primary navigation menu at the top 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: You can exit any Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the window before you have hit the **Submit** or **Apply** button, any information you entered will not be retained.

3.4.1 The Web Interface Main Screen



All user interface web pages are accessible from the primary navigation menu at the top of the main page.

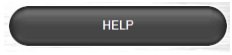
Primary-level navigation interface options are:

- Returns the user to the main page.

- Presents a drop-down menu for access to the for the system's references (e.g., GPS, NTP), output s (e.g. 10 mHz, PPS, NTP) and installed option cards (e.g., GPS, PPS).

- Presents a drop-down menu for access to the network setup and management screens.

- Presents a drop-down menu for access to the system maintenance screens and system logs.



- Presents a drop-down menu for access to system help and information on how to contact Spectracom for further help.

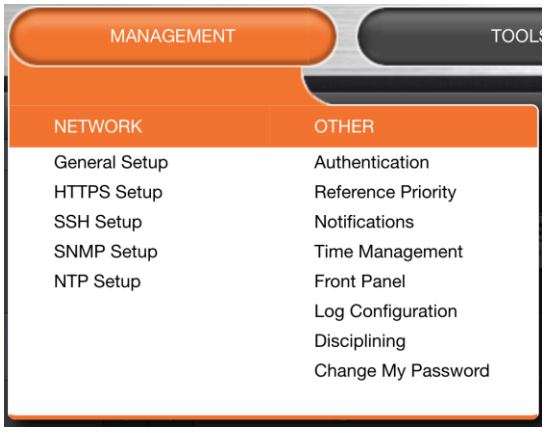
Some primary-level menu options have sub-menus (or secondary-level) options. Select an item from any of the sub-menus to access the page for that particular option. Some pages also contain tabs that can be selected which group options into logical sections.

For ease, this document defines which page to navigate to using the format: "**XXXX/YYYY**", where "**XXXX**" is the primary-level menu selection and "**YYYY**" is the drop-down menu option to be selected.

In certain instances, the second page viewed will allow access to other web pages. So, another specific page may need to be selected. This may be indicated in the manual as "**XXXX/YYYY/ZZZZ**" where "**ZZZZ**" is the next page selection to choose.

3.4.2 Accessing Setup Pages Through the MANAGEMENT Drop-Down Menu

Configuration of the unit is initiated through the **MANAGEMENT** drop-down menu, which is accessed by clicking on the **MANAGEMENT** button at the top of the screen.



Choosing an item from this menu takes the user to the setup/management screen for that item. The choices offered by the drop-down menu are divided into 2 categories: **NETWORK** and **OTHER**.
All network-specific setup screens are to the left of the menu, under **NETWORK**. These include the setup screens for:

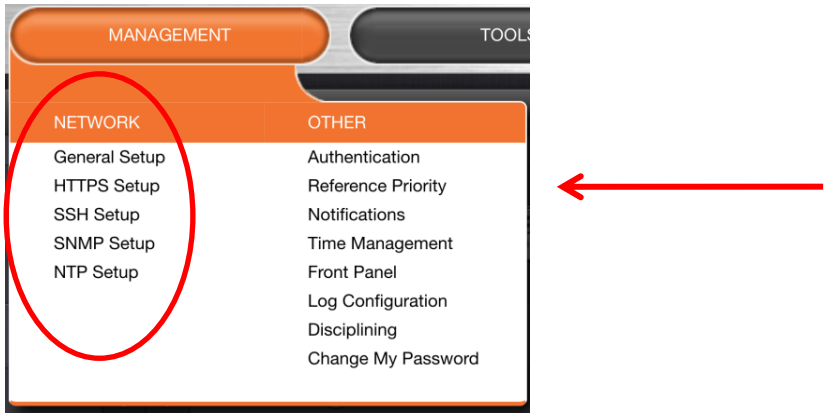
- General Setup
- HTTPS
- SSH
- SNMP
- NTP

Management screens that are not network specific are on the right of the menu. These include the management screens for:

- **Authentication**—Manage user accounts, Security Policy, LDAP Setup, RADIUS setup, Login Preference and Remote Servers. Change My Password is also available.
- **Reference Priority**—Define the order of priority for timing inputs.
- **Notifications**—Configure the notifications triggered by certain events. A notification can be a combination of a mask alarm and/or SNMP Trap and/or email.
- **Time Management**—Manage the local Clock, UTC Offset, DST Definition and Leap Second information.
- **Front Panel**—Configure the appearance of the front panel display and keypad.
- **Log Configuration**—Manage the system logs.
- **Disciplining**—Manage oscillator disciplining.
- **Change My Password**—Configure the admin password.

3.5 Network Setup Pages

All of the network setup pages can be accessed from the **MANAGEMENT** drop-down menu, under **NETWORK**.



3.5.1 General Settings

To facilitate quick setup on a network, use the **General Setup** window. This window provides the user quick access to the primary network settings necessary to connect the unit to a network:

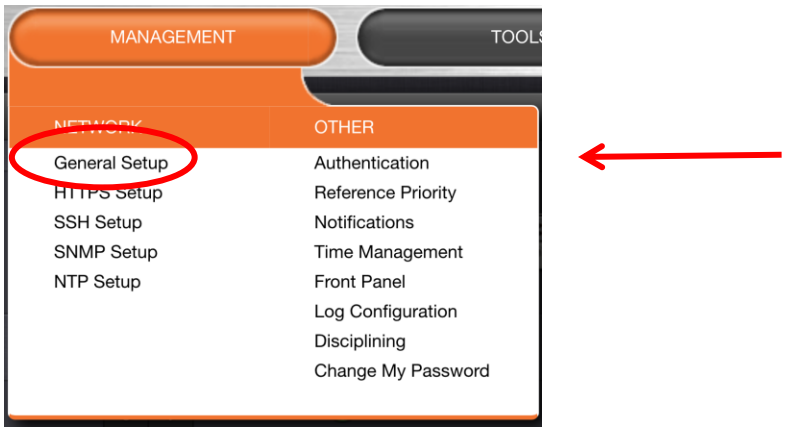
- **Hostname**—This is the server's identity on the network or IP address. The default is Spectracom.
- **Default Gateway IPv6**—The gateway (default router) address is needed if communication to the unitis made outside of the local network. By default, the gateway is disabled. In the format "**#**###.####.####.####.####.####.####.####.####," where each '**#**' is a hexadecimal value. When a DHCP server is not requested or is requested but not available and DHCP IPv6 is enabled, the server will use this Default Gateway.
- **Default Port**—When no specific port is identified for access to the network, the default port is used. The factory default port is eth0.

The **General Settings** window also displays the IPv4 address and default IPv4 gateway.

Accessing the General Settings

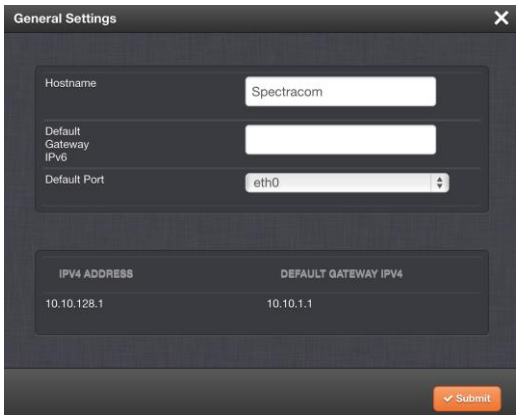
To access the general settings:

1. Navigate to the General Settings screen through **MANAGEMENT/NETWORK/General Setup**.



OR

1. Access the **Network Management** screen by clicking on **NETWORK** in the **MANAGEMENT** drop-down menu and click on the **General Settings** button in the **Actions** panel. See Accessing the Network Management Screen.
2. The **General Settings** window will display.



3.5.2 Configuring Ethernet Networks

Accessing the Network Management Screen

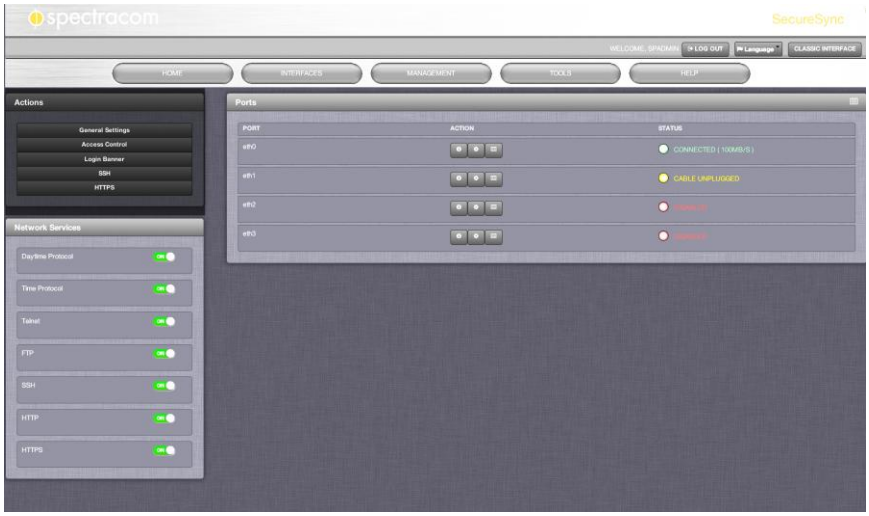
In order to monitor and manage Ethernet on the unit:

1. Navigate to the **Network Management** screen through **MANAGEMENT/NETWORK**.

2. The **Network Management** screen will display.

The **Network Management** screen is divided into 3 panels.

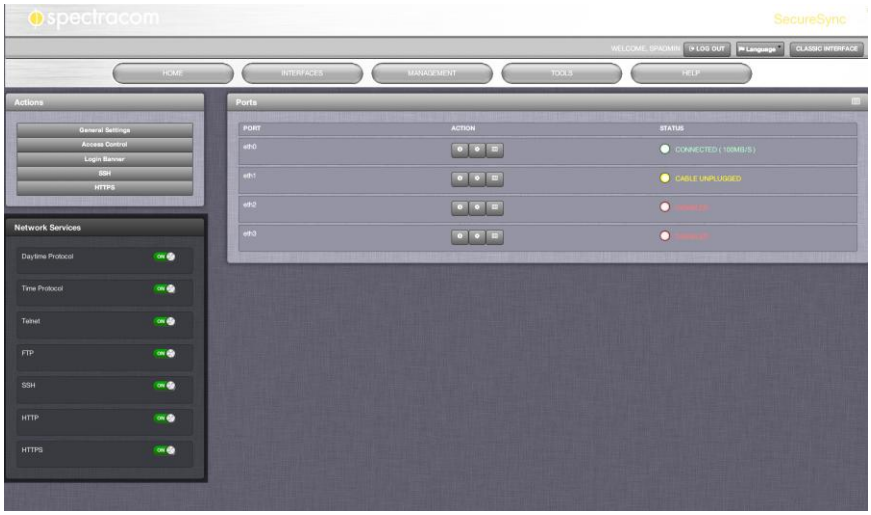
The **Actions** panel



The **Actions** panel provides:

- **General Settings**—Allows the user quick access to the primary network settings necessary to connect the unit to a network. See **3.5.1 General Settings**.
- **Access Control**—Allows the configuration of access restrictions from assigned networks/nodes.
- **Login Banner**— Allows the administrator to configure a custom banner message to be displayed on the login page (note: there is a 2000 character size limit).
- **SSH**—This button takes you to the SSH Setup window. For details on setting up SSH, see **3.7.1 Configuring SSH**.
- **HTTPS**—This button takes you to the HTTPS Setup window. For details on setting up HTTPS, see **3.7.2 Configuring HTTPS**.

The **Network Services** panel

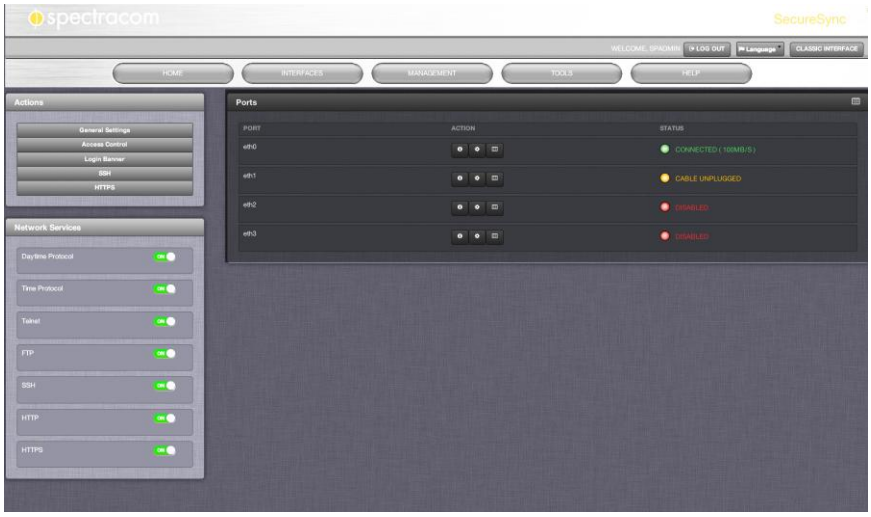


The **Network Services Panel** provides **ON/OFF** switches for:

- Daytime Protocol
- Time Protocol

- Telnet
- FTP
- SSH
- HTTP
- HTTPS

The **Ports** panel

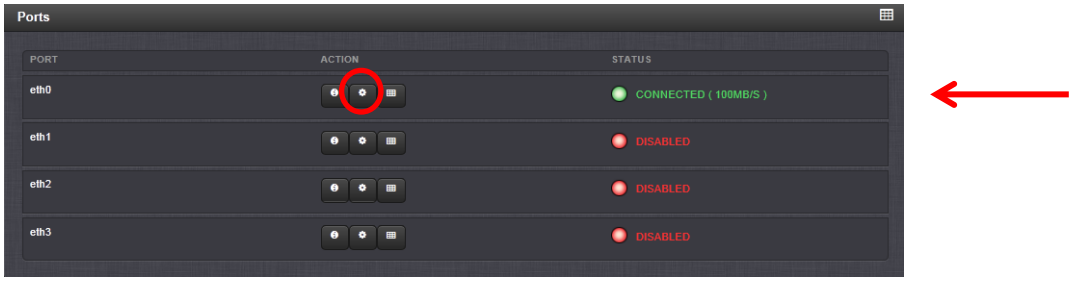


The **Ports** panel is where you set up and manage the network ports.

Configuring the Networking Ports

To configure a networking port:

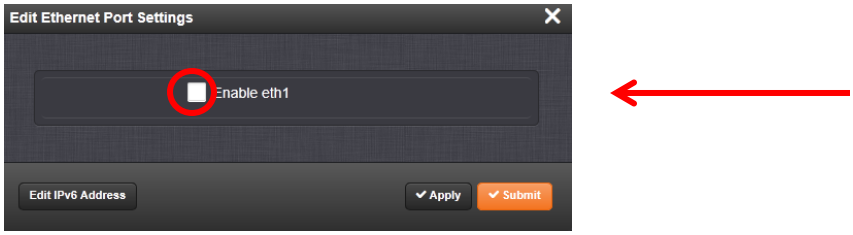
1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



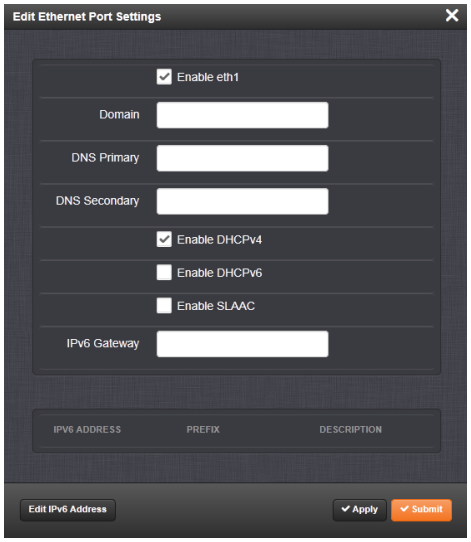
3. In the **Ports** panel, locate the port you want to configure and select the  button.

NOTE: The **eth0** port is the built-in Ethernet port.

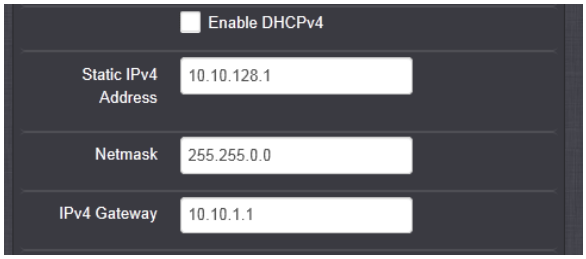
4. If the port is not already enabled, in the **Edit Ethernet Ports Settings** window, click on the **Enable** button.



5. The **Edit Ethernet Ports Settings** window will expand to show the options needed to complete port setup.



6. Complete the fields as required. The available fields are:
   - **Domain**—This is the domain name to be associated with this port.
   - **DNS Primary**—This is the primary DNS address to be used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Primary is set manually. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
   - **DNS Secondary**—This is the secondary DNS address to be used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Secondary is set manually. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
   - **Enable DHCPv4**—Check this box to enable the delivery of IP addresses from a DHCP Server using the DHCPv4 protocol. This box is checked by default.
     When DHCP is disabled (the box is unchecked), the following fields will display and must be completed:

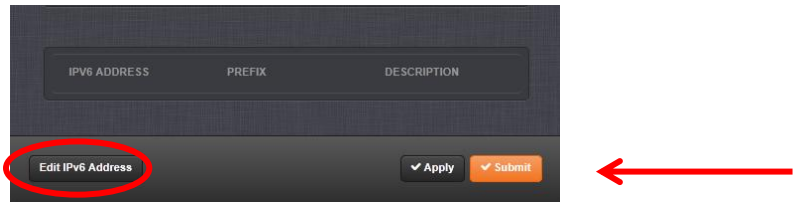


- **Static IPv4 Address—**This is the unique address assigned by the network administrator. The default static IP address of the unit is 10.10.200.1. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Netmask—**This is the network subnet mask assigned by the network administrator. In the form "xxx.xxx.xxx.xxx." Refer to Table 2-2 for a list of subnet mask values).
- **IPv4 Gateway—**The gateway (default router) address is needed if communication to the unit is made outside of the local network. By default, the gateway is disabled.

- **Enable DHCPv6**—Check this box to enable the delivery of IP addresses from a DHCP Server using the DHCPv6 protocol.

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

IPv6 addresses may be added and deleted by clicking the **Edit IPv6 Address** button at the bottom of the screen.



- **Enable SLAAC**—Check this box to enable stateless address autoconfiguration.
- **IPv6 Gateway**—The gateway (default router) address is needed if communication to the unit is made outside of the local network. By default, the gateway is disabled. In the format "####.####.####.####.####.####.####.####," where each '#' is a hexadecimal value.

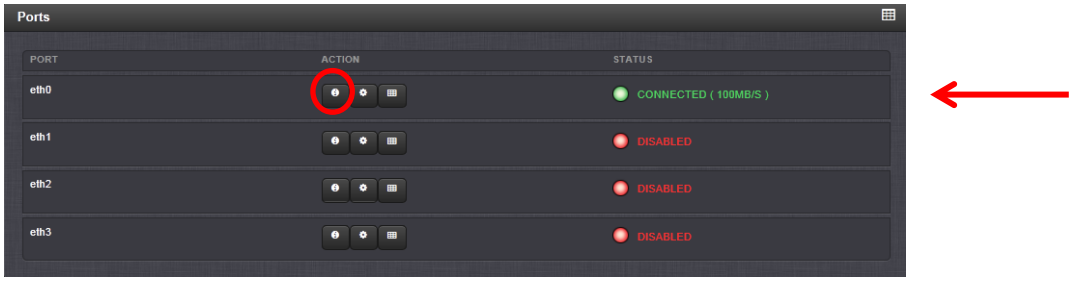
7. Click the **Apply** button or the **Submit** button at the bottom of the screen.

Viewing the Settings of a Networking Port

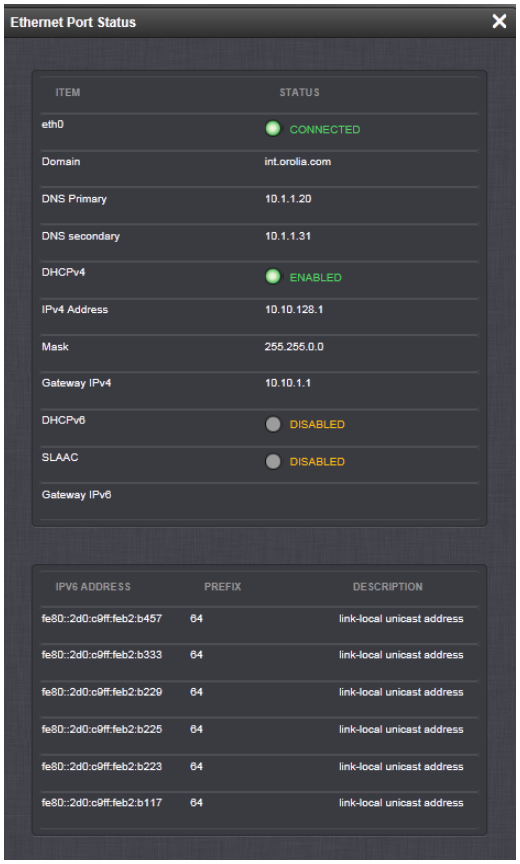
To view the settings of a networking port:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.

2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



3. In the **Ports** panel, locate the port you want to configure and select the  button.
4. The **Ethernet Port Status** window will display.



The following configurations can be viewed:

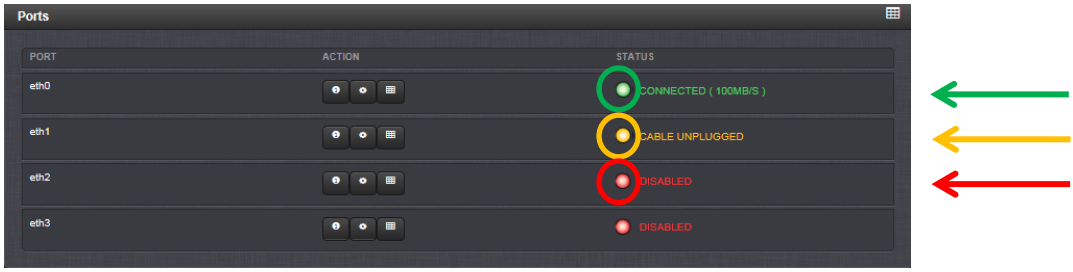
- The port number (the built in port is designated eth0. The status will be one of:
  - **CONNECTED** (showing the connection speed) in green.
  - **DISABLED** in orange.
  - **CABLE UNPLUGGED** (the port is enabled but there is not cable attached) in orange.
- **Domain**—This is the domain name associated with this port.

- **DNS Primary**—This is the primary DNS address used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Primary is set manually.
- **DNS Secondary**—This is the secondary DNS address used for this port. This is set automatically if DHCP is enabled. When DHCP is disabled, DNS Secondary is set manually.
- **DHCPv4**—This will show either "on" ("ENABLED" in green) or "off" ("DISABLED" in orange).
- **Static IPv4 Address**—This is the unique address assigned to the unit by the network administrator to be used when DHCP is disabled.
- **Mask—**This is the network subnet mask assigned to the unit by the network administrator to be used when DHCP is disabled.
- **Gateway IPv4—**The gateway (default router) address is needed if communication to the unit is made outside of the local network to be used when DHCP is disabled. By default, the gateway is disabled.
- **DHCPv6**—This will show either "on" ("ENABLED" in green) or "off" ("DISABLED" in orange).
- **SLAAC**—This will show either "on" ("ENABLED" in green) or "off" ("DISABLED" in orange).
- **Gateway IPv6**—When a DHCP server is not requested or is requested but not available and DHCPv6 is enabled, the server will use this Default Gateway.

Viewing the Connection Status of a Networking Port

To view the status of a networking port:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



3. In the **Ports** panel, you can see the connection status of each Ethernet port available. The three possible statuses are:

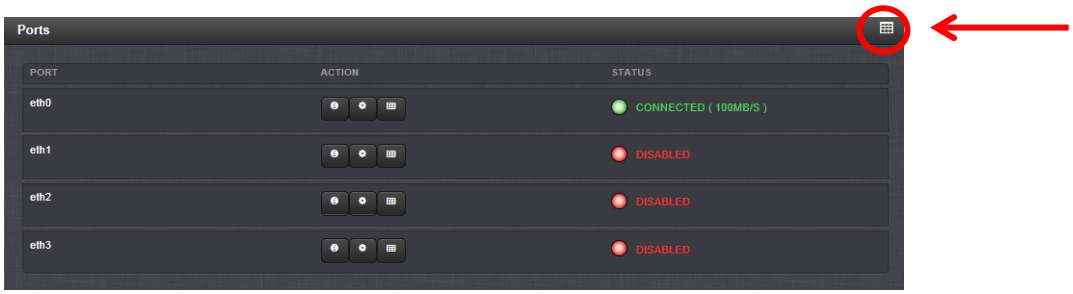
    - **CONNECTED** (showing the connection speed) in green.
    - **DISABLED** in red.
    - **CABLE UNPLUGGED** (the port is enabled but there is not cable attached) in orange.

Viewing Static Routes

To view the unit's Static Routes:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.

2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



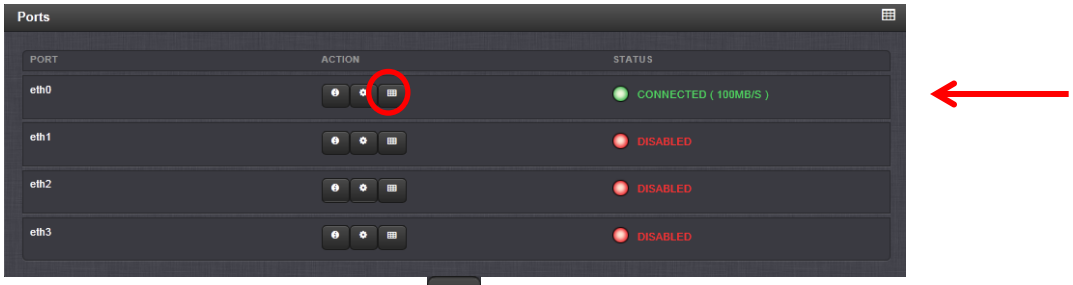
3. In the **Ports** panel, click the  button in the upper right-hand corner.
4. The **Static Routes** window will display.

5. In the **Static Routes** window, you can see the static routes table.

Adding Static Routes to the Routing Table

To add a static route to the routing table:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



3. In the **Ports** panel, click the  button in the row representing the port for which you wish to create a static route.

4. The **Static Routes** window will display.

NOTE: The **eth0** port is the default port for static routing. If a port is not given its own static route, all packets from that port will be sent through the default.

5. In the **Add Route** panel, fill in the fields.
   - **Net Address—**This is the router to which the port connects.
   - **Prefix—**This is the subnet mask in prefix form. See **2.8 Connecting Reference Inputs and Network Interface** for information on subnet masks.
   - **Router Address—**This is the IPv4 Gateway address.
6. Click the **Add Route** button at the bottom of the screen.

NOTE: In order for you to set up a static route, the Ethernet connector must be physically connected to the network.

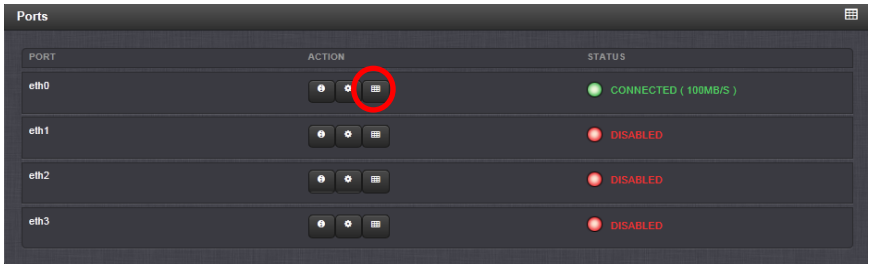
7. To delete a static address, click the **Delete** button in the entry for that address in the **ACTION** column of the **Static Routes** panel.

Viewing a Port's Routing Table

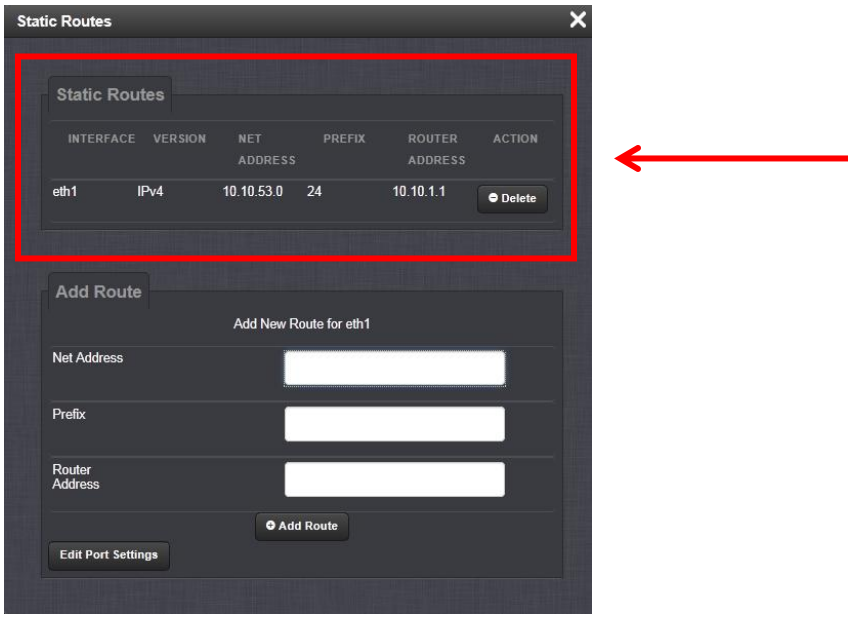
To view a port's routing table:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.

2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



3. In the **Ports** panel, locate the port you want to configure and select the  button.
4. The **Static Routes** window will display.

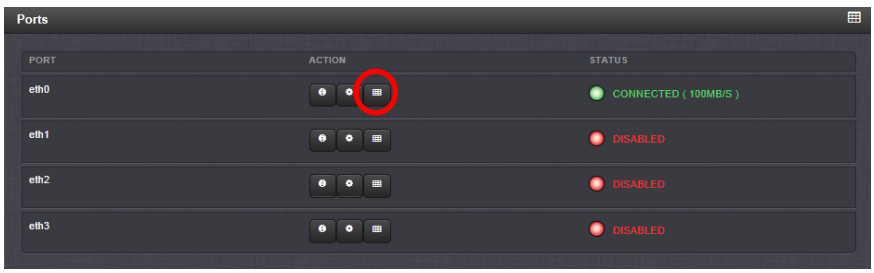


5. The **Static Routes** panel displays the port's routing table.

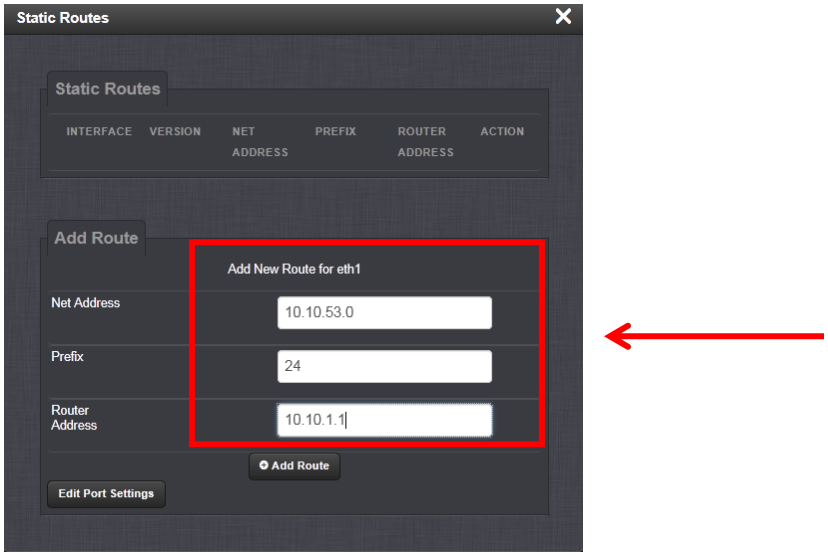
Adding/Deleting a Static Route to a Port

To add an interface route to a port's routing table:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. The **Ports** panel will show the Ethernet ports you have available and their connection status.



3. In the **Ports** panel, locate the port you want to configure and select the  button.
4. The **Static Routes** window will display.



5. Fill in the fields as required. The fields are:
   - **Net Address**—This is the router to which the port connects.
   - **Prefix**—This is the subnet mask in prefix form. See **2.8 Connecting Reference Inputs and Network Interface** for information on subnet masks.
   - **Router Address**—This is the IPv4 Gateway address.
6. Click the **Add Route** button at the bottom of the screen.

NOTE: In order for you to set up a static route, the Ethernet connector must be physically connected to the network.

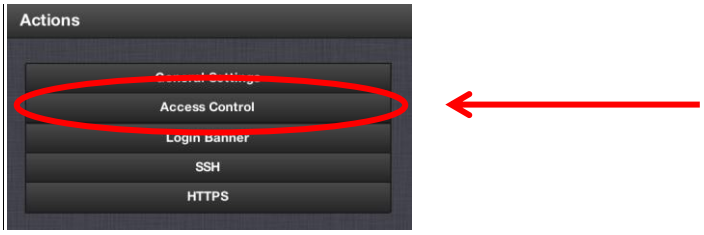
7. To delete a static address, click the **Delete** button in the entry for that address in the **ACTION** column of the **Static Routes** panel.

Configuring Network Access Rules

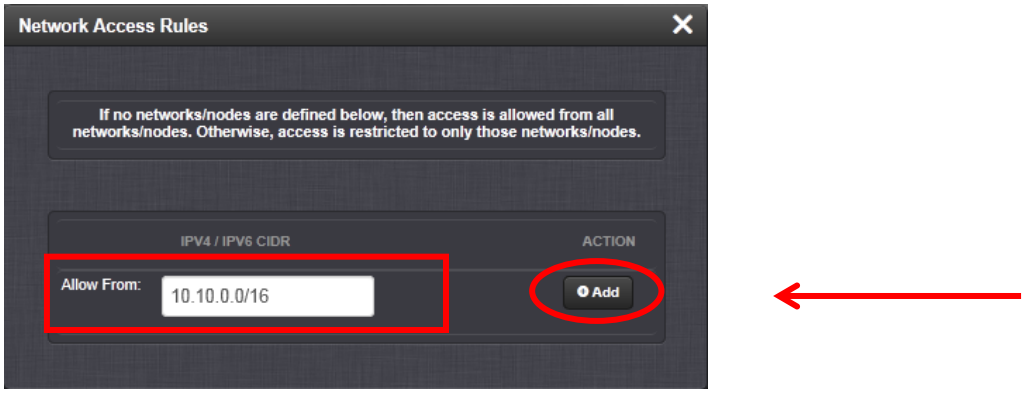
To configure access restrictions from assigned networks or nodes:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.

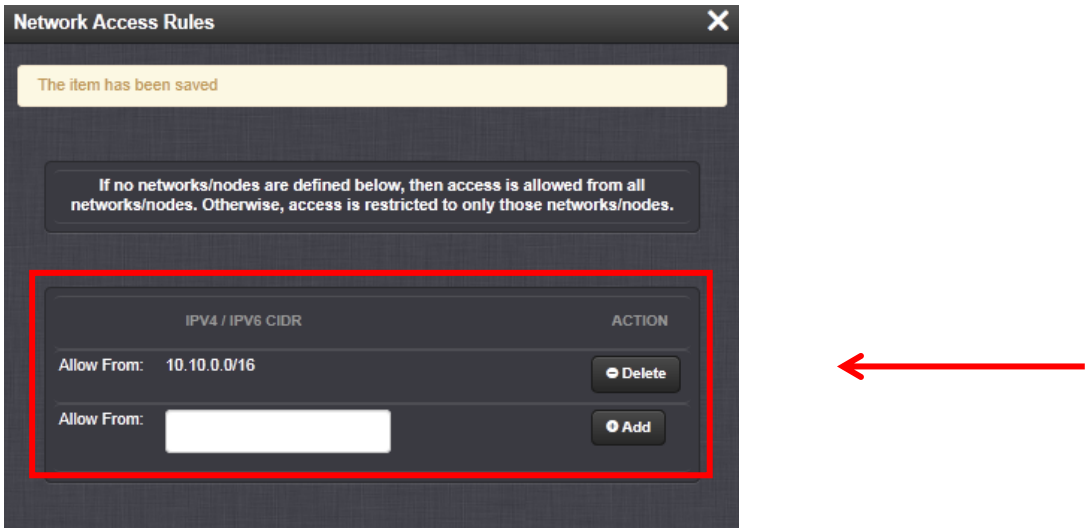
2. In the **Actions** panel, click on **Access Control**.



3. The **Network Access Rules** pop-up window displays.



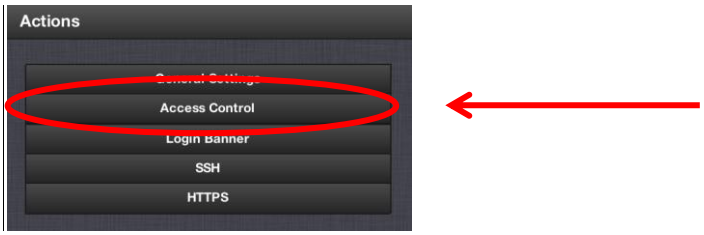
4. Enter a valid IP address in the **Allow From** field.
   - The address entered can be use IPv4, IPv4 CIDR, IPv6, or IPv6 CIDR addresses (meaning individual IP addresses or IP address ranges), e.g.:
     - IPv4—`10.10.0.0/16`, where `10.10.0.0` is the IP address and `16` is the subnet mask in prefix form. See **2.8 Connecting Reference Inputs and Network Interface** for information on subnet masks.
     - IPv6—`2001:db8::/48`, representing 2001:db8:0:0:0:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff.
5. Click the **Add** button in the **Action** column.
6. The established rule appears in the **Network Access Rules** window.



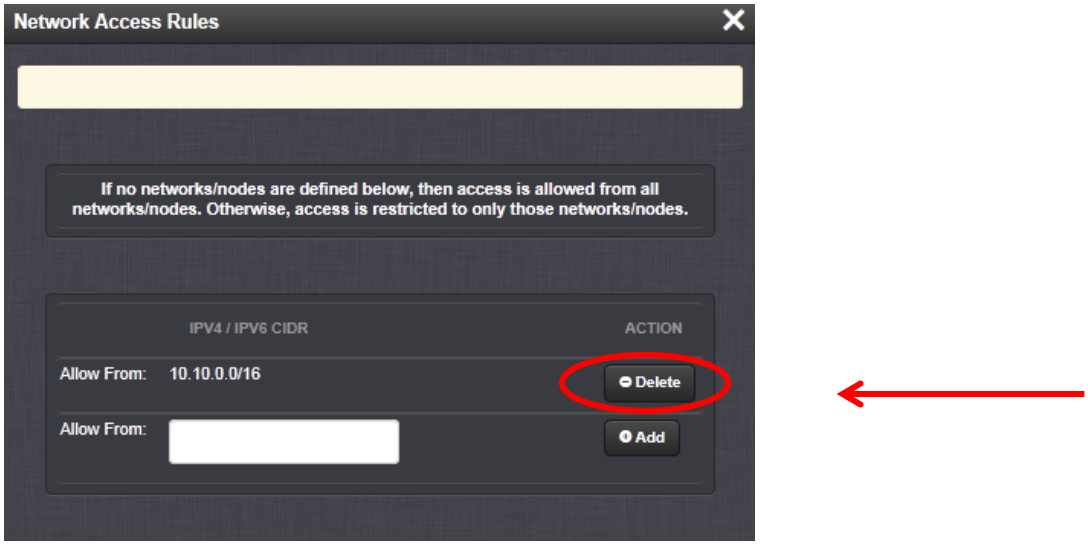
Deleting Network Access Rules

To delete access restrictions from assigned networks or nodes:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. In the **Actions** panel, click on **Access Control**.



3. Locate the rule you wish to delete and click the **Delete** button corresponding to that rule.

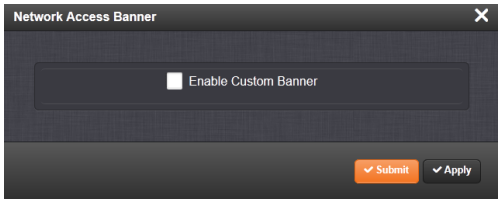


Configuring the Login Banner

To configure a custom banner message to be displayed on the login page:

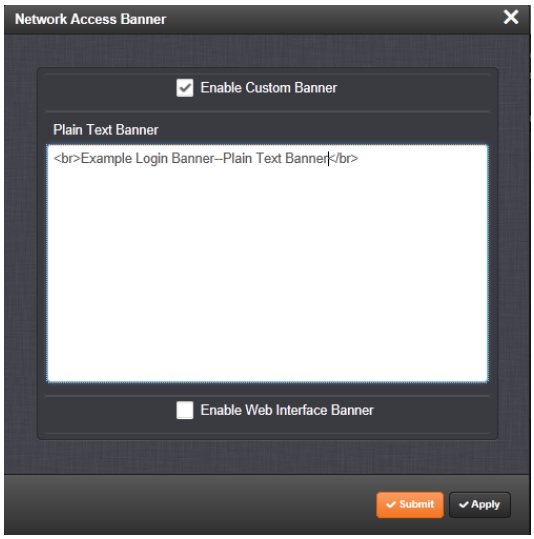
1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. In the **Actions** panel, click on **Login Banner**.

3. The **Network Access Banner** screen will display.



4. Select the **Enable Custom Banner** box.
5. In the **Plain Text Banner** text box type in the custom text you wish to appear on the login screen.

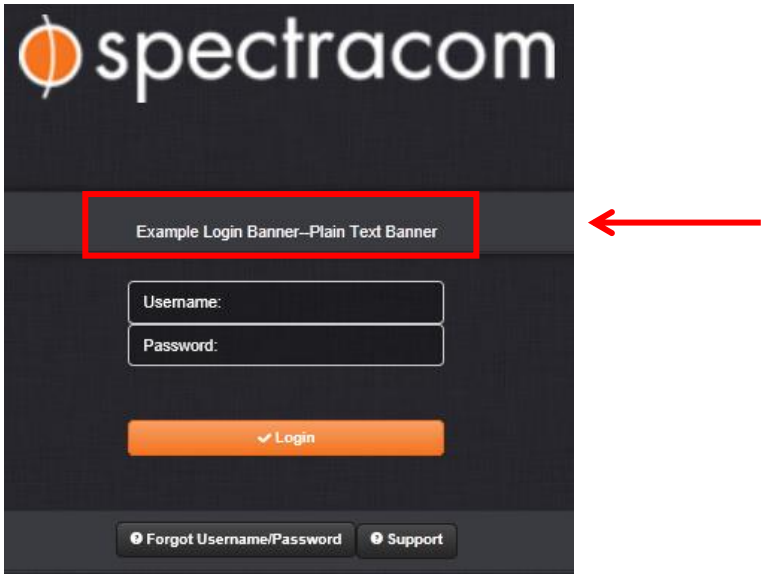
NOTE: The plain text banner is used for all interactive login interfaces (web UI, telnet, SSH, FTP, SFTP, serial, etc.). It is not required to include HTML tags. The web interface banner is used to include a web UI specific banner that can include HTML tags and be more complex than would be effective on other interactive interfaces.



6. Click the **Submit** or **Apply** button at the bottom of the window.
7. To test your new banner:
   - Log out using the **LOG OUT** button at the top of the Web interface screen.

   - Click the **LOG IN** button at the top of the web interface screen.

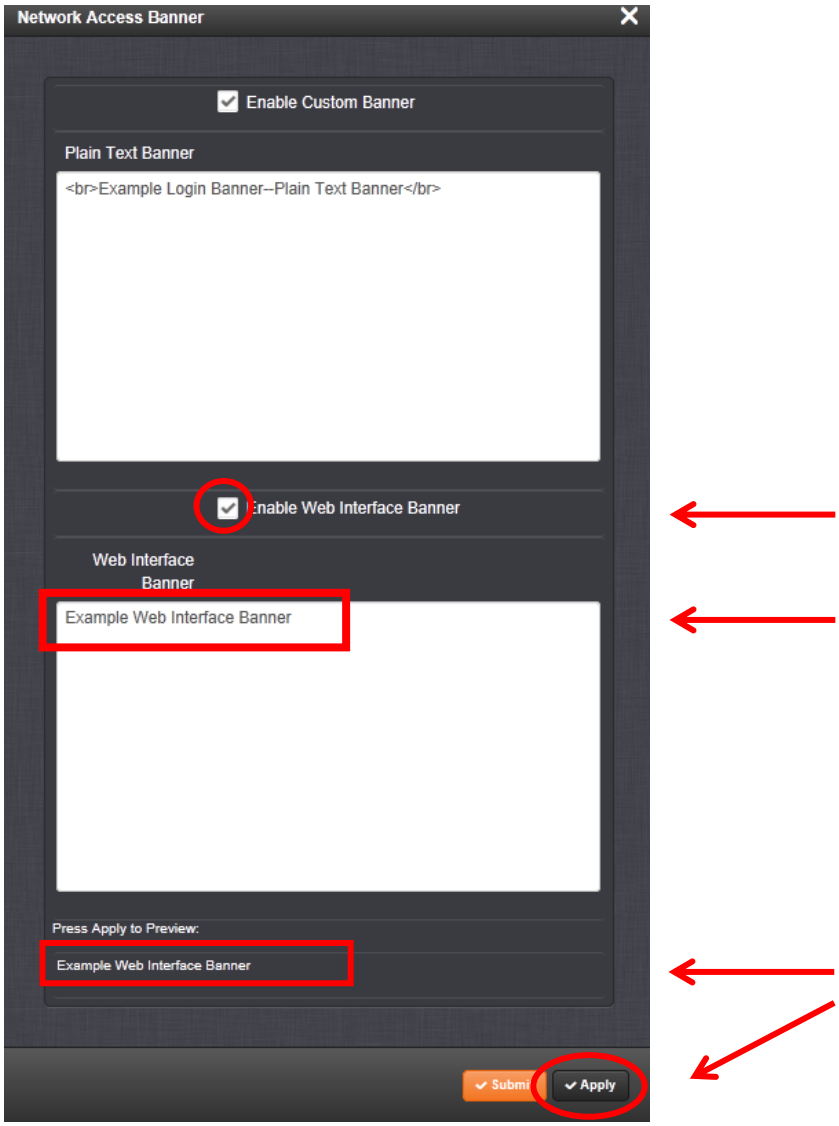
- The banner will appear above the log in fields.



You can also set up a Web interface banner. To set up a Web interface banner:

1. Follow steps 1 through 5 above.
2. On the **Network Access Banner** screen, select on the **Enable Web Interface Banner** button at the bottom of the screen.
3. The **Web Interface Banner** text box will display.
4. Enter the text you wish to appear on the Web interface login screen.

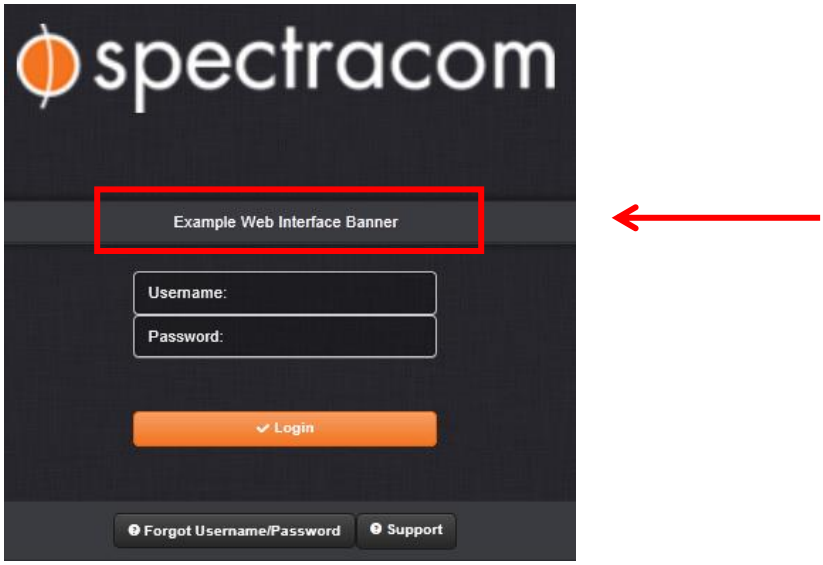
NOTE: Text entered in the Web Interface Banner text box does not need HTML tagging.



5. Click on the **Apply** button to see a preview of your entered text at the bottom of the window.
6. To test your new banner:
   - Log out using the **LOG OUT** button at the top of the Web interface screen.

   - Click the **LOG IN** button at the top of the Web interface screen.

- The banner will appear above the log in fields.



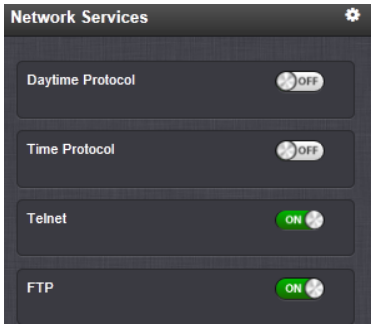
3.5.3 Enabling/Disabling Network Services

The following network services can be enabled or disabled through the **Network Services** panel of the **Network Management** screen:

- Daytime Protocol
- Time Protocol
- Telnet
- FTP
- SSH
- HTTP
- HTTPS

To enable or disable a network service:

1. Navigate to the **Network Management** screen through the **MANAGEMENT/NETWORK** dropdown menu.
2. In the **Network Services** panel, use the switch to enable or disable the network service.
   - ON=enabled.
   - OFF=disabled.



3.6 Network Setup Pages

3.7 Configuring Network Security

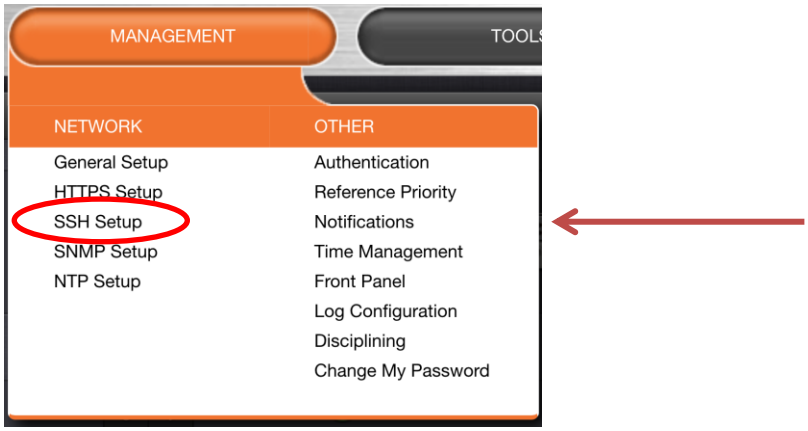
Spectracom NetClock uses OpenSSH and OpenSSL. OpenSSH is the Open Source version of the Secure Shell; which provides a set of server side tools allowing secure remote telnet like access and secure file transfer using remote copy (like SCP and FTP/SFTP). OpenSSL is the Open Source version of Secure Sockets 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 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.

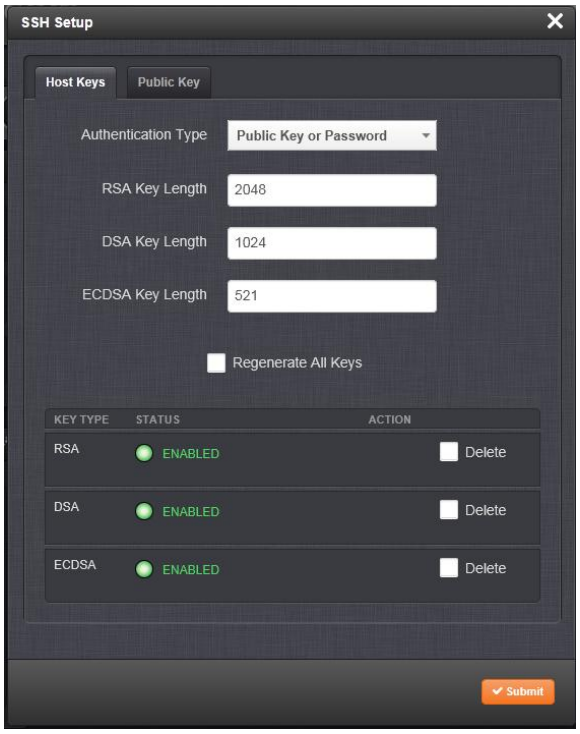
3.7.1 Configuring SSH

Accessing the SSH Setup Screen

To access the **SSH Setup** screen, choose **MANAGEMENT/NETWORK/SSH Setup**.



The SSH Setup Pop-up Screen will display.



The window contains 2 tabs.

- **Host Keys**—SSH uses Host Keys to uniquely identify each SSH server. Host keys are used for server authentication and identification.
- **Public Key**—This is a text field interface that allows the user to edit the public key files `authorized_keys` file.

NOTE: You can exit the **SSH Setup** Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **SSH Setup** window while filling out the Certificate Request Parameters form before you have hit the **Submit** button, any information you entered will not be retained. If you switch between tabs with the **SSH Setup** window, the information you have entered will be retained until you either leave the **SSH Setup** window or click the **Submit** button.

NetClock and SSH

The SSH tools supported by the unit are:

- **SSH**—Secure Shell
- **SCP**—Secure Copy
- **SFTP**—Secure File Transfer Protocol

The unit implements the server components of SSH, SCP, and SFTP.

For more information on OpenSSH, please 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: Only SSH2 is supported. SSH1 protocol is not supported, due to vulnerabilities.

The user may choose to delete individual RSA or DSA host keys.

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.

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.

NetClock units have their initial host keys created at the factory. RSA 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 of up to 4096 are supported, but may take 10 minutes or more to generate. DSA keys size support is limited to 1024 bits.

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, 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, the default key bit length size used is 2048. A key with a zero length or blank key size field is not created.

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 either by 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 unit 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

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

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.

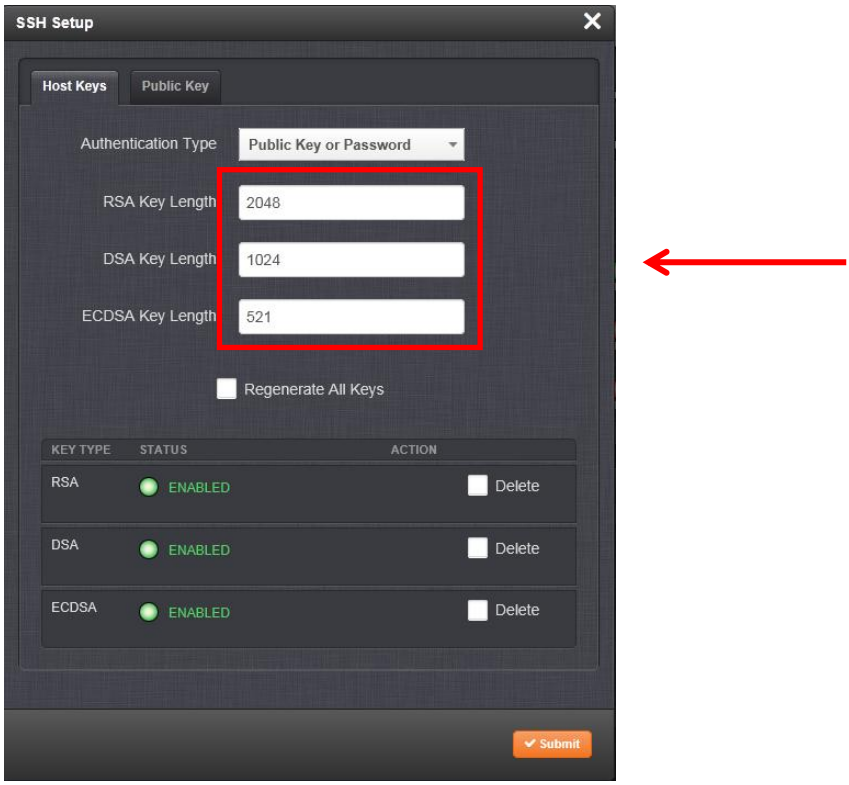
NOTE: The file format, line terminations, and other EOL or EOF characters should correspond to UNIX conventions, not Windows.

Changing Key Length Values

The user may change the key length of the RSA host key, the DSA host key and/or the ECDSA host key.

To change the key length of a host key:

1. To access the **SSH Setup** screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select the value of the key length you want to change



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 of up to 4096 are supported, but may take 10 minutes or more to generate. DSA keys size support is limited to 1024 bits.

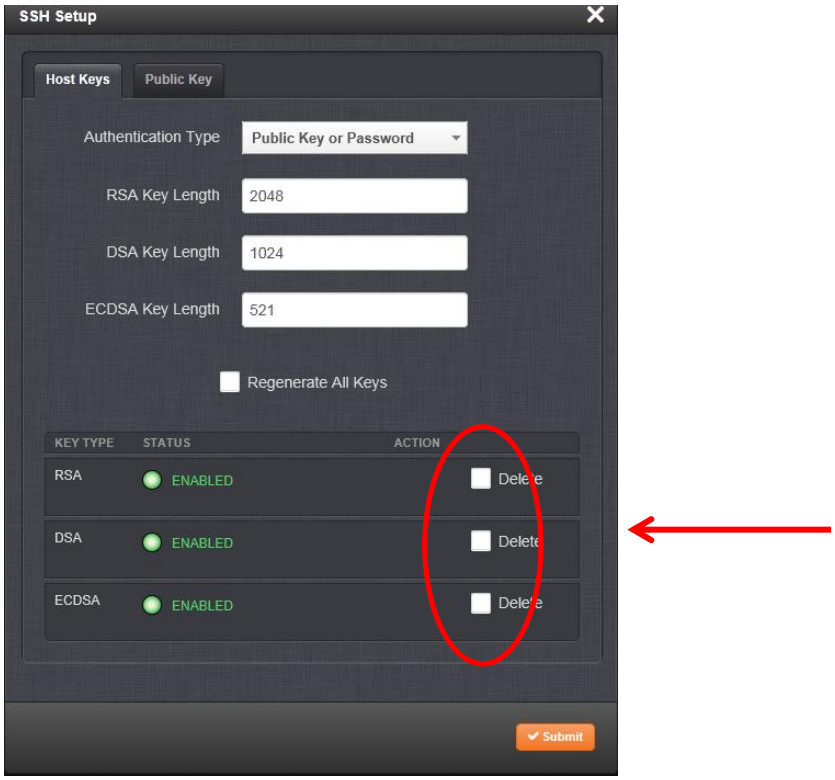
3. Click the **Submit** button at the bottom of the screen. The new values will be saved.

NOTE: Changing the values and submitting them in this manner DOES NOT generate new host public/private key pairs. See **0 Creating Host Public/Private Key Pairs** for information on how to create new host public/private key pairs.

Deleting Host Keys

The user may choose to delete individual RSA or DSA host keys. To delete a key:

1. To access the **SSH Setup** screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select **Delete** in the field for the key you wish to delete.



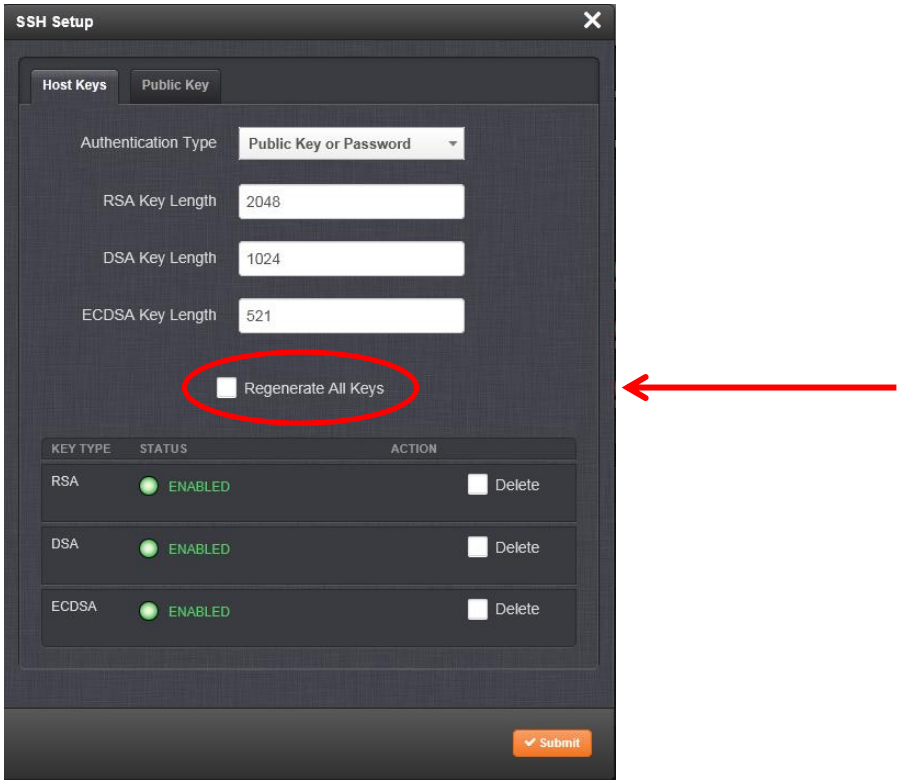
3. Press the **Submit** button at the bottom of the page.

NOTE: You can exit the **SSH Setup** Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **SSH Setup** window before you have hit the **Submit** button, any information you entered will not be retained. If you switch between tabs with the **SSH Setup** window, the information you have entered will be retained until you either leave the **SSH Setup** window or click the **Submit** button.

Creating Host Public/Private Key Pairs

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:

1. To access the SSH setup screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. If you want to change the key length of any host key, enter the desired length in the text field corresponding to the length you wish to change**.** See **0 Changing Key Length Values**.



3. Check the **Regenerate All Keys** box.
4. Click the **Submit** button at the bottom of the page.
   The Key Type/Status/Action table will temporarily disappear while the unit regenerates the keys. The 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, ECDSA.
   The unit will generate all 3 host keys, the RSA key, the DSA key and the ECDSA key.
5. Delete any of the keys you do not want. See **0 Deleting Host Keys**.

NOTE: 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 the previously specified key sizes. If a key size is undefined, the default key bit length size used is 2048. A key with a zero length or blank key size field is not created.

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 then either have to:

1. Override the warning and accept the new Public Host Key and start a new connection.
   This is the default. This option allows users to login using either method. 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.
2. Remove the old Host Public Key from their client system and accept the new Host Public Key
   This 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.
3. Load a public key into the unit. 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.

Please consult your specific SSH client's software's documentation.

Viewing, Editing and Loading Public Keys in the _authorized_keys File

Using the Web, the user can view and edit the **`authorized_keys`** file, so that the user can add and delete Public Keys. The user may also retrieve the **`authorized_keys`** file from the .ssh directory Using FTP, SCP, or SFTP.

If a user wants to completely control the public keys used for authentication, a correctly formatted `authorized_keys` file formatted as indicated in the OpenSSH web site can be loaded onto the product. The user can transfer a new public key file using the web interface.

To view and edit the `authorized_keys` file:

1. To access the SSH setup screen, choose **MANAGEMENT/NETWORK/SSH Setup**. The window will open to the **Host Keys** tab by default.
2. Select the **Public Key** tab.

3. The authorized_keys file appears in the **Public Keys File** window.

4. Edit the authorized_keys file as desired.
5. Click the **Submit** button or **Apply** button.

NOTE: Clicking the **Apply** button will apply the settings and will not close the **NTP Peer** window, allowing you to switch between tabs.

Clicking the **Submit** button will close the **NTP Peer** window.

The file is to be formatted such that the key is followed by an 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.

NOTE: 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.

Editing the `authorized_key` File Using the Command Line

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 spadmin@10.10.200.5
spadmin@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 spadmin@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.

Secure File Transfer Using SCP and SFTP

NetClock provides secure file transfer capabilities using the SSH client tools SCP and SFTP. Authentication is performed using either Account Passwords or Public Key with Passphrase.

Example output from 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
spadmin@10.10.200.135's password: admin123

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

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

```
scp -i ./id_rsa spadmin@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 spadmin@10.10.200.5
spadmin@10.10.200.135's password: admin123

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 spadmin@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.

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/.

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.

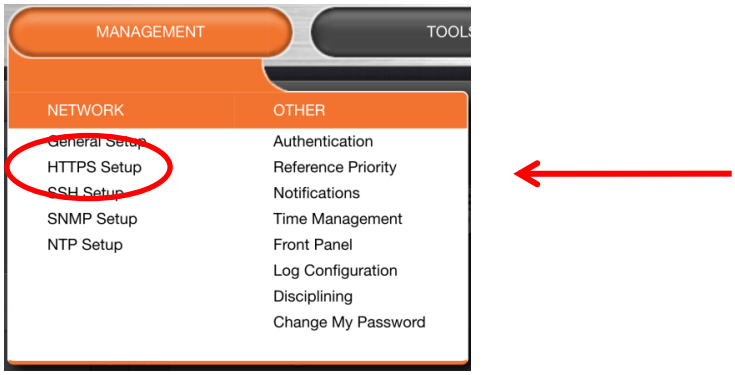
The putty SSH tools and instructions regarding their use can be found at: http://www.chiark.greenend.org.uk/~sgtatham/putty/

3.7.2 Configuring HTTPS

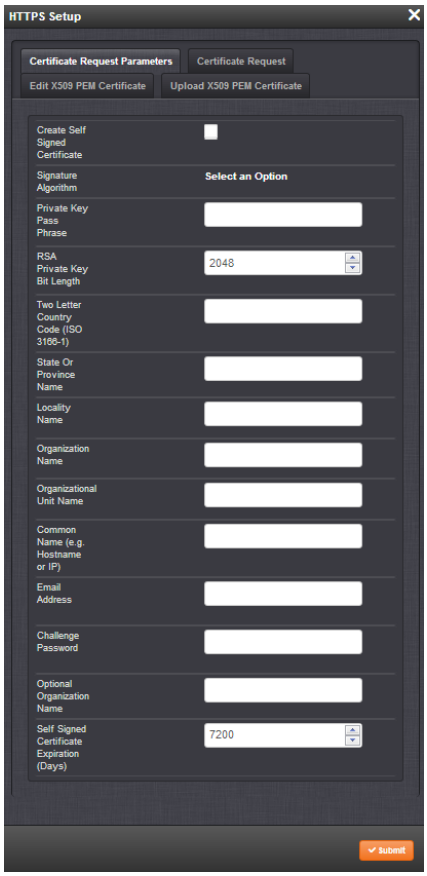
Accessing the HTTPS Setup Screen

To access the **HTTPS Setup** screen:

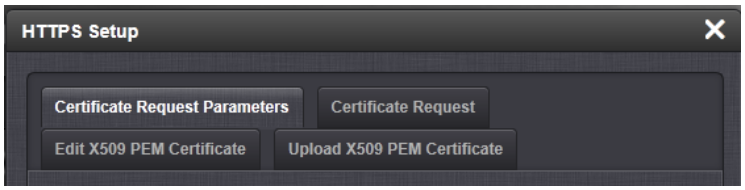
1. Choose **MANAGEMENT/NETWORK/HTTPS Setup**.



2. The **HTTPS Setup** window will appear as a pop-up window.



- The window contains 4 tabs:



- **Certificate Request Parameters**—A GUI interface that uses the OpenSSL library to create certificate Requests and self-signed certificates.
- **Certificate Request**—A holder for the certificate request generated under the Certificates Request Parameters tab. This request is sent to the Certificate Authority.
- **Upload X509 Certificate**—The certificate returned by the Certificate Authority is uploaded under this tab.
- **Edit X509 PEM Certificate**—The certificate used by the unit is stored here.

NOTE: You can exit the **HTTPS Setup** window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **HTTPS Setup** window while filling out the Certificate Request Parameters form before you have hit the **Submit** button, any information you entered will not be retained. If you switch between tabs with the **HTTPS Setup** window, the information you have entered will be retained until you either leave the **HTTPS Setup** window or click the **Submit** button.

NetClock and HTTPS

HTTPS provides secure/encrypted, web-based management and configuration of unit from a PC. An SSL certificate is required to be in the unit in order to make this secure HTTPS connection.

The unit 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 Certificate Authority. If a Certificate Authority is not available the user can simply use the self-signed certificate that comes with the unit until it expires or create their own self-signed certificates to allow the use of HTTPS.

Each unit comes with a default Spectracom self-signed SSL certificate. The typical life span of a certificate is about 10 years. HTTPS is available using this certificate until this certificate expires.

NOTE: If deleted, the HTTPS certificate cannot be restored. A new certificate will need to be generated.

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 each time you login.

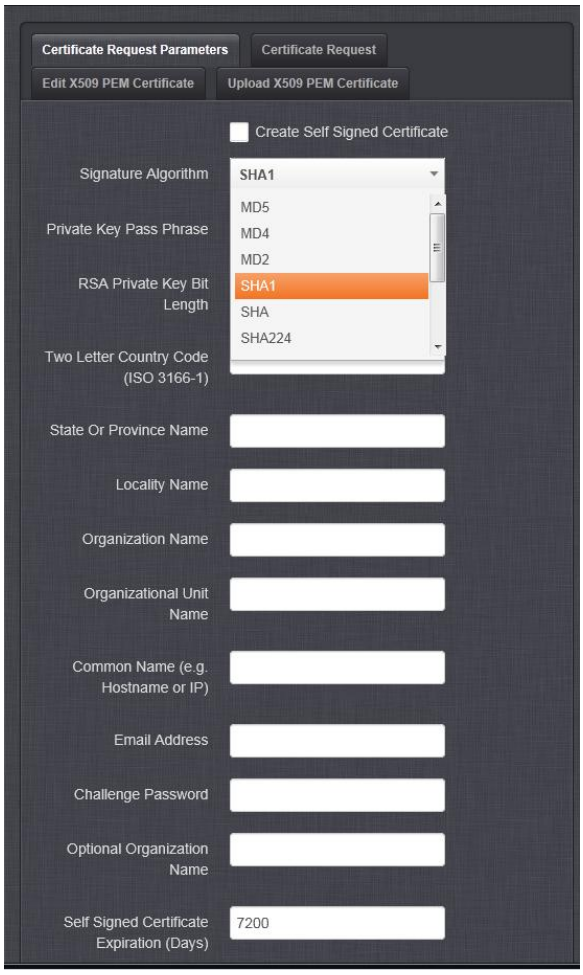
The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS). The OpenSSL package also provides tools and software for creating X.509 Certificate Requests, Self Signed Certificates and Private/Public Keys. For more information on OpenSSL, please see www.openssl.org.

The unit's software supports X.509 DER and PEM and P7 PKCS#7 PEM and DER formatted certificates. The user can create a customer specific X.509 self-signed certificate, an RSA private key and X.509 certificate request using the web interface. RSA private keys are supported because they are the most widely accepted (at this time, DSA keys are not supported).

Creating an HTTPS Certificate Request

To create an HTTPS Certificate Request:

1. Navigate to the **MANAGEMENT/NETWORK/HTTPS Setup** screen and fill in the available fields.



2. Choose the **Certificate Request Parameters** tab (this should be the default page).
3. Fill in the available fields:
   - **Create Self Signed Certificate**—Check this box if the Certificate you are creating is a self signed certificate.
   - **Signature Algorithm**—Choose the algorithm to be used from:
     - SHA1
     - MD5
     - MD4
     - MD2
     - SHA
     - SHA224
     - SHA256
     - SHA384
     - SHA512

- **Private Key Pass Phrase**—This is the RSA decryption key. This must be at least 4 characters long.
- **RSA Private Key Bit Length**—2048 bits is the default. Using a lower number may compromise security and is not recommended.
- **Two-Letter Country Code**—This code should match the ISO-3166-1 value for the country in question.
- **State Or Province Name**—From the address of the organization creating up the certificate.
- **Locality Name**—Locale of the organization creating the certificate.
- **Organization Name**—The name of the organization creating the certificate.
- **Organization Unit Name**—The applicable subdivision of the organization creating the certificate.
- **Common Name (e.g. Hostname or IP)**—This is the name of the host being authenticated. The Common Name field in the X.509 certificate must match the hostname, IP address, or URL used to reach the host via HTTPS.
- **Email Address**—This is the email address of the organization creating the certificate.
- **Challenge Password**—Valid response password to server challenge.
- **Optional Organization Name**—An optional name for the organization creating the certificate.
- **Self Signed Certificate Expiration (Days)**—How many days before the certificate expires. The default is 7200.

The user is required to select a signature algorithm, a private key passphrase of at least 4 characters, a private key bit length, the certificate expiration in days, and the rest of the remaining fields.

It is recommended that the user consult their Certificate Authority for the required fields in an X.509 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 to avoid problems the Certificate Authority might otherwise have reconciling certificate request and company record information.

If necessary, consult your web browser vendor's documentation and Certificate Authority to see which key bit lengths and signature algorithms your web browser supports.

Spectracom recommends that when completing the Common Name field, the user provide a static IP address, because DHCP-generated IP addresses can change. If the hostname or IP address changes, the X.509 certificate must be regenerated.

It is recommended that the RSA Private 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.

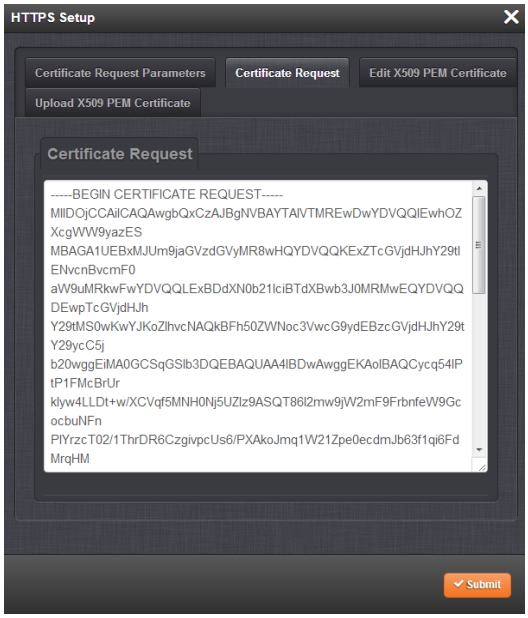
NOTE: The default key bit length value is 2048.

If using only self-signed certificates (see **0 Creating a Self Signed Certificate),** the user should choose values based on the company's security policy.

4. When the form is complete, click the **Submit** button. Clicking the **Submit** button automatically generates the Certificate Request in the proper format for submission to the Certificate Authority.

NOTE: It may take several minutes for the unit to create the certificate request and the private key. The larger the key, the longer amount of time is required. If a system is rebooted during this time, the certificate will not be created.

The generated request can be seen by choosing the **Certificate Request** tab in the **HTTPS Setup** window.



NOTE: If you switch between tabs while filling out the **Certificate Request Parameters** form, the information you entered will be retained until you exit the **HTTPS Setup** window or hit the **Submit** button.
If you exit the **HTTPS Setup** window, the information you entered will not be retained.

Creating a Self Signed Certificate

To create a Self Signed Certificate:

1. Under the Certificate Request Parameters tab in the HTTPS Setup Window, complete the form (see **0 Creating an HTTPS Certificate Request**).
2. Check the box marked Create Self Signed Certificate at the top of the form.
3. Click the **Submit** button at the bottom of the form.

A Self Signed Certificate will be generated simultaneously with the Certificate Request that is generated and then displayed under the **Certificate Request** tab. You may use Self Signed Certificate while waiting for the HTTPS Certificate from the Certificate Authority.

Requesting an HTTPS Certificate

To request an HTTPS Certificate:

1. Create the HTTPS Certificate Request by completing the Certificate Request Parameters form in the **MANAGEMENT/NETWORK/HTTPS Setup Window** (see **0 Creating an HTTPS Certificate Request**) and click the **Submit** button.
2. Select the **Certificate Request** tab in the **HTTPS Setup** window. Clicking the **Submit** button at the bottom of the Certificate Request Parameters form will have generated your Certificate Request. You can view the Certificate Request in **Certificate Request** window.

NOTE: If you wish to create a different or additional Certificate Request, you may fill out a new form under the Certificate Request Parameters tab, and the unit will automatically generate the new Certificate Request.
The newly generated Certificate Request will replace the Certificate Request previously generated. Therefore, if you wish to retain your previously generated Certificate Request for any reason, you will need to copy that request and save it in text document before you generate your new Certificate Request.

3. Copy the generated Certificate Request from the **Certificate Request** window and submit it per the guidelines of the Certificate Authority. The Certificate Authority will issue a verifiable, authenticable third party certificate.

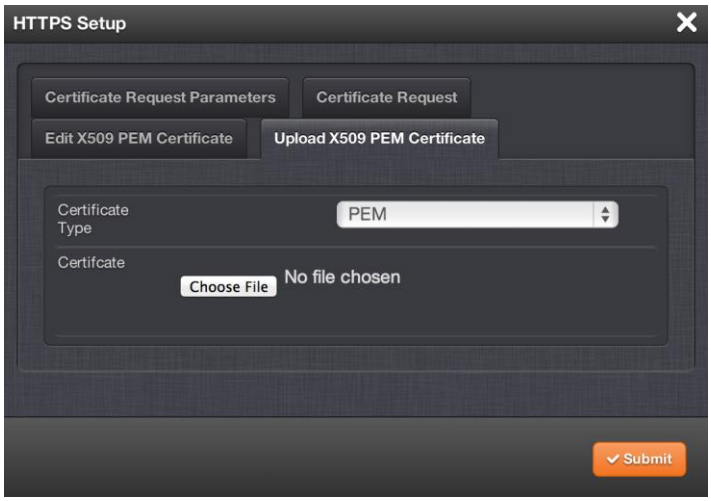
Until this certificate is received, the user's self-signed certificate may be used.

When the web interface is accessed from a Windows computer while the self-signed certificate is being used, the user's web browser will present a popup window. The certificate can be viewed by the user and installed through 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.

Uploading the X509 PEM Certificate

After the HTTPS Certificate has been issued by the Certificate Authority, the certificate needs to be loaded onto the unit. To upload the certificate:

1. Store the Public Keys File provided to you by the Certificate Authority in a location accessible from the computer on which you are running the Web interface.
2. Access the **MANAGEMENT/NETWORK/HTTPS Setup** window.
3. Choose the **Upload X509 PEM Certificate** tab.



4. Click the **Choose File** button and locate the Public Keys File provided by the Certificate Authority in its location where you stored it in step 1.
5. Click the **Submit** button.

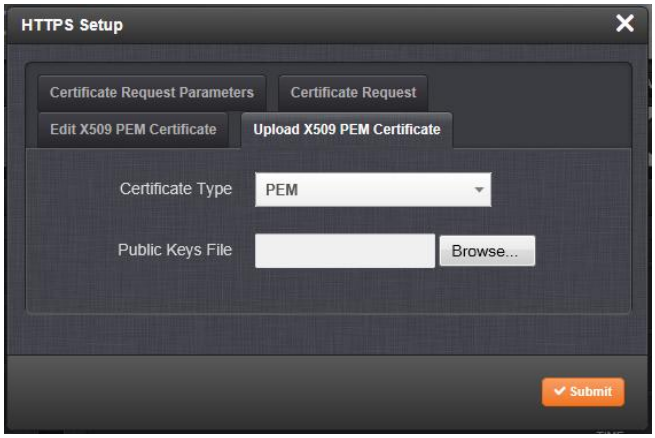
Once the X509 PEM Certificate has been loaded, it can be viewed by choosing the **Edit X509 PEM Certificate** tab in the **HTTPS Setup** window.

NOTE: The text inside the text box under the **Edit X509 PEM Certificate** tab is editable. However, changes should not be made to a certificate once it is imported. Instead, a new certificate should be requested. An invalid certificate may result in denial of access to the unit through the Web interface.

Loading an HTTPS Certificate that is not in the X.509.PEM format

After the HTTPS Certificate has been issued by the Certificate Authority, the certificate may not be in the X.509PEM format. To upload an HTTPS Certificate that is not in the X509.PEM format:

1. Store the Public Keys File provided to you by the Certificate Authority in a location accessible from the computer on which you are running the Web interface.
2. Navigate to the **MANAGEMENT/NETWORK/HTTPS Setup** window.
3. Choose the **Upload X509 PEM Certificate** tab.



4. Choose the Certificate Type for the HTTPS Certificate supplied by the Certificate Authority from the **Certification Type** drop-down:

NOTE: The user may choose one of the following alternate certificate types.
DER
PKCS7 PEM
PKCS7 DER

5. Click the **Browse…** button and locate the Public Keys File provided by the Certificate Authority in its location where you stored it in step 1.
6. Click Submit.

NOTE: The unit will automatically format the certificate into the proper format.

Once the X509 PEM Certificate has been loaded, it can be viewed by choosing the **Edit X509 PEM Certificate** tab in the **HTTPS Setup** window.

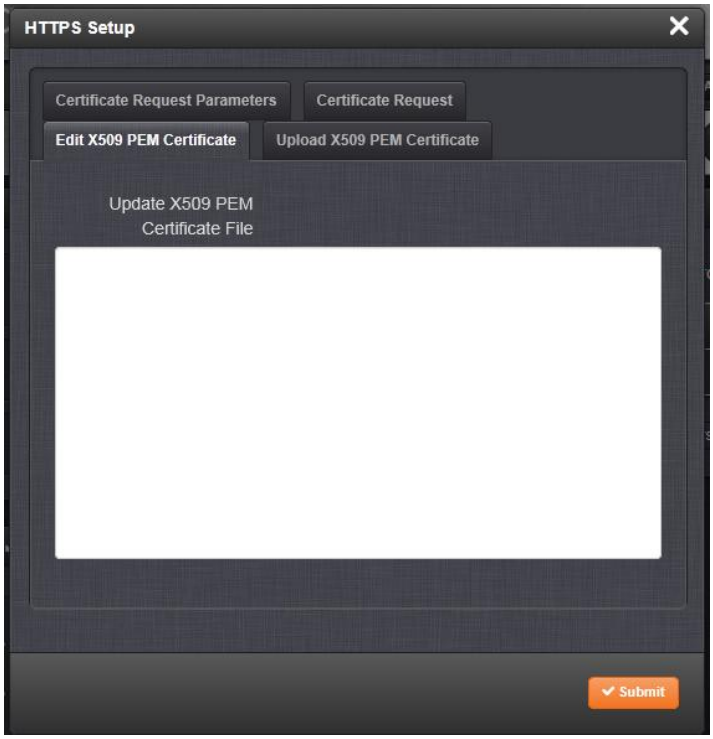
NOTE: The text inside the text field under the **Edit X509 PEM Certificate** tab is editable. However, changes should not be made to a certificate once it is imported. Instead, a new certificate should be requested. An invalid certificate may result in denial of access to the unit through the Web interface.

Manually Inserting the HTTPS Certificate from a Text File

Many certificate authorities simply provide you with a certificate in the form of a plain text file. If your certificate is provided in this manner, and the certificate is in the X.509 PEM format, you may simply copy and paste the text into the web interface:

1. Navigate to the **MANAGEMENT/NETWORK/HTTPS Setup** window.

2. Choose the **Edit X509 PEM Certificate** tab.



3. Copy the text of the certificate and paste it into the **Update X509 PEM Certificate File** text field.

NOTE: Only X.509 PEM certificates can be loaded in this manner.

NOTE: The text inside the text field under the **Edit X509 PEM Certificate** tab is editable. However, changes should not be made to a certificate once it is imported. Instead, a new certificate should be requested. An invalid certificate may result in denial of access to the unit through the Web interface.

3.7.3 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 recommended 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 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 NetClock, you must utilize the front panel keypad and LCD to restore the "spadmin" account's default password. The spadmin account can then be used to enable HTTPS using the "**`defcert`**" command. The "**`defcert`**" command generates a new self-signed SSL certificate. Refer to **2.9 Front Panel Keypad/LCD Operation (NetClock Model 9483)** for information on using the keypad and LCD display.

3.7.4 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.

Option / Feature	Default Setting	Recommended Setting	Where to Configure
HTTP	Enabled	Disabled	Web User Interface or Command Line Interface
HTTPS	Enabled (using customer-generated certificate and key or default Spectracom self-signed certificate and common public/private key SSH/SCP/SFTP enabled with unit unique 1024-bit keys)		Web User Interface
SNMP	Disabled	Disabled or Enabled (with SNMP v3 w/ encryption*)	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			
Serial Port	Available	Available	Not Applicable
Telnet	Enabled	Disabled (use SSH instead)	Web User Interface
SSH	Enabled (default private 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 3-1: Default and Recommended Configurations

3.8 Resetting NetClock to Factory Default Configuration

In certain situations, it may be desired to reset all configurations back to the factory default configuration. The GNSS location any configurations and the locally stored log files can be cleared via the web interface.

EXCEPTION: The Authentication logs and NTP logs cannot be cleared.

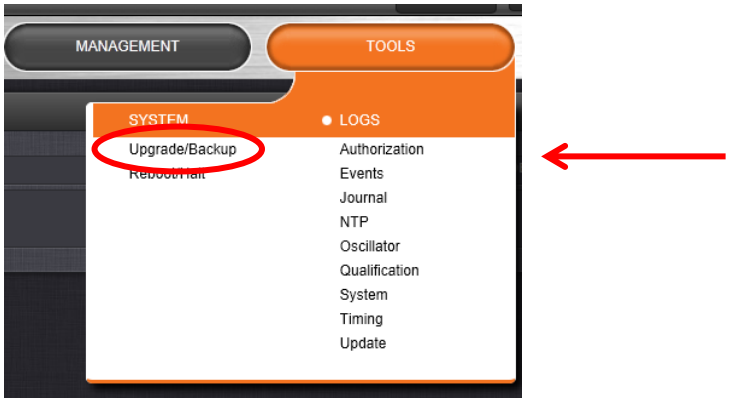
NOTE: Restoring configurations (reloading a saved configuration), erasing the stored GNSS location and clearing the log files are separate processes. You may restore one without restoring the others.

If the unit was assigned a static IP address before cleaning the configurations, it will be reset to DHCP after the clean has been performed. If no DHCP server is available after the clean operation, the static IP address will need to be manually reconfigured. Refer to **2.8 Connecting Reference Inputs and Network Interface**.

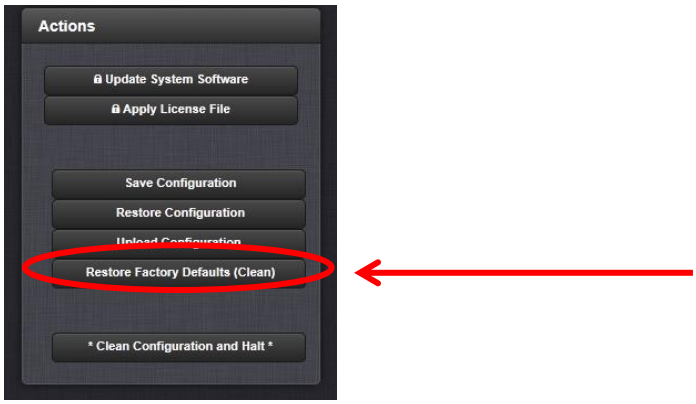
3.8.1 To reset all configurations back to the factory default settings:

To restore the configuration files to the factory defaults:

1. Navigate to **TOOLS/SYSTEM/Upgrade/Backup**.



2. In the **Actions** panel, click on the **Restore Factory Defaults (Clean)** button.



3. The unit restores the configuration files to the factory settings, and then reboots in order to read the new configuration files. Once powered back up, it will be configured with the previously stored file.

NOTE: While the GNSS position is stored and retained through power cycles, choosing Clean (Restore Factory Configuration) will erase the stored GNSS position.

If the GNSS location is erased, the next time that the GNSS antenna is connected and the GNSS receiver is able to continuously track at least four satellites, the 33 minute long GNSS survey will be performed again, so the position can be recalculated and locked-in.

3.9 Backing-up and Restoring Configuration and Log Files

Once the NetClock has been configured, it may be desired to backup the configuration or log files to a PC or other device for off-unit storage. If necessary in the future, the original configuration of the NetClock can then be restored to the same unit.

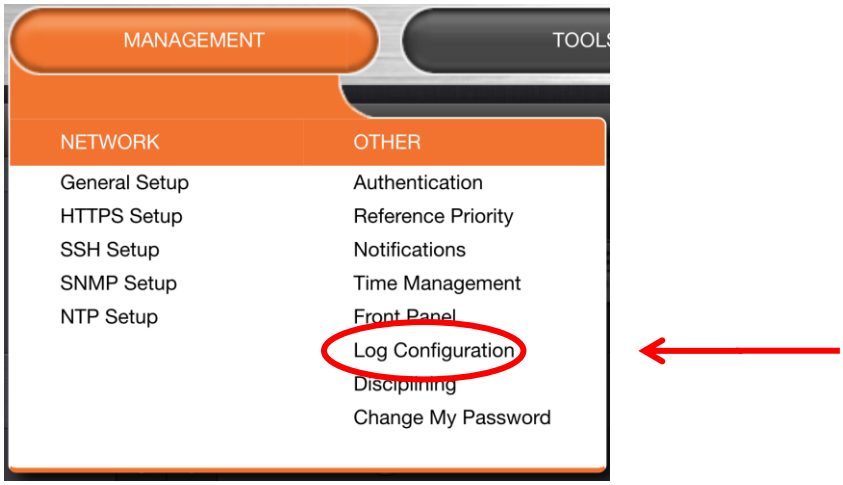
The capability to backup and restore configurations also adds the ability to "clone" multiple NetClock units with similar settings. Once one NetClock unit has been configured as desired, configurations that are not specific to each unit (such as NTP settings, log configs, etc) can be backed up and loaded onto another NetClock unit for duplicate configurations.

NOTE: For security reasons, configurations relating to security of the product, such as SSH/SSL certificates are not backed up to a PC.

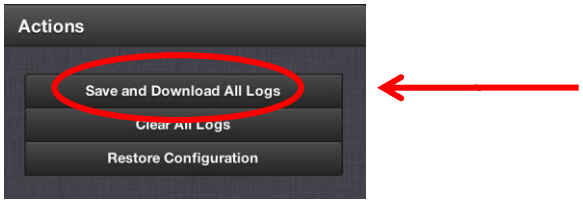
3.9.1 Saving and Downloading All Logs

To save and down all logs:

1. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



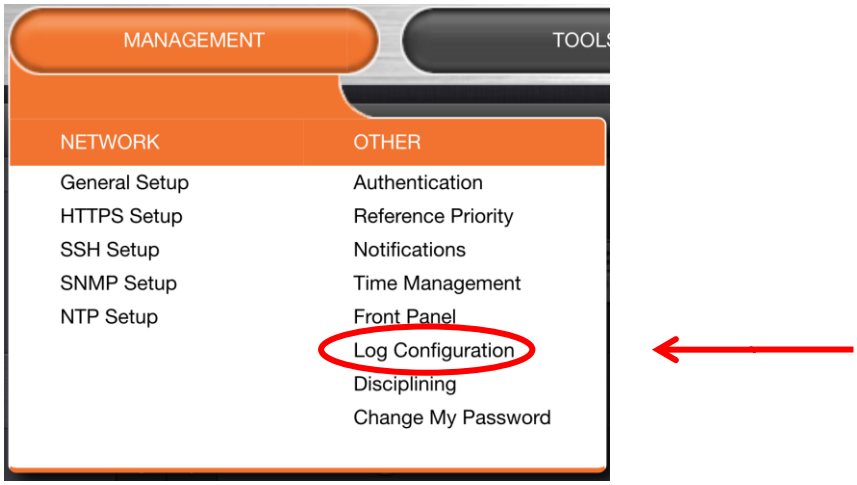
2. In the **Actions** panel, click on the **Save and Download All Logs** button.



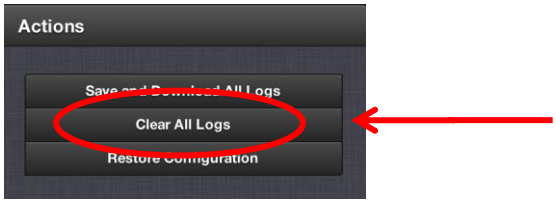
3.9.2 Clearing All Logs

To clear all the logs:

1. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



2. In the **Actions** panel, click on the **Clear All Logs** button.

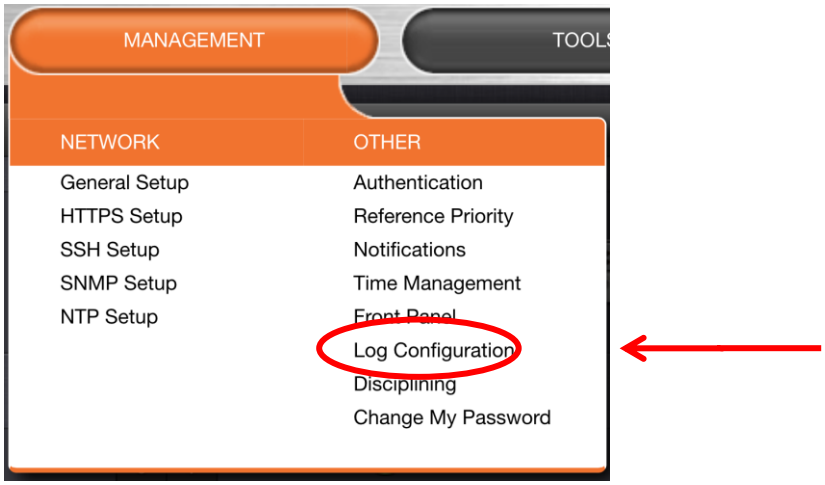


3. In the message window that displays, click **OK**.

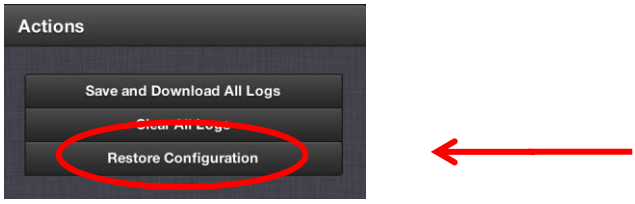
3.9.3 Restoring Log Configurations

To restore log configurations:

1. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



2. In the **Actions** panel, click on the **Restore Configurations** button.



3. Click the **Browse** button.
4. Navigate to the directory where the configurations are stored and click **Upload**.

3.10 Issuing the HALT Command before Removing Power

Once power is applied to the unit, it should not be removed unless the HALT command is issued to the unit. Using the Halt command to shut down the system can allow for faster startup after the next power-up of the unit.

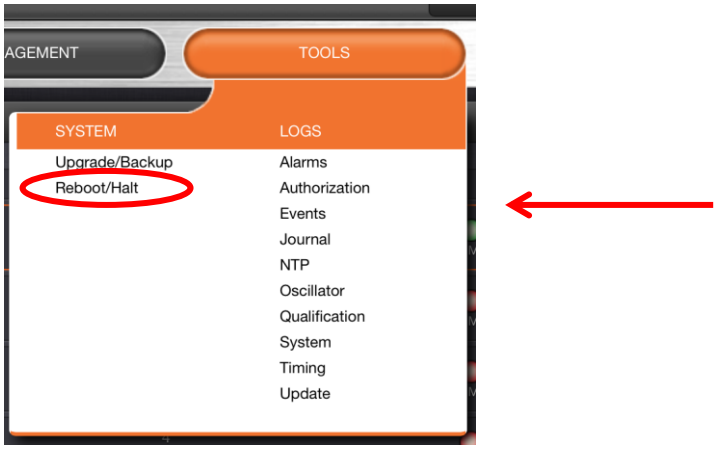
The HALT command may be issued through the web interface, the front panel serial port, or the front panel keypad.

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

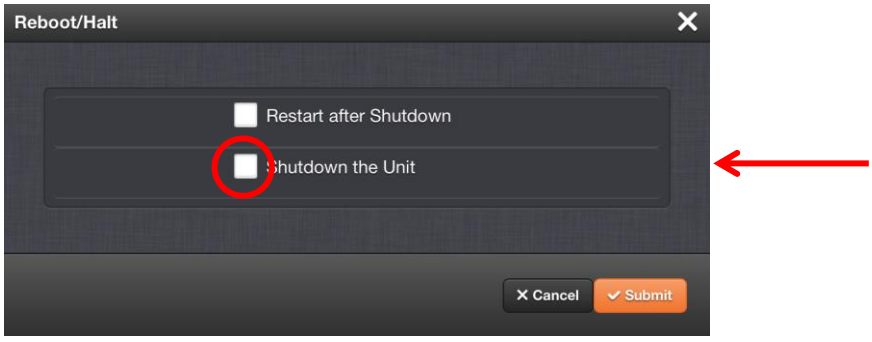
Once the Halt process has been initiated via the web UI or front panel, the front panel LCD will display `Power off NetClock` and the front panel LED time display will stop incrementing.

3.10.1 Issuing the HALT Command Through the Web User Interface

1. From the **TOOLS** drop-down menu choose **SYSTEM/Reboot/Halt**.



2. Select the **Shutdown the Unit** checkbox.



3. Click the **Submit** button.
4. Wait 30 seconds after entering the **HALT** command before removing power.

Once the Halt process has been initiated, the front panel LCD will display `Power off NetClock` and the front panel LED time display will stop incrementing.

3.10.2 Issuing HALT Command through the LCD/Keypad the Serial Port, Telnet, SSH

The Halt command can be initiated via the Keypad and LCD display. Refer to **2.9 Front Panel Keypad/LCD Operation** for information on using the keypad to perform a Halt.

With a serial connection to the front panel serial port, telnet connection or SSH connection, type **`halt`** <Enter> to halt the unit for shutdown.

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

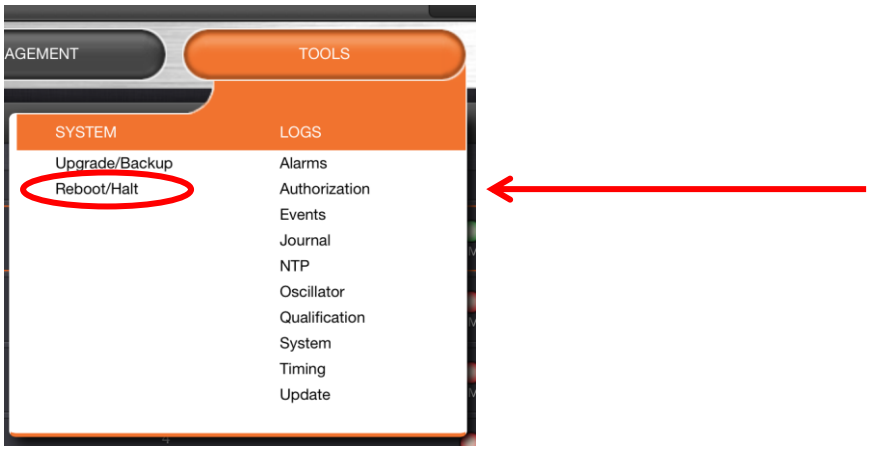
For more information on commands, see Section 12:**NetClock 9400** Series Commands.

Once the Halt process has been initiated, the front panel LCD will display `Power off NetClock` and the front panel LED time display will stop incrementing.

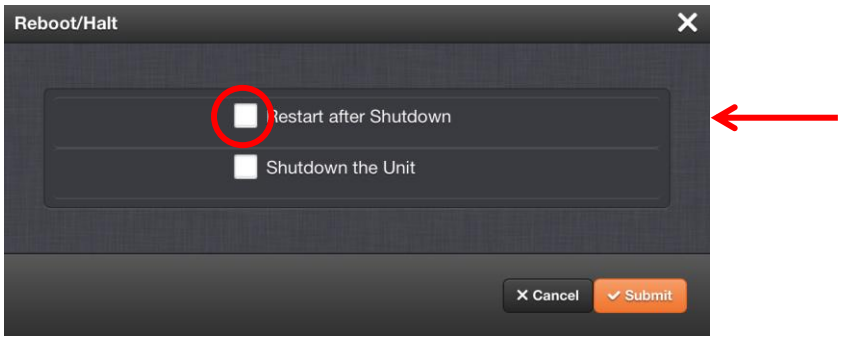
3.11 Rebooting the System

To reboot the unit:

1. From the **TOOLS** drop-down menu choose **SYSTEM/Reboot/Halt**.



2. Select the **Restart after Shutdown** box in the **Reboot/Halt** window.



3. Click the **Submit** button.

The unit will now be rebooted and be accessible again shortly thereafter.

3.11.1 Issuing the REBOOT Command through the LCD/Keypad, Serial Port, Telnet, SSH, SNMP.

The Reboot command can be initiated via the Keypad and LCD display. Refer to **2.9 Front Panel Keypad/LCD Operation** for information on using the keypad to perform a system reboot.

With a serial connection to the front panel serial port, telnet connection or SSH connection, type **`reboot`** <Enter> to reboot the unit.

Reboot is also is available to be performed through an `snmpset` operation.

For more information on commands, see Section 12:**NetClock 9400** Series Commands.

Once the Reboot process has been initiated, the front panel LCD will display a "*Power off NetClock*" message, and the front panel LED time display will stop incrementing until the unit has started booting back up again.

3.12 Changing or Resetting the Administrator Login Password

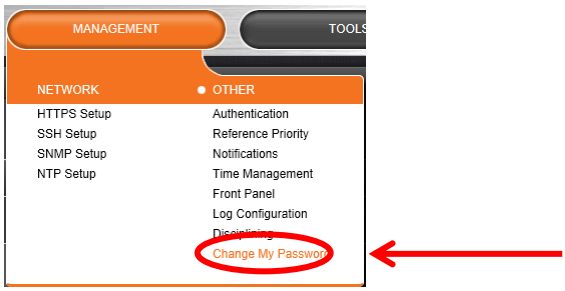
The factory default administrator password value of **`admin123`** can be changed from the default value to any desired value. If the current password is known, it can be changed from the web interface.

NOTE: To follow this procedure, the user must be logged in as the **spadmin** user. If you are unable to login as spadmin, follow the procedure in **3.12.1 Resetting the Administration Account Password When Forgotten/Lost**.

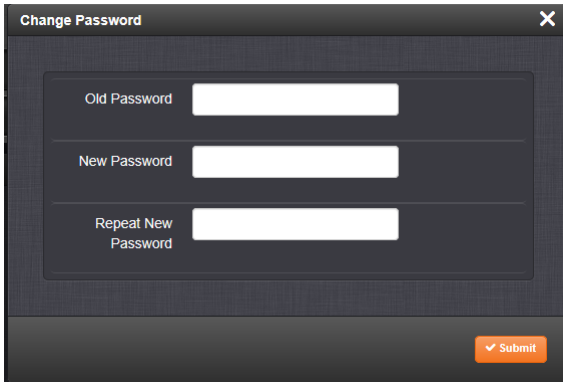
If the password has already been changed from the default value, but the current value is no longer known, the administrator password can be reset back to the factory default value. Once reset, it can then be changed to a new desired value via the web interface.

To change the admin password from a known value to another desired value using a web browser:

1. Navigate to **MANAGEMENT/OTHER/Change My Password**.



2. The **Change Password** pop-up window will display.



3. In the **Old Password** field, type in the current password you wish to replace.
4. In the **New Password** field, type in the new password you wish to use.

NOTE: The new password can be from 8 to 32 characters in length.

5. In the **Repeat New Password** field, retype the new password you wish to use.
6. Click the **Submit** button at the bottom of the screen.

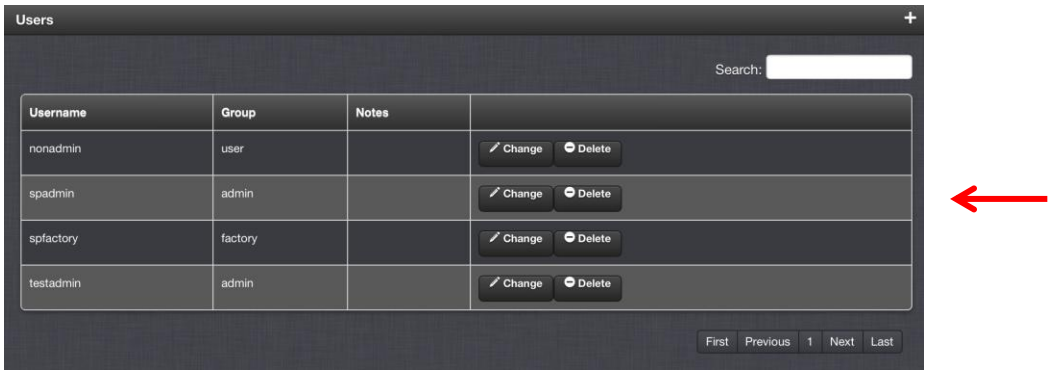
3.12.1 Resetting the Administration Account Password When Forgotten/Lost

If the current **spadmin** account password has been changed from the default value and has been forgotten or lost, you can reset the **spadmin** password back to the factory default value of **admin123**.

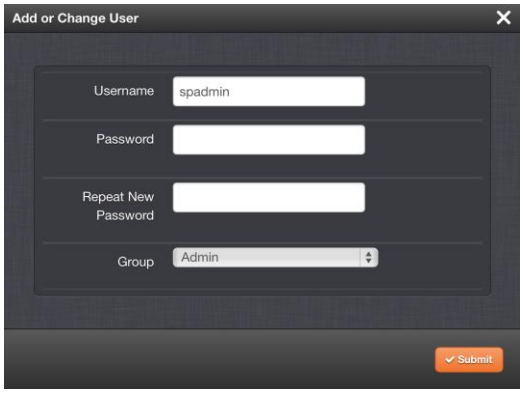
Resetting the **spadmin** account password does not reset any user-created account passwords. This process only resets the **spadmin** account password.

Any user with admin permission can reset the spadmin password through the **MANAGEMENT/OTHER/Authentication** window. To reset the spadmin password through the **MANAGEMENT/OTHER/Authentication** window:

1. Navigate to the **MANAGEMENT/OTHER/Authentication** window.
2. Locate the **spadmin** entry in the **Users** table.



3. Click on the  button.
4. In the **Add or Change User** window:
   a. Enter a new password.
   b. Confirm the new password.



NOTE: The new password can be from 8 to 32 characters in length.

5. Click on the **Submit** button at the bottom of the window.

If you do not have access to the unit through another admin account, the `spadmin` password must be reset via the front panel keypad or using the front panel serial port.

To reset the **`spadmin`** account password using the keypad:

1. Use the front panel LCD and the keypad to perform a "**RESETPW**". Refer to **2.9 Front Panel Keypad/LCD Operation** regarding the use of the front panel keypad. ("Resetpw" is located in the **Home/System** menus).
2. You will be prompted to confirm the operation before the password is reset. The **`spadmin`** account password is now reset to "**`admin123`**".

To reset the spadmin account password using the serial port:

1. Connect a PC to the front panel serial port and log in using an account with admin group rights (such as the **`spadmin`** account).
2. Type: **`resetpw`** <Enter>. The **`spadmin`** account password is now reset.

After resetting the password follow the procedure above to change the spadmin password in the **MANAGEMENT/OTHER/Authentication** window.

3.13 Configuring and Reading the "System Time"

NetClock has an "internal clock", referred to as the "System Time". The System Time is synchronized to its input references (such as GPS, NTP, PTP, etc) or it can be manually configured by a user to a desired time/date. The System Time is then used to generate all of the available time-of-day outputs (such as the front panel LED display, NTP time stamps, time stamps in the log entries, ASCII data outputs, etc).

3.13.1 Configuring the System Time Timescale

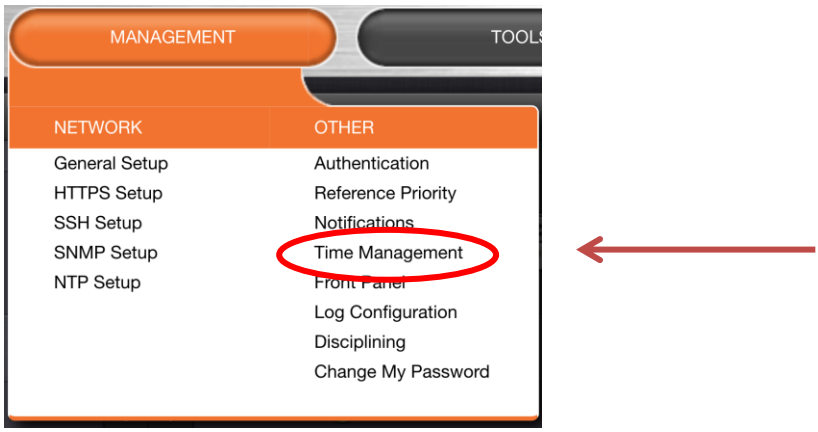
The System Time can be configured to operate in various timescales, such as UTC, GPS and TAI (Temps Atomique International). All of these times are offset from each other by varying amounts, so the times are not all exactly the same.

NOTE: UTC Timescale is also referred to as "ZULU" time. GPS timescale is the raw GPS time as transmitted by the GPS satellites (as of September, 2013, GPS time is currently 16 seconds ahead of UTC time. UTC timescale observes leap seconds while GPS timescale does not).

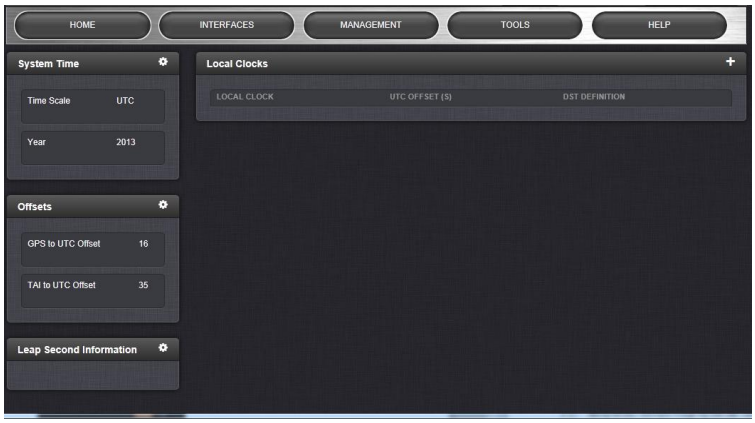
NOTE: The TAI timescale also does not observe leap seconds. The TAI timescale is fixed to always be 19 seconds ahead of GPS time. As of September, 2013, TAI time is 35 seconds ahead of UTC.

To access time management:

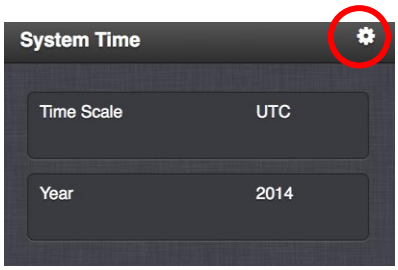
1. Navigate to the **Reference Priority Setup** screen, by choosing **MANAGEMENT/OTHER/Time Management**.



2. The **Time Management** screen will display.



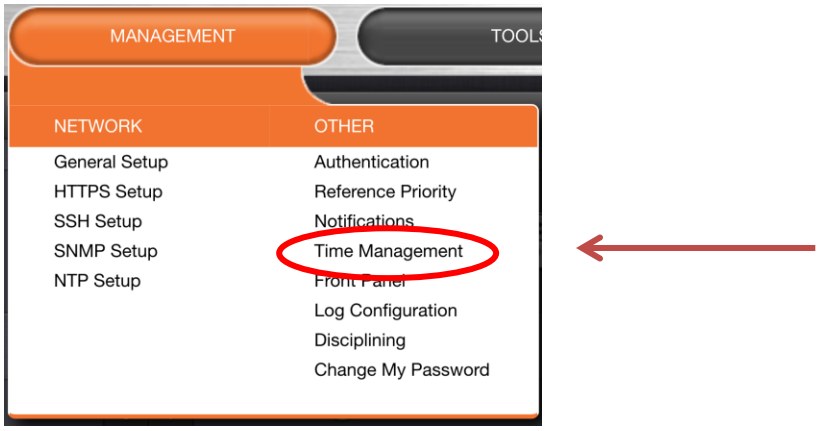
3. Click on the  button in the **System Time** panel in the upper left-hand corner of the **Time Management** screen.



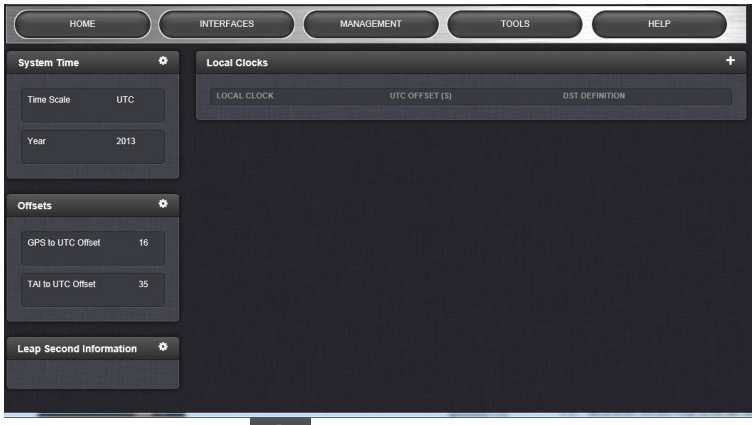
Some of the available NetClock inputs (such as ASCII data inputs, etc) won't necessarily provide time to NetClock in the same timescale selected in the System Time's Timescale field. These inputs have internal conversions that allow the timescale for the inputs to also be independently defined, so that they don't have to be provided in the same timescale. For example, the System timescale can be configured as "UTC", but the IRIG input data stream can provide NetClock with "local" time, with no time jumps occurring when the reference is selected.

If an output reference is using the GPS or TAI timescale, and the System Time is set to "UTC", then the "Set Timescale Offsets" box must be populated with the proper timescale offset value in order for the time on the output reference to be correct. Some references (like GPS) provide the timescale offset to the system. In the event that the input reference being used does not provide this information, it must be set in the Offsets panel of the Reference Priority screen.

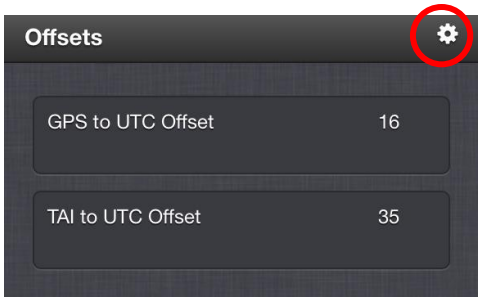
1. Navigate to the **Reference Priority Setup** screen, by choosing **MANAGEMENT/OTHER/Time Management**.



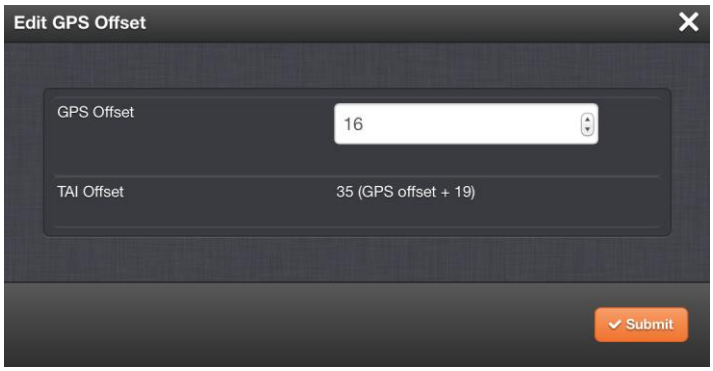
2. The **Time Management** screen will display.



3. Click on the  button in the **Offsets** panel on the left-hand side of the **Time Management** screen.



4. The **Edit GPS Offset** pop-up window will display.



Since the GPS and TAI offsets have a fixed relationship, only the GPS offset can be set on this page. If only the TAI offset is known, subtract 19 from it to get the GPS offset.

NOTE: If the System Time is set to the "UTC" timescale, and all output references either use the "UTC" or "local" timescale, then it is not necessary to set the GPS and TAI Timescale Offsets.

IMPORTANT NOTE: It is imperative to configure any input reference's timescales appropriately. Otherwise, a System Time error may occur!

Some NetClock outputs will be provided in the same timescale that is selected in the System timescale field. The NTP output for network synchronization and the time stamps included in all log entries will be in the same timescale as the configured System Timescale. For example, if "GPS" is selected as the System timescale, the log entries and the time distributed to the network will all be in GPS time (time broadcasted directly from the GPS constellation). But, the LED display can still be configured to show the current "local" time.

In most cases, "UTC" will be the desired Timescale to select.

3.13.2 Reading and Manually Setting the System Time

The current System Time can be either obtained or manually set through **System Time** panel of the **Reference Priority Setup** screen, accessible through the **MANAGEMENT/OTHER/Time Management** drop-down menu. (Note that the current System Time and date are also displayed in the top left-hand corner of the web interface, above the main menus).

The System Time can be manually set by the user. Once the time and/or date has been manually set, the System Time will be synchronized to values that have been manually set, and those values will be used for the generation of the outputs (NTP, Log entries, front panel display, etc.).

NOTE: System time must be set in UTC timescale, not local time.

In order for the time to be able to be manually set by a user and used for synchronization, the Input Reference Priority table on the **Setup/Reference Priority** page needs to have this capability enabled. The Index row of this table that has User set in both the Time and 1PPS columns needs to be configured as "Enabled."

Once the System Time has been manually set, it will continue to use this incrementing time as the System reference, unless a valid, higher priority input reference becomes available (a higher priority input reference will cause the System Time to change to the input reference's time/date) or until the unit is rebooted/power cycled.

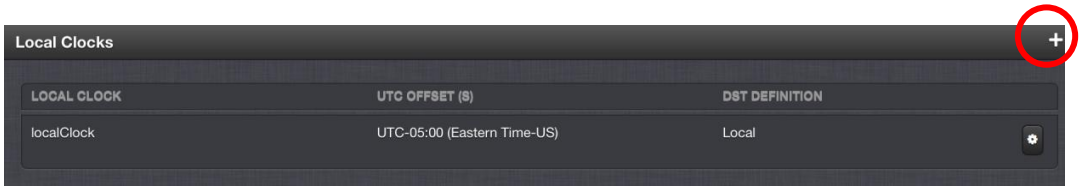
System Time is "maintained" during power-down and should be fairly close to the correct time upon power-up. It is also possible to use this "start-up" time as the synchronized time by enabling synchronization to the battery backed time. The "start-up" time can also be used when a valid 1PPS input is also applied. This is referred to as "Local System" reference.

IMPORTANT NOTE: Disable NTP before setting user time, and re-enable NTP after time is set. If it is desired to use the NTP output with a user set time/date (instead of it being synchronized to an external reference such as GNSS or IRIG input), it is highly recommended that either the time/date be very accurately set to the current time/date, or that all other input references in the Input Reference Priority table be set to "Disabled". If another higher priority input reference becomes available with the reference input being enabled, the user set System Time's time/date values will automatically be corrected to the incoming reference. The time jump that would occur if the System Time was not set at least fairly close to the input reference when the reference syncs the System would prevent NTP from using System Time as a reference, until the NTP Service is either manually disabled and then re-enabled, or until the unit is rebooted/power-cycled.

3.13.3 Local Clock Setup

The selected TimeScale for System Time defines the Timescale of the System. As the System Time is the basis for the time of all outputs, it may be desired to output the time with an offset for "Local time" (Time Zone offset and Daylight Saving Time adjusted). The Local Clock provides the means to apply a time offset for local time to various outputs. Local Clocks are only used in conjunction with the UTC timescale (Local Clocks do not apply to the GPS and TAI Timescales). To set up a local clock:

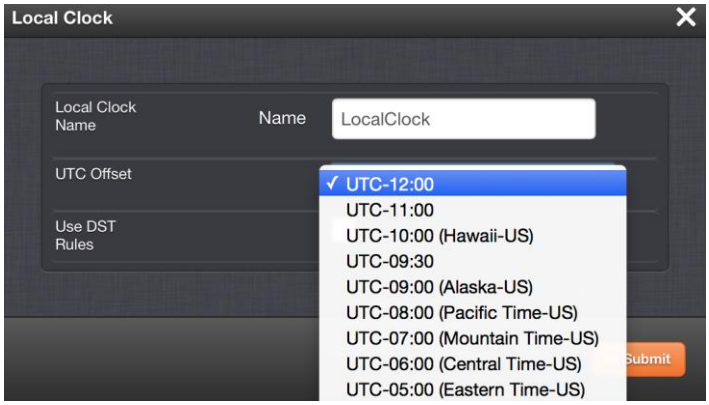
1. If necessary, navigate to **MANAGEMENT/OTHER/Time Management.**
2. Click on the "+" button in the **Local Clocks** panel in the **Time Management** screen.



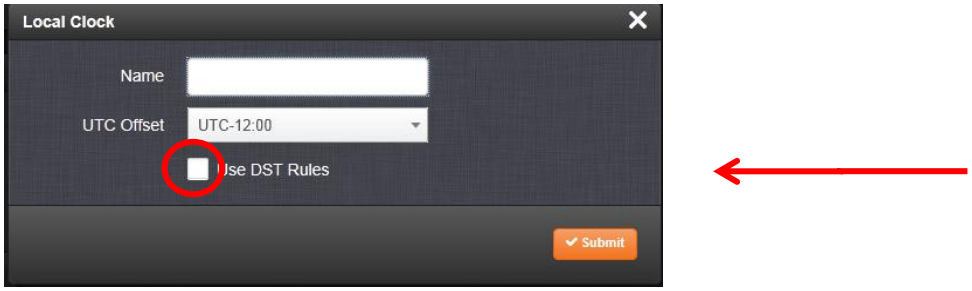
3. The **Local Clock** pop-up window will display

4. Enter a name for your local clock.
   - The name must be between 1 and 64 characters long and spaces are allowed.
   - The name can be any meaningful name that helps you know your point of reference (for example: "New York", "Paris" or "Eastern HQ", etc.).
   - This name will be used as cross-reference drop-down in the applicable Input or Output port configuration. Please note the following limitations apply to this option:
     - Acceptable characters for the name include: **A-Z**, **a-z**, **0-9** and **(-+_)** and spaces are converted to underscores because the name must be a single word.

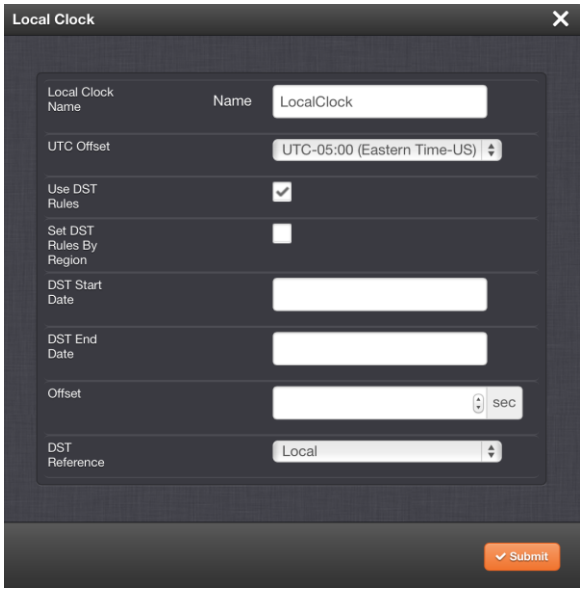
5. In the **UTC Offset** field, choose a UTC offset from the drop-down list.



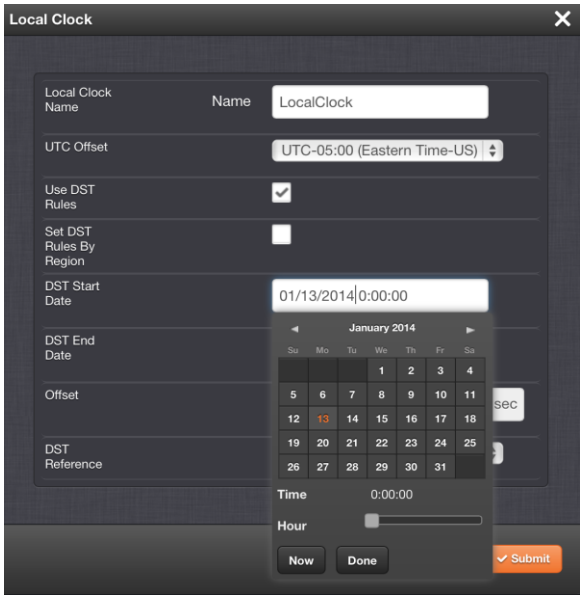
- All of the **UTC Offset** drop-downs are configured as UTC plus or minus a set number of hours.
- Examples for the US: For **Eastern**, choose UTC–05:00, for **Central**, choose UTC-06:00, for **Mountain**, choose UTC-07:00 and for **Pacific**, choose UTC-08:00.
- If you wish to use DST (Daylight Savings Time) rules, click the **Use DST Rules** box. Otherwise the time for the local clock will always be standard time.



- DST options will appear in the **Local Clock** window.

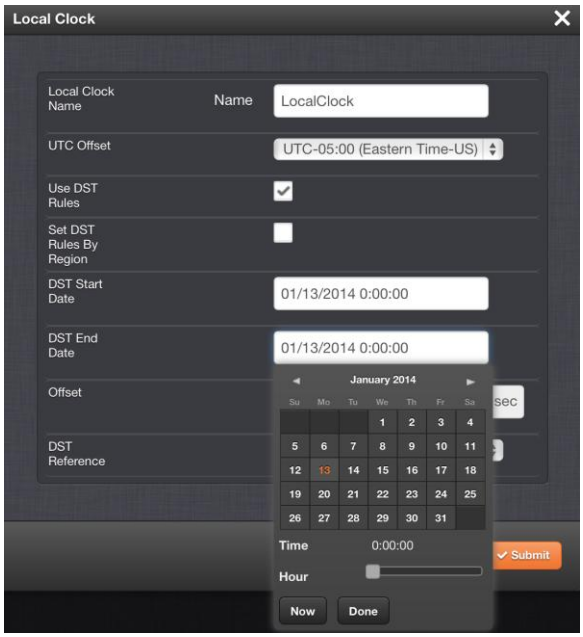


- **DST Start Date**—For if you want to manually set the start day of DST.
  - Click on the DST Stare Date field to reveal a calendar and an hour slider.



  - Choose a date in the calendar and an hour with the slider.
  - The date followed by the time will display in the DST Start Date field. The time will display in the **Time** field between the calendar and the **Hour** slider.
  - Clicking the Now button will make the current time the start of DST.

- **DST End Date**—For if you want to manually set the start day of DST.
  - Click on the DST Stare Date field to reveal a calendar and an hour slider.



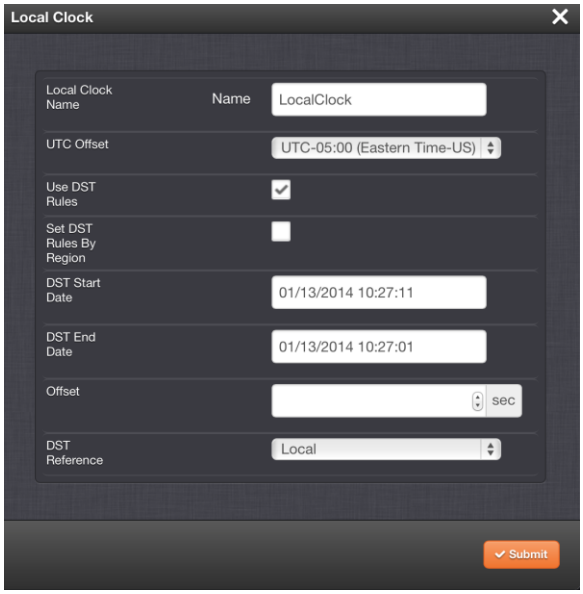
- Choose a date in the calendar and an hour with the slider.
- The date followed by the time will display in the DST Start Date field. The time will display in the **Time** field between the calendar and the **Hour** slider.
- Clicking the **Now** button will make the current time the end of DST.

- **Offset**—In seconds. Use this field to manually define your local clock's DST offset.
- **DST Reference**—When using a Local Clock with an input reference (such as IRIG input, in order to provide proper internal conversion from one Timescale to another, the unit needs to know if the input time is in Local Timescale or UTC Timescale. Select "Reference is Local time" or "Reference is UTC" depending on the Timescale of the Input reference this Local Clock is being used with. Additional Local Clocks may need to be created if multiple input Timescales are being submitted.

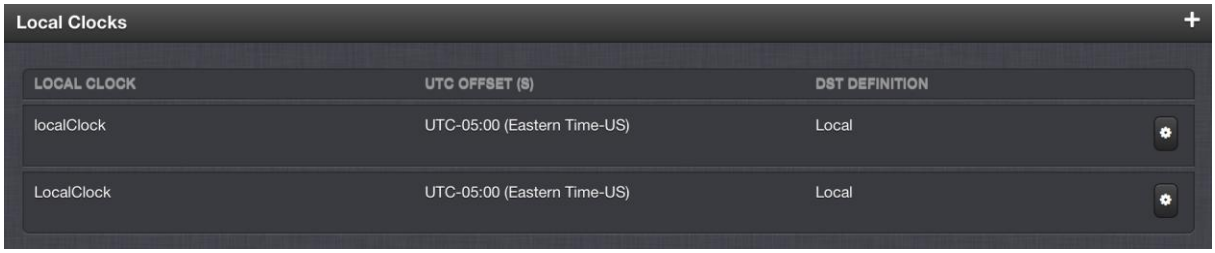
NOTE: The option of a manually defined DST is provided for those customers who may be in a location that does not follow any of the pre-configured DST rules. You can input start time, end time and the hour to change for the daylight saving. By selecting this option, the DST rule can be custom defined based on the weekday, week, and month of the local time you defined for this interface.

- If you select **Set DST Rules by Region** a drop-down list with display with a choice of:
  - EU (Europe)—For 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).
  - US-Canada—For if your location complies with the USA's DST Rule (as it was changed to back in 2006, where the "DST into" date is the Second Sunday of March and the "DST out" date is the first Sunday of November).
  - Australia.

NOTE: If a pre-configured rule DST rule happens to be changed in the future (like the change to the US DST rule in 2006), this option allows the DST rules to be edited without the need to perform a software upgrade for a new DST rule to be defined. Select this drop-down and enter the DST parameters for the new rule.

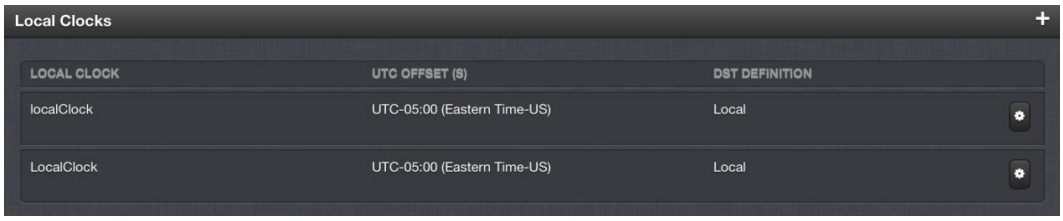


6. Click the **Submit** button at the bottom of the window.
7. Your local clock will appear in the **Local Clocks** panel.

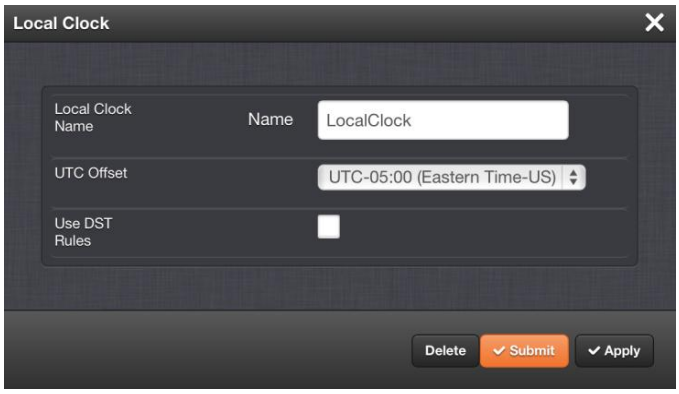


Changing a Local Clock's Offset

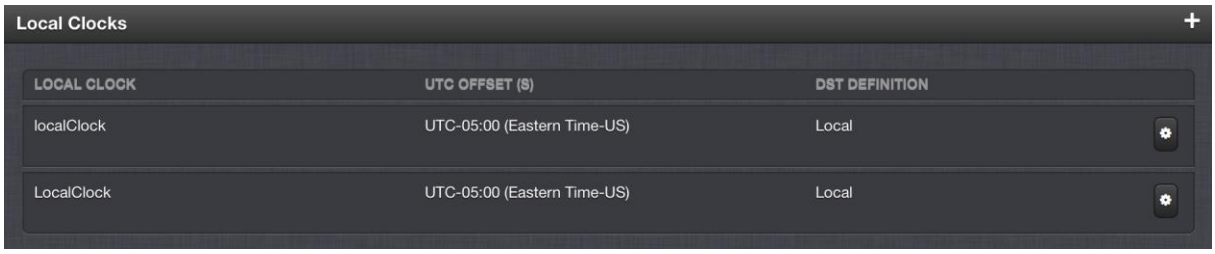
1. If necessary, navigate to **MANAGEMENT/OTHER/Time Management.**
2. Click on the  button in the **Local Clocks** for the local clock you wish to remove.



3. The **Local Clock** pop-up window will display.

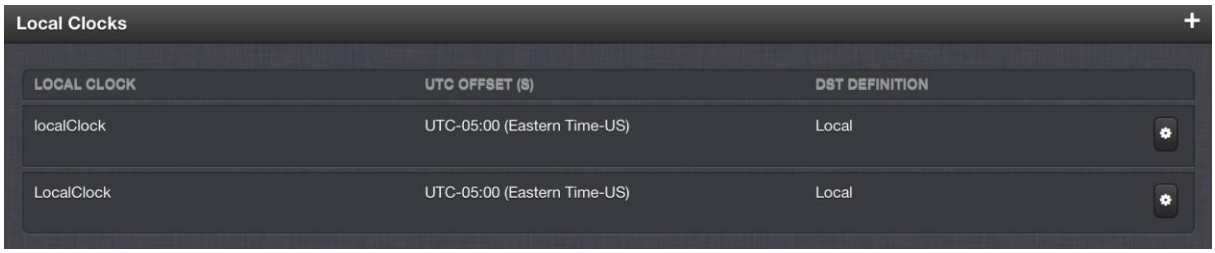


4. Make the necessary change in the **Local Clock** window.
5. Click the **Submit** button at the bottom of the screen.
6. The local clock appears as edited in the **Local Clocks** panel.

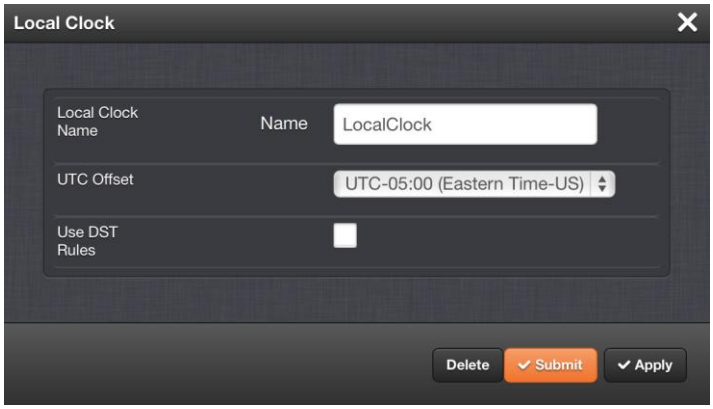


Deleting a Local Clock

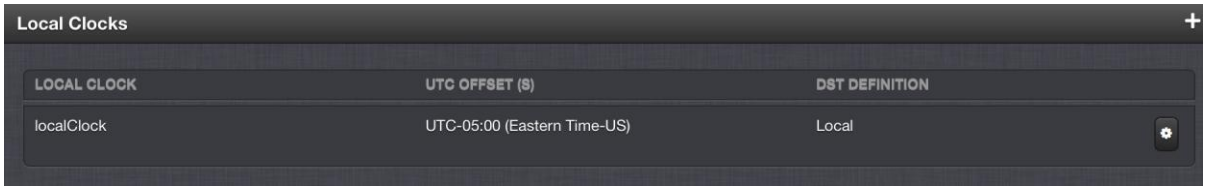
1. If necessary, navigate to **MANAGEMENT/OTHER/Time Management.**
2. Click on the  button in the **Local Clocks** panel for the local clock you wish to delete.



3. The **Local Clock** pop-up window will display.



4. Click on the **Delete** button at the bottom of the window.
5. The Local Clock will no longer appear in the **Local Clocks** panel.



3.13.4 Examples - DST Rule Configurations

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

In the **Local Clock** pop-up window:

1. Assign the clock a meaningful name for this clock in the **Local Clock Name** field.
1. Select “UTC +01:00” from the **UTC Offset** pull down menu.
2. Confirm that the **Use DST Rules** checkbox is not selected.
3. Review the changes made and click the **Submit** button.
4. The unit will display the status of the change.

Example 2: To create a Local System Clock for a unit installed in the Eastern Time Zone of the US, and desiring the Local Clock to automatically adjust for DST (using the post 2006 DST rules for the US).

In the **Local Clock** pop-up window:

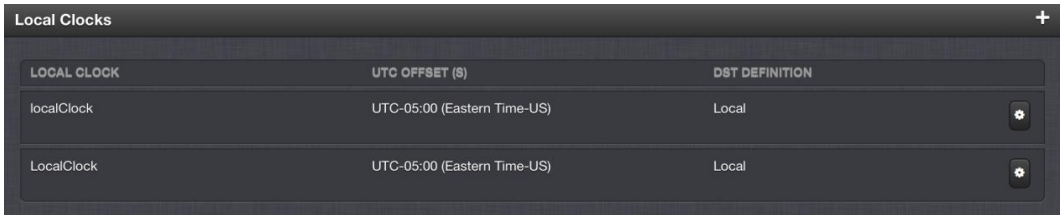
1. Assign the clock a meaningful name for this clock in the **Local Clock Name** field.
2. Select “UTC -05:00” from the **UTC Offset** pull down menu.
3. Select the **Use DST Rules** checkbox.
4. Select the **Set DST Rules by Region** checkbox.
5. From the **DST Region** drop-down select “US-Canada.”
6. Review the changes made and click the **Submit** button.
7. The unit will display the status of the change.

3.13.5 Editing a Previously Created Local Clock

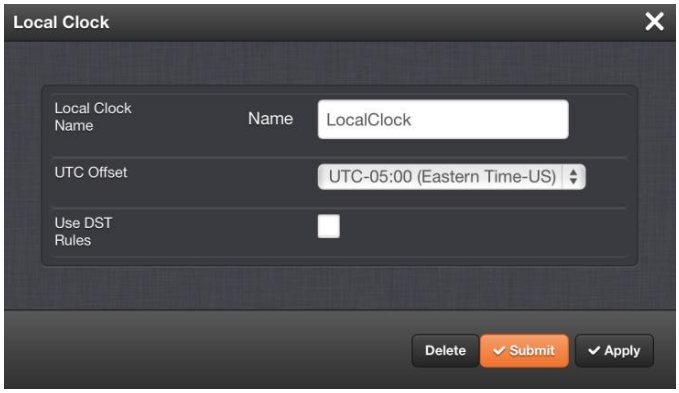
Any previously created Local Clock can be edited as desired. Select the name of the Local Clock from the top of the **Setup / Local Clock** page. Edit the desired value(s) in the Local Clock setup requiring modification and click Submit.

The modifications made will affect the DST correction/computations for all inputs and outputs that are configured to use the name of the just edited Local Clock
To edit a previously created local clock:

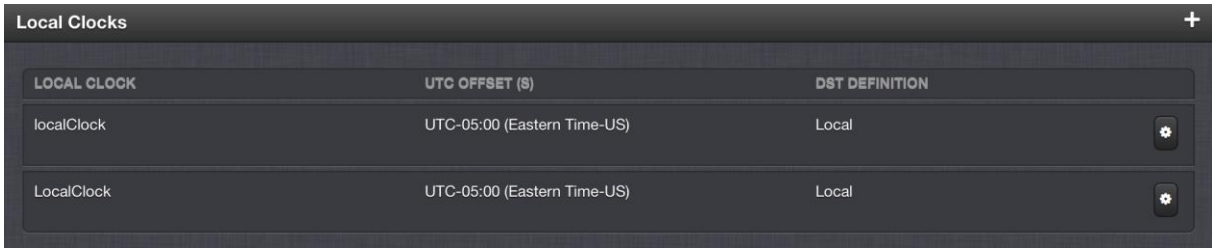
1. If necessary, navigate to **MANAGEMENT/OTHER/Time Management.**
2. Click on the ⚙ button in the **Local Clocks** for the local clock you wish to remove.



3. The **Local Clock** pop-up window will display.



4. Make the necessary change in the **Local Clock** window.
5. Click the **Submit** button at the bottom of the screen.
6. The local clock appears as edited in the **Local Clocks** panel.



3.13.6 Example - Applying Local Clock to Front Panel

The following example scenario includes steps that can be used to apply a local clock to the NetClock front panel to show local time.

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** pop-up window.
2. In the **Show Content Field**, select the display you want from the drop-down list. The options are:

   - **Rotate**—This option enables rotation of the content display in the LCD window when the keypad is not in use. Content will rotate through all enabled content for installed options. When **Rotate** is selected, a further option appears on the screen:
     - **Rotation Delay**—This option sets the duration in seconds for content display during rotation before the next content screen is displayed. Valid duration range is between 1 and 30 seconds.
   - **Network** (the default)—This option displays the current network settings. If an option card is installed that provides additional network interfaces, there will be additional network choices (i.e., Network: eth0, Network: eth1, etc.).
   - **Status**—This option displays current key status indications (such as NTP Stratum level, TFOM –"Time Figure of Merit", Sync status and Oscillator lock status).
   - **Position**—This option displays current latitude, longitude and antenna height.
   - **Day of Year**—This option displays the day of year (such as "Day of Year 104").
   - **GNSS**—This option displays the number of satellites currently being used (and the strongest signal strength out of all these satellites) and their relative signal strengths of all the receiver channels that are tracking satellites as a bar graph.
   - **Date**—This option displays the current date (such as "16 April 2012").

NOTE: The date is based on the configured LCD's timescale. It is possible that a date other than "today's local date" may be shown, if the configured time scale has already rolled over to its new date, though local time has not yet rolled over to its new date.

   - **Keys**—This option is applicable to SAASM GPS receiver option module only. The front panel will display "NOT SUPPORTED" unless a SAASM receiver is installed.
   - **None**—This option configures the LCD window to remain blank unless the keypad is unlocked and in use.

3. In the **Timescale/Local Clock** field, choose the timescale or local clock you wish to use as the time reference for the time shown on the front panel.
   - The options available are:
     - UTC
     - TAI
     - GPS
     - Any local clocks you have set up. The Time Zone and DST rules, as configured in the Local Clock will now be applied to the front panel time display. For more information on Local Clocks see **3.13.3 Local Clock Setup**.

NOTE: With **Timescale** configured as "Local" and during DST (Daylight Saving Time, as configured in the Local Clock), a "DST indicator" (decimal point) will be displayed to the bottom-right of the minutes portion of the LED time display. The "DST indicator" extinguishes during "Standard" time. If the Local Clock is configured as "No DST/Always Standard Time", the DST indicator won't ever be lit.

4. Select the **Lock Keypad** check box if you want to lock the front panel keypad. The default is unlocked (unchecked).
5. Deselect the **Allow Position Display** checkbox if you do not want enable the unit's position display screen. If this box is currently selected, the front panel display screen is set to "none." The default is for the position display screen to be enabled (the box is checked).

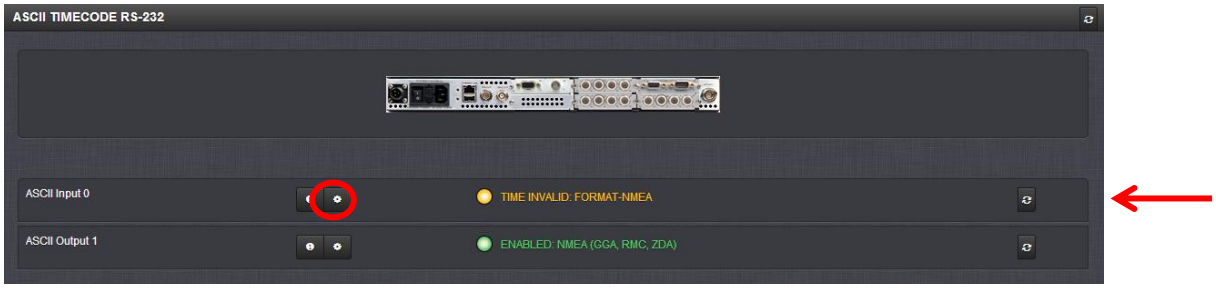
3.13.7 Example Configuration for Spectracom TimeView Displays Clocks

Applying the ASCII RS-485 Outputs to synchronize Spectracom TimeView or other wall display clocks is a common scenario. If there are any Spectracom TimeView digital display clocks to be connected to the Remote RS-485 output of the NetClock, configure the Remote RS-485 output port as follows:

- Spectracom Format 0
- 9600 baud
- Desired local clock for local time output
- Broadcast

To configure the ASCII data output ports:

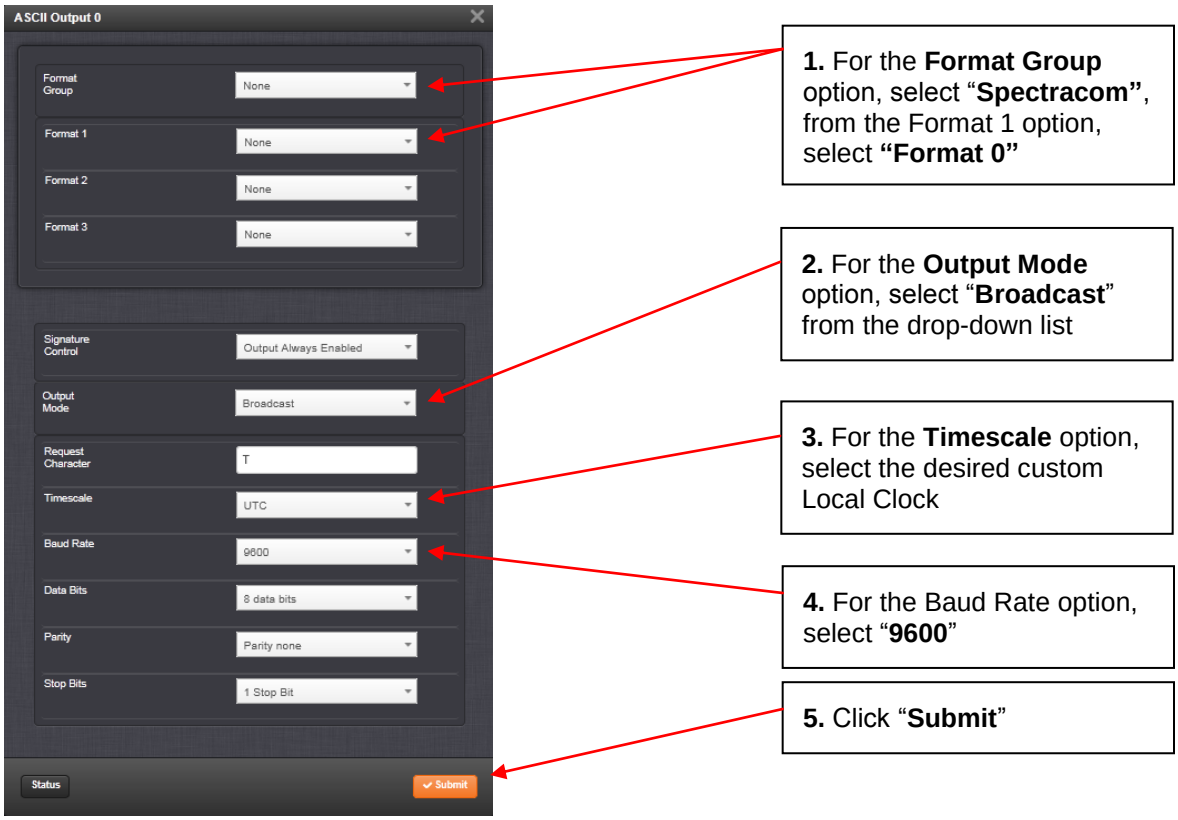
1. Navigate to the **ASCII TIMECODE RS-232** entry for the card you wish to configure through the **INTERFACES/OPTION CARDS** drop-down menu.
2. The **ASCII TIMECODE RS-232** window will appear.



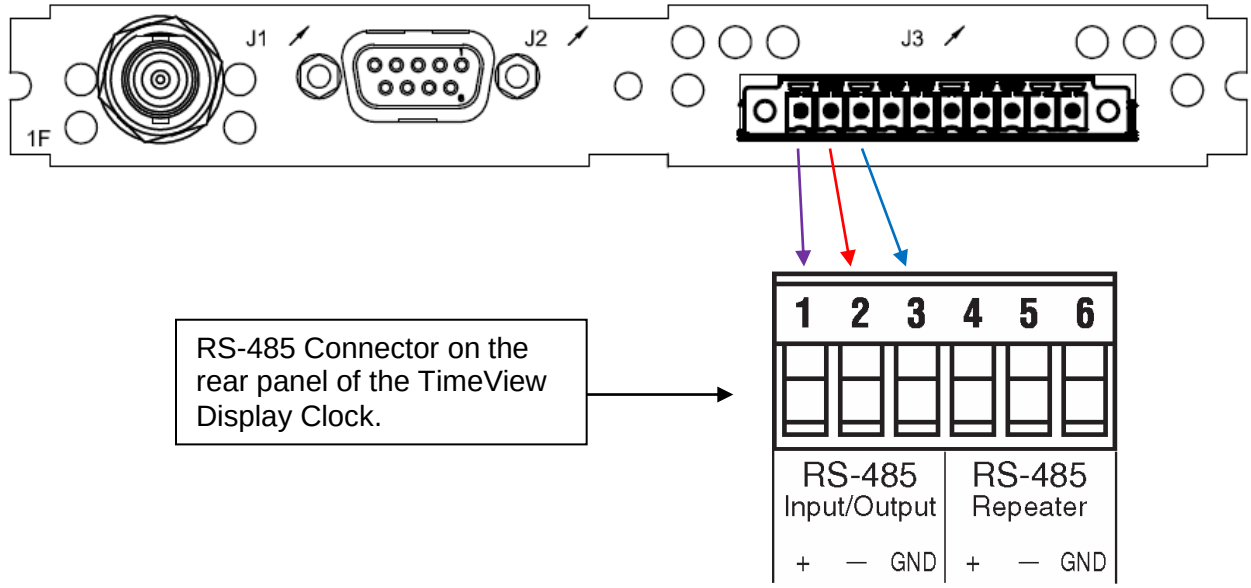
3. Click on the  button in the **ASCII Input** row.

NOTE: If you have only one input or output of any type, the unit will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

4. The **ASCII Output 0** edit window will display.



Interface Wiring between NetClock and TimeView Display Clocks



3.13.8 Reference Information about Daylight Saving Time Change

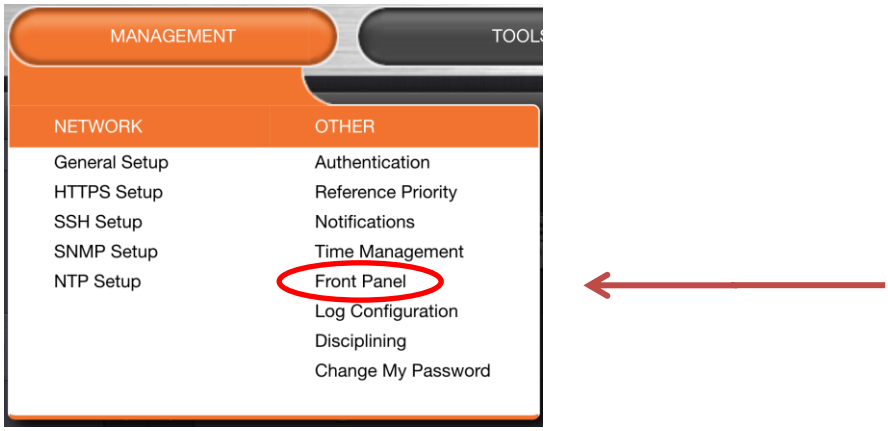
The general Time Zone and DST rule information can be found from the following web sites: http://www.worldtimeserver.com/, http://webexhibits.org/daylightsaving/b.html.

3.13.9 Front Panel LED/LCD Display and Keypad Configuration (9483 only)

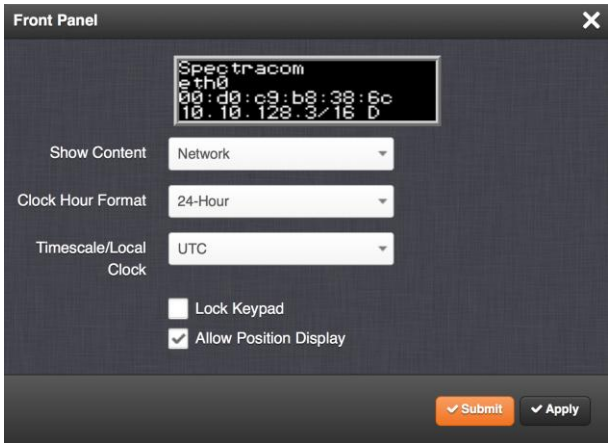
Accessing the Front Panel Setup Screen

The user can view a representation the NetClock's front panel display and configure the information that the front panel will display. To view and configure the information displayed on the NetClock's front panel:

1. Navigate to the **Front Panel** setup screen, by choosing **MANAGEMENT/OTHER/Front Panel**.



2. The **Front Panel** setup pop-up window will display.



- The pop-up window contains:
  - A representation of the current information that appears on the front panel.
  - **Show Content**—A drop-down of the options that can be shown on the front screen. This field determines what is normally displayed in the LCD window when the keypad is not in use. The desired screen to display can be selected with either the keypad or with this drop-down field. While switching from one screen to another either "Keypad Locked" or "Keypad Unlocked" will be displayed on the LCD (depending on the setting of the keypad "Lock" field).
  - **Clock Hour Format—**This option configures the time display on the front panel as either in 12-hour or 24-hour format.

- **Timescale/Local Clock—**This option configures the time scale for the LED time display. The available options are UTC, TAI (Temps Atomique International), GPS and Local. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GNSS satellites (as of September, 2013, GPS time is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **MANAGEMENT/OTHER/Time Management** page. Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.
- **Lock Keypad**—Checking this box will lock the keypad. If desired, the front panel keypad can be locked to prevent inadvertent operation. Locking and unlocking of the keypad can be performed either with the keypad or with this drop-down field. When Lock is configured not checked (the default), the front panel keypad operation is available.
- **Allow Position Display—**This must be checked (the default) for the front panel position to display content. If this box is not selected, the front panel display screen is set to "none."

Front Panel Control and Output

The Front Panel LED time display, the LCD display and the keypad operation can be configured from the **Setup/Front Panel** page from the web interface.

The front panel contains an LED time display which can be configured to show the current time (UTC, TAI, GPS or Local time scale) in either 12 or 24 hour format. By factory default, the LED will display UTC time in 24 hour format (such as displaying "18" at 6PM).

The front panel also features an LCD display. Besides being used in conjunction with the keypad, the LCD window can be configured to display different screens when the keypad is not in use. To prevent inadvertent keypad operation, it can be locked and unlocked from the web interface.

Configuring the Content Outputs of the Front Panel LCD Time Display

To configure the Front Panel LED Display:

6. Navigate to the **MANAGEMENT/OTHER/Front Panel** pop-up window.
7. In the **Show Content Field**, select the display you want from the drop-down list. The options are:

- **Rotate**—This option enables rotation of the content display in the LCD window when the keypad is not in use. Content will rotate through all enabled content for installed options. When **Rotate** is selected, a further option appears on the screen:
  - **Rotation Delay**—This option sets the duration in seconds for content display during rotation before the next content screen is displayed. Valid duration range is between 1 and 30 seconds.
- **Network** (the default)—This option displays the current network settings. If an option card is installed that provides additional network interfaces, there will be additional network choices (i.e., Network: eth0, Network: eth1, etc.).
- **Status**—This option displays current key status indications (such as NTP Stratum level, TFOM –"Time Figure of Merit", Sync status and Oscillator lock status).
- **Position**—This option displays current latitude, longitude and antenna height.

- **Day of Year**—This option displays the day of year (such as “Day of Year 104”).
- **GNSS**—This option displays the number of satellites currently being used (and the strongest signal strength out of all these satellites) and their relative signal strengths of all the receiver channels that are tracking satellites as a bar graph.
- **Date**—This option displays the current date (such as “16 April 2012”).

NOTE: The date is based on the configured LCD’s timescale. It is possible that a date other than “today’s local date” may be shown, if the configured time scale has already rolled over to its new date, though local time has not yet rolled over to its new date.

- **None**—This option configures the LCD window to remain blank unless the keypad is unlocked and in use.

8. In the **Timescale/Local Clock** field, choose the timescale or local clock you wish to use as the time reference for the time shown on the front panel.
    - The options available are:
        - UTC
        - TAI
        - GPS
        - Any local clocks you have set up. The Time Zone and DST rules, as configured in the Local Clock will now be applied to the front panel time display.

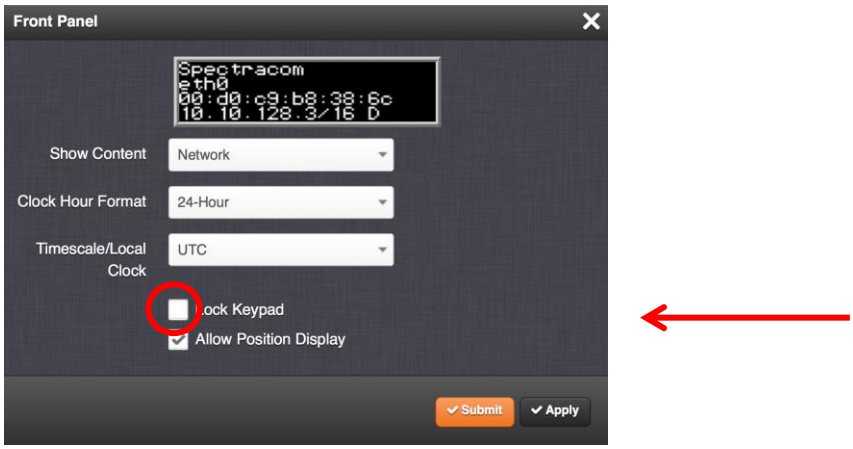
NOTE: With **Timescale** configured as “Local” and during DST (Daylight Saving Time, as configured in the Local Clock), a “DST indicator” (decimal point) will be displayed to the bottom-right of the minutes portion of the LED time display. The “DST indicator” extinguishes during “Standard” time. If the Local Clock is configured as “No DST/Always Standard Time”, the DST indicator won’t ever be lit.

9. Select the **Lock Keypad** check box if you want to lock the front panel keypad. The default is unlocked (unchecked).
10. Deselect the **Allow Position Display** checkbox if you do not want enable the position display screen. If this box is currently selected, the front panel display screen is set to “none.” The default is for the position display screen to be enabled (the box is checked).

Locking/Unlocking the Keypad of the Front Panel

To lock the keypad of the front panel:

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** pop-up window.
2. Select the **Lock Keypad** checkbox so that a check in the box appears.



3. Click the **Submit** button or the **Apply** button at the bottom of the window.

To unlock the keypad on the front panel:

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** pop-up window.
2. Click on the **Lock Keypad** checkbox, so that the check in the box disappears.
3. Click the **Submit** button or **Apply** button at the bottom of the window.

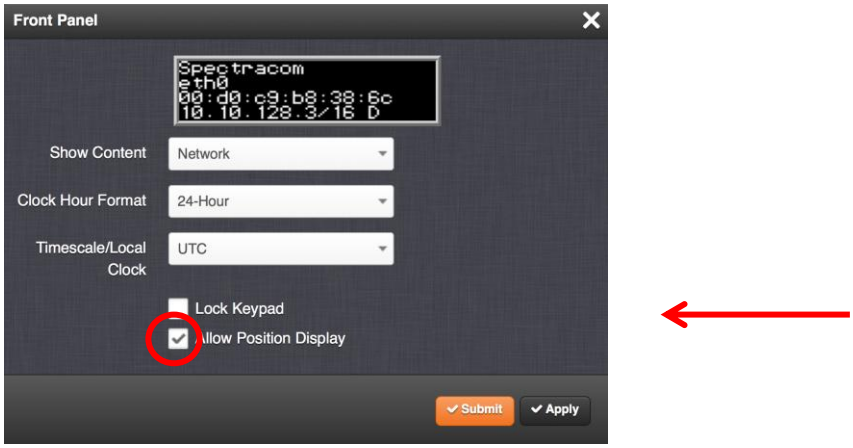
NOTE: If the keypad is unlocked, pressing any keypad key will temporarily return the LCD display to the “Home” menu display for keypad operation. A minute after the last keypad press, the configured LCD screen will be displayed again.

Enabling/Disabling the Position Display Screen

To enable the position display screen:

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** pop-up window.

2. Select the **Allow Position Display** checkbox so that a check appears in the box.



3. Click the **Submit** button or the **Apply** button at the bottom of the window.

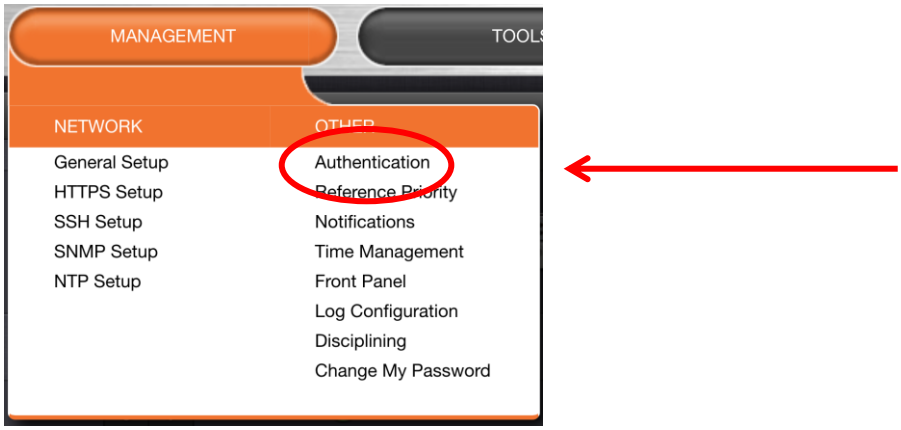
To disable the position display screen on the front panel:

1. Navigate to the **MANAGEMENT/OTHER/Front Panel** pop-up window.
2. Select the **Allow Position Display** checkbox.
3. Click the **Submit** button or **Apply** button at the bottom of the window.

The default is for the position display screen to be enabled (the box is checked).

3.14 User Accounts

User accounts can be created and managed from the **Users** page. The **Users** page is accessed through the **MANAGEMENT/OTHER/Authentication** menu.



The **Users** window presents a table of all user accounts showing the **Username** of each user, the **Group** to which that user account is assigned, and any **Notes** about the user account.

The NetClock comes with two default user accounts set up: the default administrator account (`spadmin`) and the factory service (`spfactory`) account. Additional user accounts may be added and deleted as desired.

NOTE: The password for the **`spadmin`** account can be changed (and it is recommended to do so for security reasons). However, the **`spadmin`** account name cannot be changed, and the account cannot be removed from the unit.

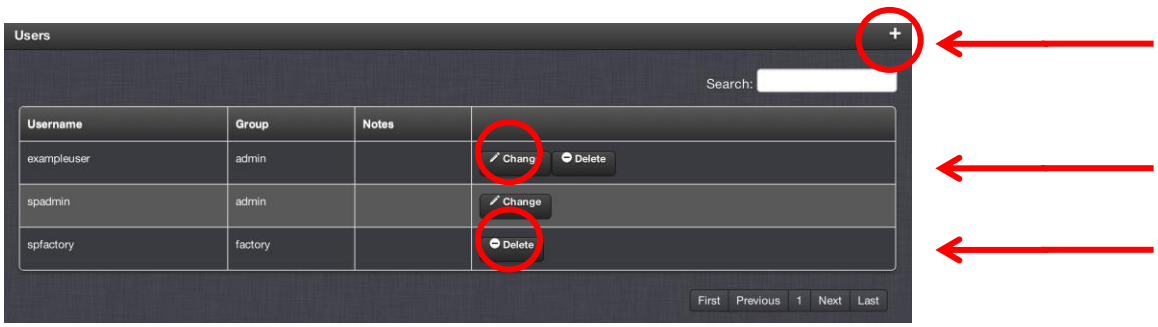
NOTE: The `spfactory` account is for use by Spectracom service personnel. While the `spfactory` account can be deleted by an administrator, it should be noted that this may potentially limit remotely provided technical support.

User accounts can be created to have either limited user or full administrator rights. Each user can be assigned its own login password.

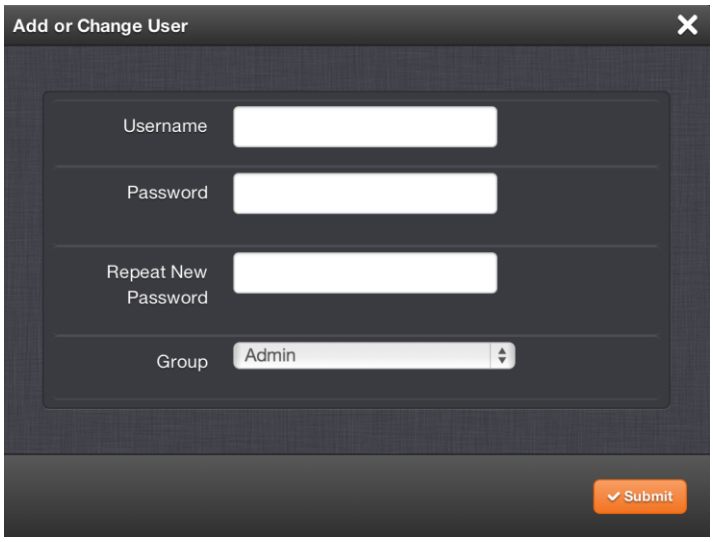
To create a user account, click on the "+" button in the top-right corner of the **Users** screen.

To delete a user account, click the Delete button in that account's entry on the **Users** screen.

To make changes to a user account, click the Change button in that account's entry on the **Users** screen.



When either the Change or the "+" button is clicked the **Add or Change** User window appears.



Adding a User Account

To add a user account:

1. Access the Authentication page through **MANAGEMENT/OTHER/Authentication** drop-down menu.
2. Click on the "+" button in the top-right corner of the **Users** screen.
3. Enter a **Username**. The user name can be any combination of lower-case characters only (upper-case characters, punctuation symbols and numbers are not allowed). The minimum username length is 3 characters, and the maximum is 32 characters.
4. Enter a **Password**. The password can be any combination of upper- and lower-case characters. The minimum password length is 8 characters, and the maximum length is 32 characters.
5. Repeat the new **Password**, to confirm that the password you typed is the password you want.
6. Choose the permission group to which you want the user to belong in the **Group** field.

   There are two available permission groups for each user account: "user" and "admin". The "user" permission level assigns permission to access and change all settings, with the exception of the following capabilities, which are limited to the "admin" permission level only.

   - Changing network settings
   - Adding and deleting user accounts
   - Upgrading NetClock system software
   - Resetting the NetClock configuration
   - Clearing log files
   - Changing Disciplining Setup options
   - Changing configuration options for the following protocols or features:
     - NTP
     - HTTPS, SSH
     - LDAP/RADIUS
     - SNMP (with the exception of configuring SNMP notifications)

Altering an existing user account

To manage a user account that has already been created:

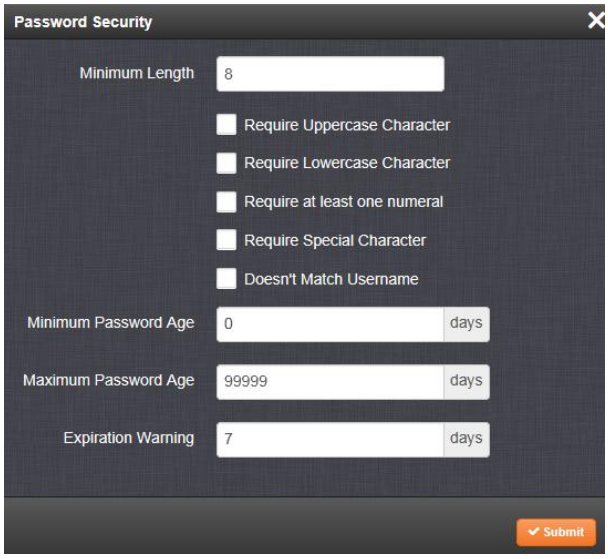
1. Access the Authentication page through **MANAGEMENT/OTHER/Authentication** drop-down menu.
2. Click on the Change button for the user account you wish to alter.
3. In the Add or Change User window the Username field will be populated.
    a. To change the user account name, type the new name you want.
    b. To change the user account's password, type the new password in the **Password** field and confirm it in the **Repeat New Password** field.
    c. To change the user account's user permission group, select the group from the drop-down menu.

3.14.1 Managing Password Security

To manage password security:

1. Access the Authentication page through **MANAGEMENT/OTHER/Authentication** drop-down menu.
2. In the **Actions** panel, click on the **Security Policy** button.

3. The **Password Security** pop-up window will display.



4. Fill in the fields as desired.
5. Click on the **Submit** button at the bottom of the window.

3.15 Oscillator Disciplining

NetClock can be purchased with various types of internal oscillators. Available oscillator types include: Standard OCXO (Ovenized Crystal Oscillator), TCXO (temperature-compensated Oscillator), or an Rb (Rubidium) oscillator. All of these internal oscillators are self-calibrating and can be disciplined to a 1PPS input reference for maximum accuracy.

The purpose of the internal oscillator is to provide NetClock with an accurate 10 MHz output (9483 only) that is extremely stable, even when input references aren't available. The oscillator also provides a very accurate internal time base in case reference inputs are either lost or declared not valid. The oscillator is also used to generate the 1PPS output.

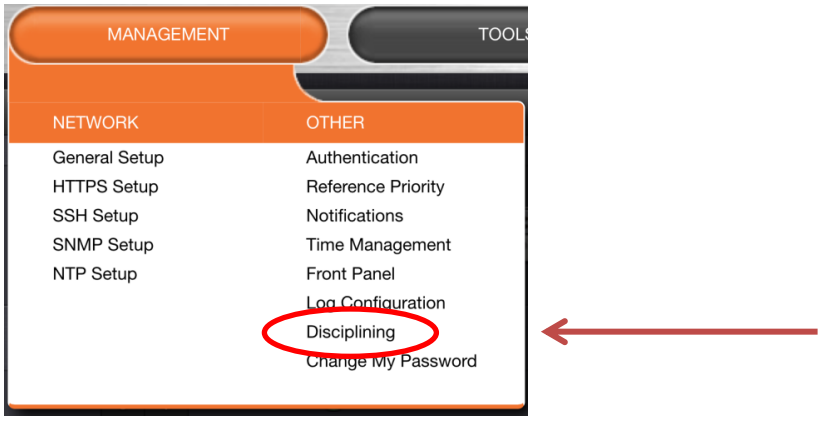
Because of its high degree of stability, the Rubidium oscillator provides the greatest ability to extend the hold-over period when input references are not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

NOTE: The NetClock must be ordered with the desired oscillator installed at the time of the initial purchase. The oscillators cannot be swapped after the NetClock has been shipped from the factory.

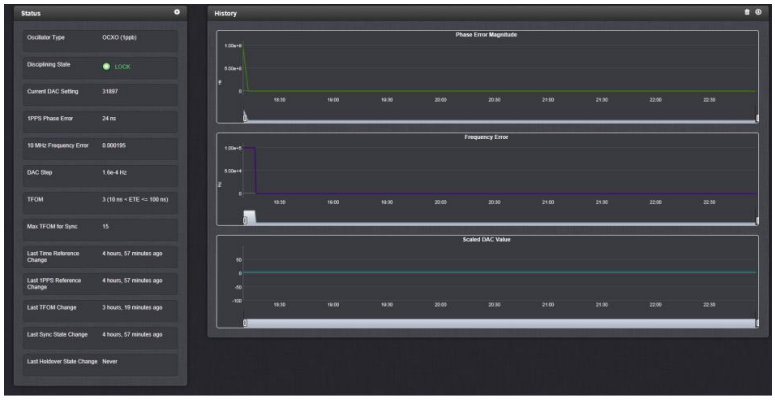
The NetClock's internal oscillator is normally disciplined to an input reference in order to provide the highest degree of oscillator accuracy and to account for oscillator drift. While disciplining (with a 1PPS input reference input present and valid), the oscillator's output frequency is monitored and based on the measured frequency, the oscillator is steered to maintain a very accurate 10 MHZ output. If no valid 1PPS input references are present (or input references are present but not considered valid), the oscillator will be in Freerun mode instead.

Accessing the Oscillator Disciplining page

1. Navigate to the **Oscillator Management** screen, by choosing **MANAGEMENT/OTHER/Disciplining**.

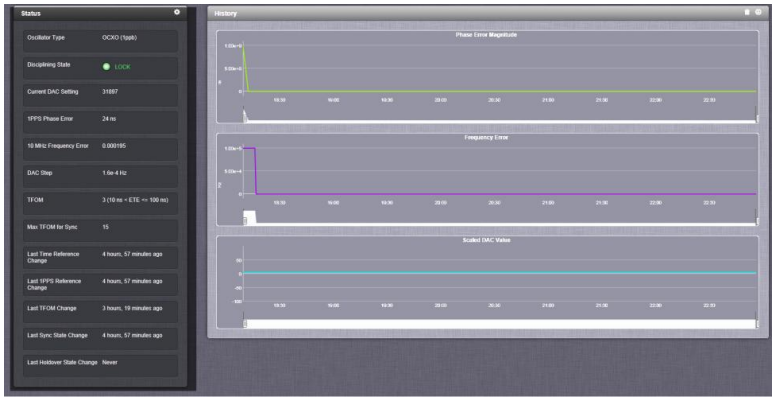


2. The **Oscillator Management** page will display.



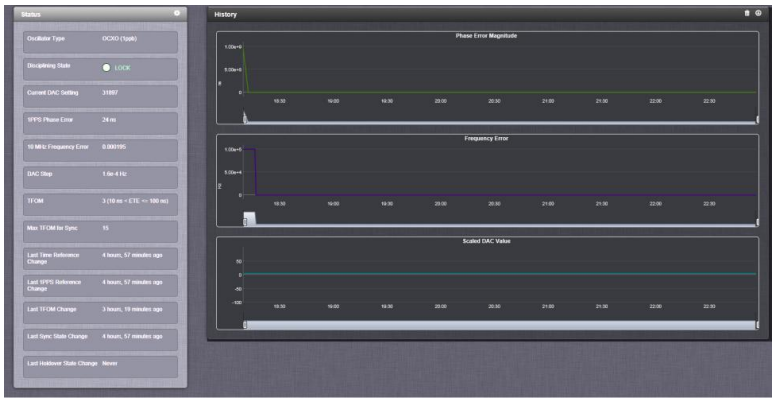
The **Oscillator Management** page consists of 2 panels:

The **Status** panel.



The **Status** panel displays the current state of the unit's timing state.

The **History** panel.



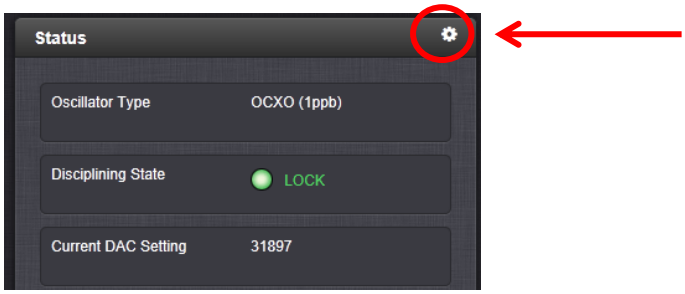
The **History** panel provides a graphical representation of the unit's timing state.

The **Oscillators Settings** page provides the user with some control of the disciplining process. This page is also used to configure the length of time the NetClock is allowed to remain in the Holdover mode.

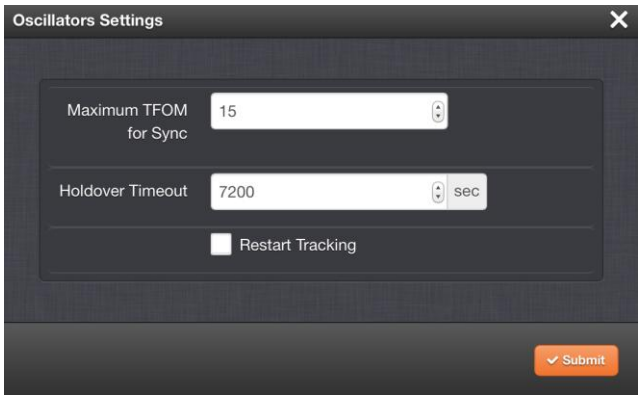
Disciplining Setup (Maximum TFOM for Sync and Holdover Timeout)

1. Navigate to the **Oscillator Management** screen, by choosing **MANAGEMENT/OTHER/Disciplining**.

2. Click the  button at the top of the **Status** panel.



3. The **Oscillators Settings** pop-up screen displays.



4. Fill in the fields:

- **Maximum TFOM for Sync—**When TFOM (Time Figure of Merit, see below) is greater than Max TFOM, disciplining will still be attempted against the selected reference to improve the TFOM. If the condition persists, the system will transition to holdover, and eventually out of sync. When disciplining is performed such that TFOM is no longer greater than max TFOM, the system will transition back into sync.

  TFOM is the unit's estimation of how accurately it is synchronized with its time and 1PPS reference inputs, based on several factors, known as the Estimated Time Error or ETE. The larger the TFOM value, the less accurate the internal clock is aligned with its 1PPS input that is used to perform disciplining. If this estimated error is too large, it could adversely affect the performance of oscillator disciplining. The available TFOM range is 1 through 15. You may refer to the following for the TFOM to ETE conversions:

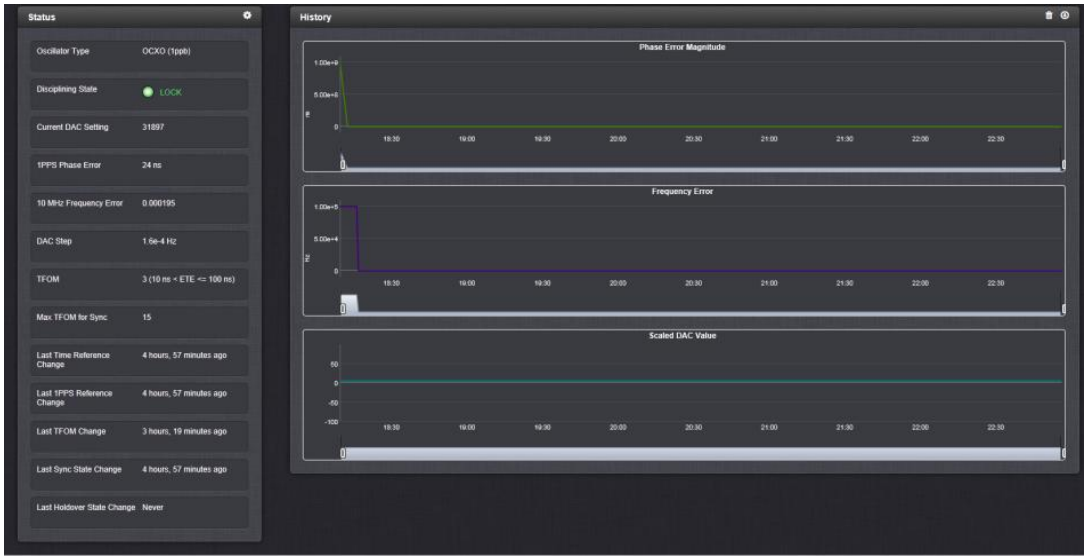
Reported TFOM Value	Estimated Time Error (ETE)
1	<= 1 nsec
2	1 nsec < ETE <= 10 nsec
3	10 nsec < ETE <= 100 nsec
4	100 nsec < ETE <= 1 usec
5	1 usec < ETE <= 10 usec
6	10 usec < ETE <= 100 usec
7	100 usec < ETE <= 1 msec
8	1 msec < ETE <= 10 msec
9	10 msec < ETE <= 100 msec
10	100 msec < ETE <= 1 sec
11	1 sec < ETE <= 10 sec
12	10 sec < ETE <= 100 sec
13	100 sec < ETE <= 1000 sec
14	1000 sec < ETE <= 10000 sec
15	ETE > 10000 sec

- **Holdover Timeout(s)—**The default is 7200 (2 hours).
- **Restart Tracking—**Click the checkbox to implement **Restart Tracking**. This option causes the disciplining algorithm to stop tracking the input reference and start over (as if it was just acquired). This can be useful if there is a large phase offset between reference 1PPS and system 1PPS, in which case it will re-align the system 1PPS with the reference 1PPS very quickly but may cause the 1PPS output to jump.

5. Click the **Submit** button.

Monitoring Oscillator Internal Timing Using Real-Time Graphs

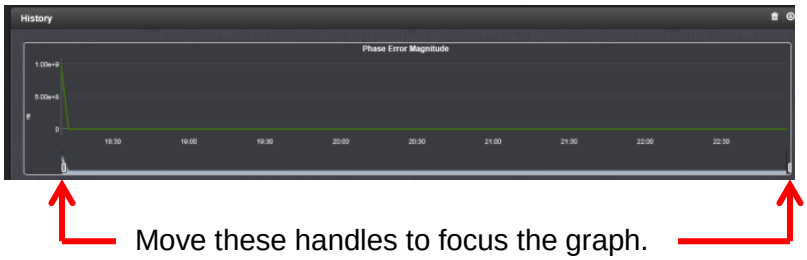
The **Oscillator Management** page provides real-time graphical monitoring of unit's internal timing in the **History** panel.



The page provides 3 graphs, for:

- Phase Error Magnitude
- Frequency Error
- Scaled DAC Value

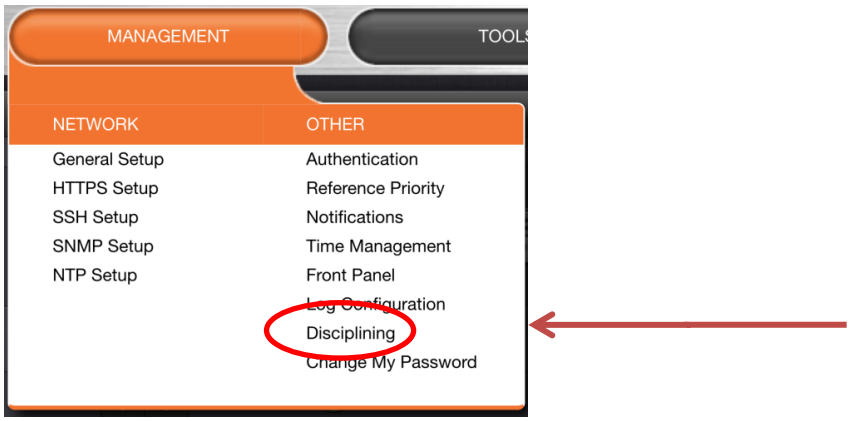
You can get a more detailed view of any of the graphs by grabbing the handles at either end and pulling them in. The graph will focus in on the time interval you choose in real time.



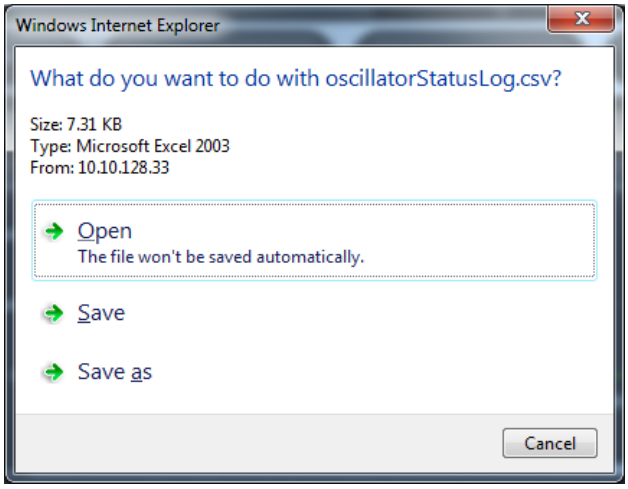
Exporting and saving the Oscillator Logs

To export the oscillator logs:

1. Navigate to the **Oscillator Management** screen, by choosing **MANAGEMENT/OTHER/Disciplining**.



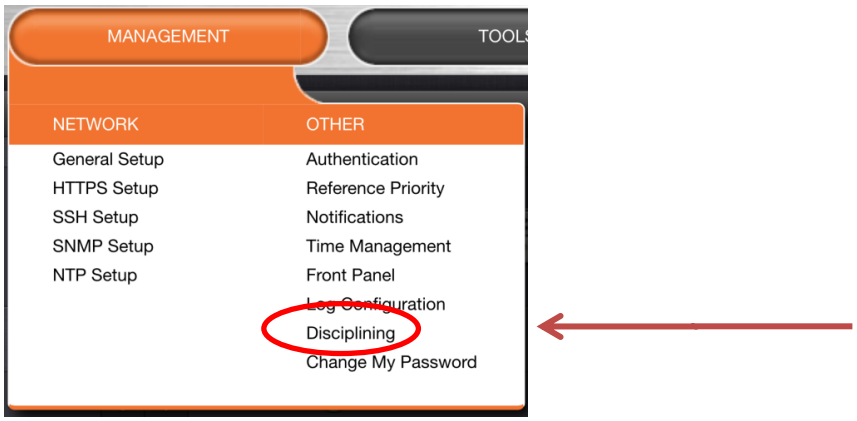
2. Click the  button at the top-right corner of the **History** panel.
3. In the message window that displays, choose what you would like to do with the log file `oscillatorStatusLog.csv` you export.



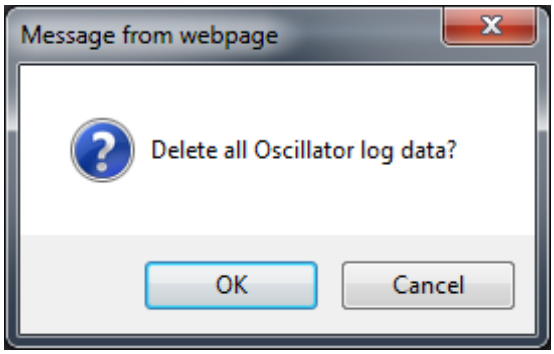
Deleting the Oscillator Logs

To delete the oscillator logs:

1. Navigate to the **Oscillator Management** screen, by choosing **MANAGEMENT/OTHER/Disciplining**.



2. Click the  button at the top-right corner of the **History** panel.
3. Click **OK** in the message window that displays.



3.15.1 Holdover Mode

Holdover

When input references have been supplying input to the unit and input from all the references has been lost, the unit will not immediately declare loss of time synchronization, but first will go into Holdover mode. While the unit is in Holdover mode, the time outputs are derived from an internal oscillator incrementing the System Time.

Because of the stability of the internal oscillator, accurate time can still be derived even after all the primary references are no longer valid or present. The more stable the oscillator is without an external reference, the longer this holdover period can be and have it still maintain very accurate outputs. The benefit of Holdover is that time

synchronization and the availability of the time outputs is not immediately lost when input references are no longer available.

The NetClock will remain in Holdover mode until either:

a) any enabled and valid input reference becomes available again. If one or more references return and are declared valid before the Holdover period has expired (even momentarily), the NetClock exits the Holdover mode and returns to its fully synchronized state.
b) the Holdover Timeout period expires. When the Holdover Timeout period expires, the NetClock declares loss of synchronization.

Holdover Mode does not persist through reboots or power cycles. If a reboot or power cycle was to occur while the unit is in Holdover mode, it will power-up and remain in a "not synchronized" state until at least one valid Time and 1PPS input reference becomes available again. While in this state, NTP will be Stratum 15 and outputs will not be usable. If the input references are restored and then lost or declared not valid again, the unit will then go back into the Holdover mode again.

Also, if the only available input reference is a manually set "user" time and the unit is subsequently rebooted or power cycled, time sync will be lost when it powers back-up. The time will need to be set manually again in order for the unit to return to its fully synchronized state.

Holdover Timeout

Holdover Timeout is a user-configurable allowable time period in which the unit remains in Holdover mode before it declares loss of synchronization. Holdover Timeout can be adjusted according to personal requirements and preferences. The factory default Holdover period is 2 hours. The Holdover Timeout value can be managed from the **Oscillators Settings** pop-up screen, accessed through **Disciplining Setup**.

NOTE: Changes made to the Holdover Timeout always take effect immediately. If the unit is in holdover and the Holdover Timeout is changed to a value that is less than the current time period that the unit has been Holdover Mode, the unit will immediately transition to out of sync.

The estimated error rates for each oscillator type, after losing the input references, are listed in the table *Estimated Oscillator Error Rates during Holdover*, below. Estimated rates are based on the oscillator being locked to a reference for 2 weeks and the ambient temperature remaining stable.

Oscillator Type	Typical Error Rates after 4 hrs	Typical Error Rates after 24 hrs
Rb (Rubidium)	0.2 microseconds (nominal)	1 microseconds (nominal)
Standard OCXO	1 microseconds (nominal)	25 microseconds (nominal)
TXCO	12 microseconds (nominal)	450 microseconds (nominal)

Estimated Oscillator Error Rates during Holdover

The length of the allowed Holdover Timeout period is displayed and configured in seconds. The table below provides example conversions for typically desired Holdover periods.

Desired Holdover Length	Holdover Length (in seconds) to be entered
2 hours	7200 seconds (default value)
24 hours	86400
7 days	604,800
30 days	2,419,200
1 year	29,030,400

NOTE: Due to Leap Seconds that are periodically inserted into the UTC and Local timescales, it is not normally recommended to exceed 30 days of Holdover without an external reference that can supply Leap Second information being applied (such as GNSS).

Configuring a Holdover value exceeding 30 days could result in a one second time error in the UTC or Local timescales until an external reference (GNSS or IRIG input) is restored or a manually configured Leap Second is asserted by a user (leap seconds do not affect the GPS and TAI time scales).

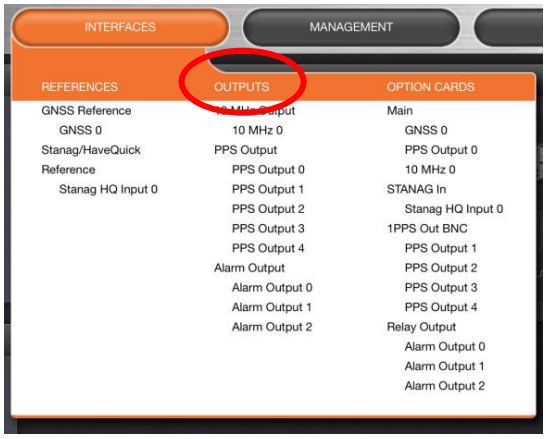
If no external references (such as GNSS or IRIG) are available when a Leap Second is scheduled to occur, manual Leap Seconds can also be applied to the UTC or Local time base in the “Set Leap Second” table located in the **MANAGEMENT/OTHER/Time Management** page.

3.15.2 System On-time Point, 1PPS/10 MHz Frequency Output Generation and Configuration

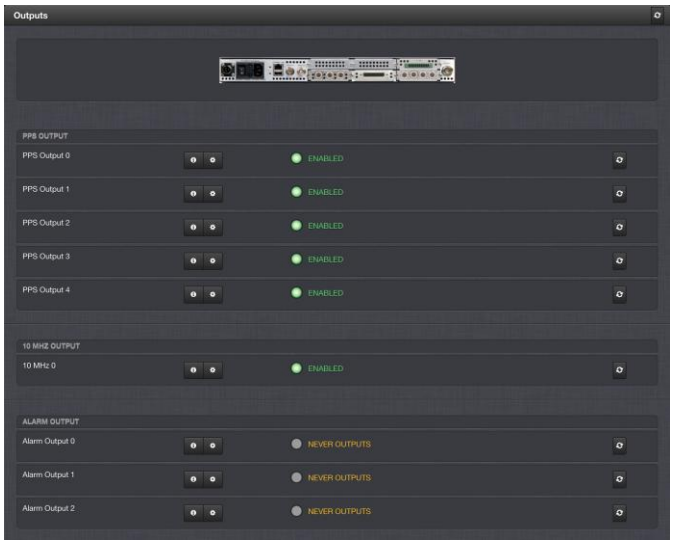
Accessing the 1PPS and 10MHz Configuration Screens

NOTE: Both models, 9383 and 9389 include 1PPS outputs. Only the model 9483 has a 10 MHz output.

To access the 1PPS and 10 MHz Configuration Screens navigate to the **Outputs** screen through the **INTERFACES/OUTPUTS** drop-down menu.



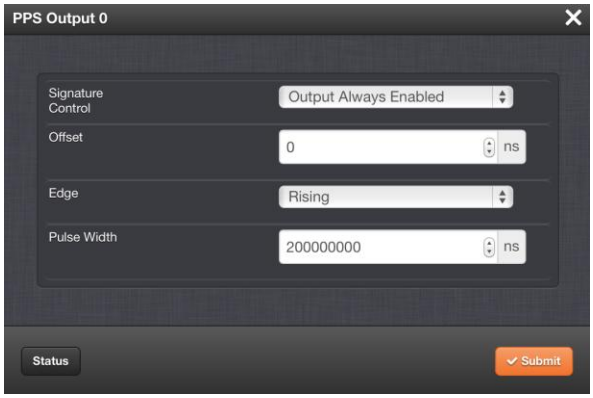
The **Outputs** screen will display.



NOTE: If you have only one output of any type, the unit will number that output 0. Additional outputs will be numbered 1 or above.

To configure base unit 1PPS output:

1. Click on the  button for the PPS output you wish to configure.
2. The **PPS Output 0** screen will display.



Configuration parameters for the 1PPS output are as follows:

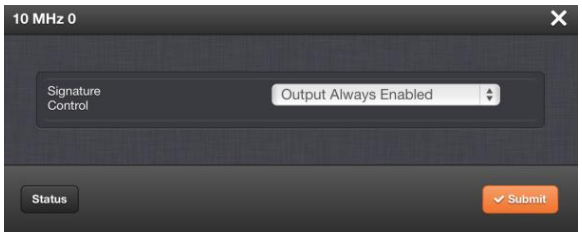
1. Fill in the available 1PPS output configuration fields as follows:
   - **Signature Control**—A drop-down list. Signature Control controls when the 1PPS output will be present
     - **Output Always Enabled**—The 1PPS output is present, even when the unit is not synchronized to its references
     - **Output Enabled in Holdover**—The 1PPS output is present unless the unit is not synchronized to its references (the 1PPS output is present while in the Holdover mode).
     - **Output Disabled in Holdover**—The 1PPS output is present unless the unit's references are considered not qualified and invalid. (the 1PPS output is not present while in the Holdover mode).
     - **Output Always Disabled**—The 1PPS output is not present, even if any of the unit's references are present and considered qualified.
   - **Offset**—Displays the currently configured 1PPS Offset (accounts for cable delays and other latencies). The Offset is entered and displayed in nanoseconds.
   - **Edge**—Used to determine if the on-time point of the 1PPS output is the rising or falling edge of the signal.
   - **Pulse Width**—Configures the Pulse Width of the 1PPS output. The Pulse Width is entered and displayed in nanoseconds (default Pulse Width is 200 milliseconds).
2. Click the **Submit** button at the bottom of the window.

Configuring 10 MHz Frequency Output (9483 only)

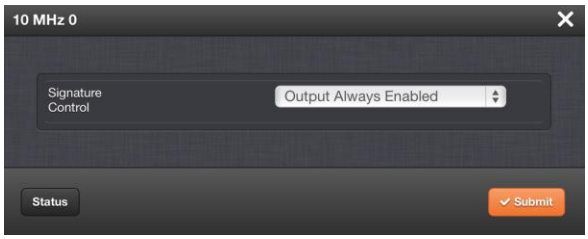
To configure the base unit 10 MHz output:

1. Click on the  button for the 10 MHz output you wish to configure.
2. The **10 MHz 0** screen will display.

To configure the 10 MHz output parameters:



1. Navigate to the 10 MHz edit screen.



2. Choose a value from the **Signature Control** field drop-down list as follows:

   - **Output Always Enabled—**The 10 MHz output is present, even when the unit is not synchronized to its references.
   - **Output Enabled in Holdover—**The 10 MHz output is present unless the unit is not synchronized to its references (the 10 MHz output is present while in the Holdover mode).
   - **Output Disabled in Holdover—**The 10 MHz output is present unless the unit's references are considered not qualified and invalid (the 10 MHz output is not present while in the Holdover mode).
   - **Output Always Disabled—**The 10 MHz output is not present, even if any of the unit's references are present and considered qualified.

3. Click the **Submit** button at the bottom of the window.

3.16 Reference Priority Input Configuration

NOTE: The following section is illustrative of how various time and frequency references can be configured as synchronization signals. Your unit will be limited to the configuration of supplied.

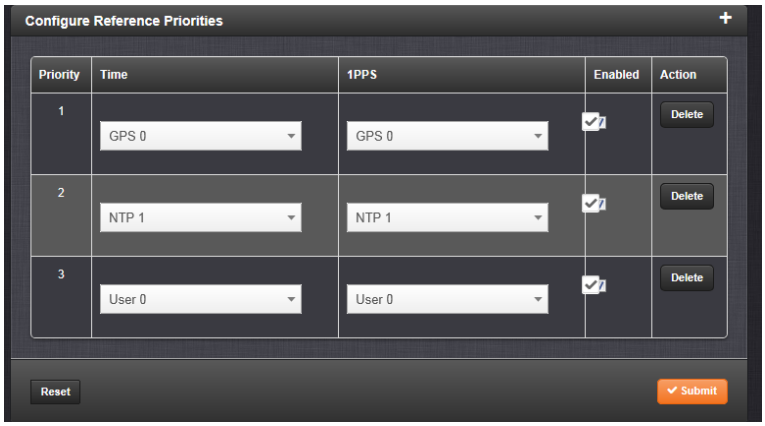
The NetClock can be synchronized to different external time sources. GPS and another NTP server are most typical. Or, a user can enter the system time manually, which NetClock can synchronize as the current time. In some cases, another reference may be available such as precision time protocol or T1/E1 signals

NOTE: If you are installing any new option module cards after your initial setup, you will need to either manually set up the desired card in the Reference Priority Table, or click on **Restore Factory Defaults** from the **Actions Panel** option on the Configure Reference Priorities screen (it is accessible from the **Management/Other/Reference Priorities** section) in order to update the table with the new reference information.

In order for NetClock to declare synchronization, it needs both valid 1PPS and valid time reference inputs.

Multiple references can be used to provide redundant inputs. The Reference Priority table allows multiple references to be defined in the order of priority desired. If the highest priority reference is available, it is selected. But if it's not available, the next lower priority reference will be selected, as long as it is available.

The **Configure Reference Priorities** panel is used to define the priority order for the desired inputs.



Each available type of Time and 1PPS input reference is assigned a "title" to be used in the Reference Priority table. The title defines the type of reference it is (e.g., "GPS 0" indicates GNSS input). These reference titles are defined in following table:

Title	Reference
ASCII Timecode	ASCII serial timecode input
External 1PPS	External 1PPS input
Frequency	External Frequency input
GPS	GNSS input
PTP	PTP input
IRIG	IRIG timecode input
Local System	The built-in clock OR internal 1PPS generation
NTP	NTP input
User	Host (time is manually set by a user)
HAVEQUICK	HAVEQUICK input

Reference Priority Input Names

NOTE: The number displayed indicates the number of feature inputs of that type presently installed in the NetClock - starting with "0" representing the first feature input. For example:

- IRIG 0: 1st IRIG input instance
- Frequency 1: 2nd frequency input instance
- NTP 2: 3rd NTP input instance

The columns of the Reference Priority table are defined as follows:

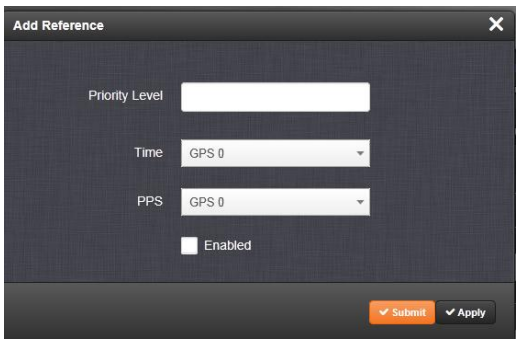
- **Priority**—Defines the order or priority for each index (row). The range is 1 to 16, with 1 being the highest priority and 16 being the lowest priority. The highest priority reference that is available and valid is the reference that is selected.
- **Time**—The reference selected to provide the necessary "Time" reference.
- **1PPS**—The reference selected to provide the necessary "1PPS" reference.
- **Enabled**—The reference is enabled.
- **Delete**—Removes the Index (row) from the Reference Priority table.

Adding an Entry to the Reference Status Table

To add an entry to the **Reference Status** table:

1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. Click on the "+" button in the upper right-hand corner of the **Configure Reference Priorities** table.

3. The **Add Reference** window will display.



4. In the **Add Reference** window, enter:
   - **Priority Level**—This is the priority you want to give your reference.
   - **Time**—Enter the time reference.
   - **PPS**—Enter the PPS reference.
   - **Enabled**—Check this box to enable the new reference.
1. Click on the **Apply** button or the **Submit** button.

NOTE: Clicking the **Apply** button will apply the settings and will not close the **Add Reference** window.
Clicking the **Submit** button will close the **Add Reference** window.

Deleting an Entry from the Reference Status

To delete an entry from the **Reference Status** table:

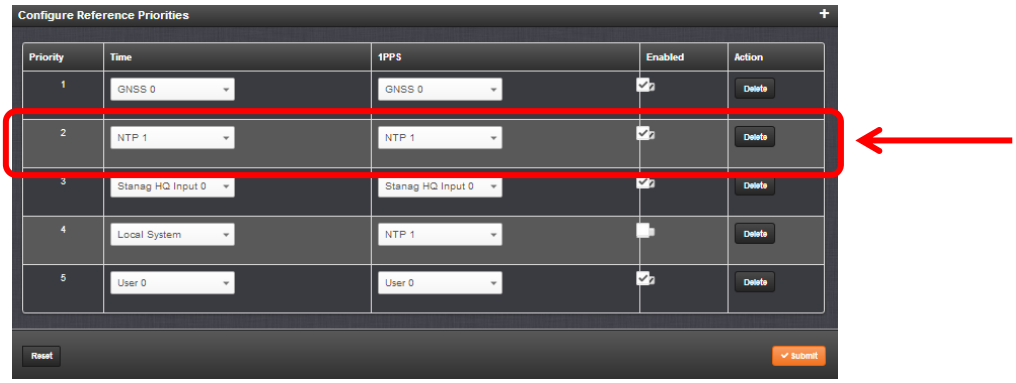
1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. Click on the **Delete** button in the right-hand corner for the entry you wish to delete in the **Configure Reference Priorities** table.

3. Click the **Okay** in the pop-up window that displays.

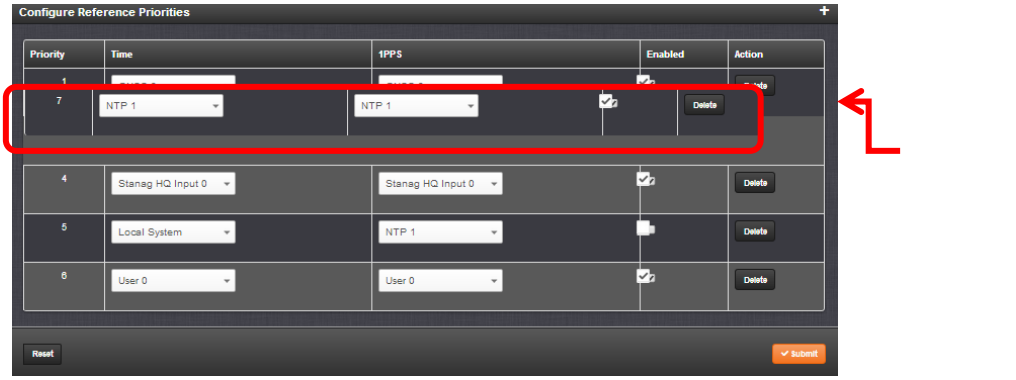
Reordering items in the Reference Priority Table

To reorder the priority of a reference:

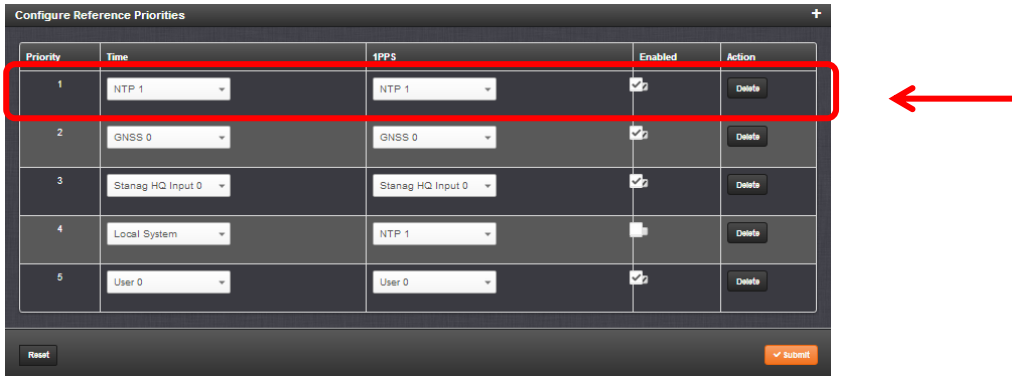
1. Navigate to the **Configure Reference Priorities** screen through the **MANAGEMENT/OTHER/Reference Priority** menu.
2. Click and old on the item whose priority you wish to reorder.



3. Drag that item to the place in the order you wish the item to take.



4. The Reference Priority table is now reordered.



5. Click the **Submit** button.
6. Clicking the **Reset** button will return the priority order to that how it was when the window was opened.

Example: Desire the Ability to use "User Set Time" for the Input Time Reference, but want to use IRIG as the Input 1PPS Input:

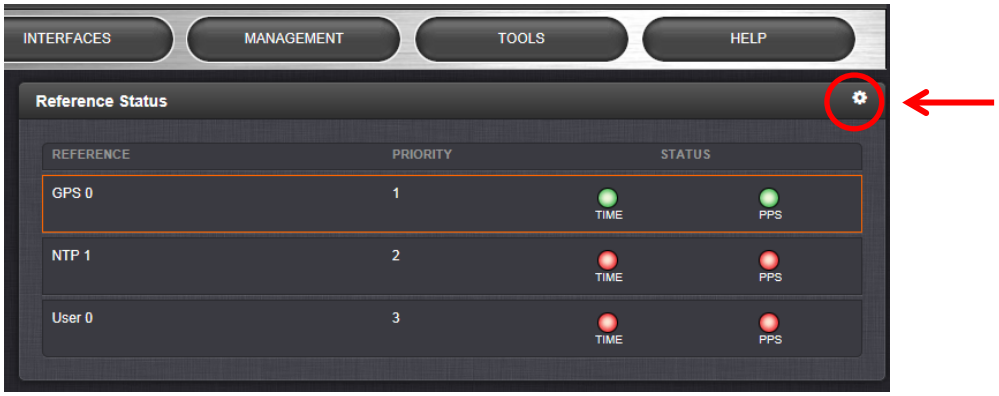
1) From the **Add Entry** table, change the **State** option to "Enabled"
2) Set the Priority for this new Index (1-15 with the lower the number, the higher its priority as the input).
3) Set the **Time** field to "User" (this is the input Time reference).

4) Set the **1PPS** field to “IRIG” (this is the input 1PPS reference).
5) Click the **Add** button.
6) Click the **Submit** button.
7) Observe a new entry has been added to the **Reference Priority Setup** table. This new entry can be edited as desired directly in the Reference Priority table.

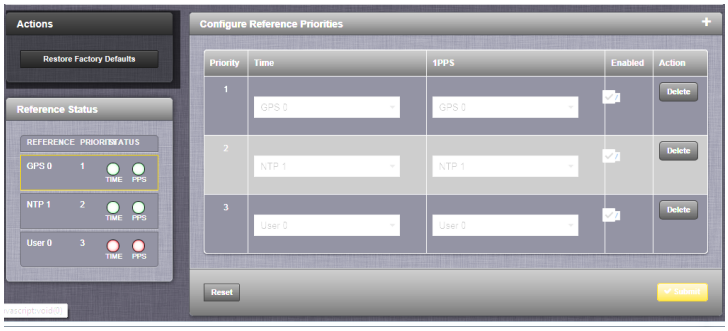
Resetting Reference Priorities to Factory Defaults

To reset the Reference Priority table to the factory default configuration:

1. Navigate to the **Configure Reference Priorities** screen **the MANAGEMENT/OTHER/Reference Priority** menu.



2. In the **Actions** panel, click on the **Restore Factory Defaults** button.



Important Information Regarding “User” Input Reference (Manually Set Time):

The “User” reference input provides a “one-time-only” ability to use a manually set time as the system time. It requires manual intervention each time it is to be used (just having this “User” reference enabled does not automatically allow the current time to be considered valid and used as a reference). In order for the time to be considered valid, the user needs to “set” the time.

If a higher priority reference is enabled and the input reference goes away with no other external time references being available, the user needs to set the time manually in order for the unit to continue to be synchronized. Or, if the unit is power cycled anytime thereafter, with no other references enabled or available, the time must be manually set to be considered valid, before being used to synchronize the unit.

For example, GNSS input is enabled and present, and configured as a higher priority than "User". If GNSS is then lost, in order for the time to remain synced, the user has to "set" the time manually. Having "User" enabled in the Reference table allows the ability for the user to set the time manually. If GNSS is restored and because GNSS is configured as a higher priority than the "User" (manually set time), GNSS will become the selected time reference. If GNSS goes away again, the user has to once again "set" the time manually again in order for the time to remain synchronized.

In this example, if GNSS reception is lost and if the time is not manually set by the user, and if no other references are available, the unit will go into the Holdover mode the moment GNSS is lost. If GNSS is not restored or the time is not manually set before the Holdover period expires, Time Sync is lost and the outputs may become unusable (the length of available Holdover is configured in the **Setup/Disciplining** page).

Also, if no other external references are available after a power cycle, the time needs to be manually set again in order for the unit to be synced unless battery backed time synchronization is enabled. After a power cycle, the unit cannot return to the Holdover mode until a reference is available and then all of those reference(s) are subsequently lost. After power-up the unit will remain in Time Sync alarm until either external references are restored or the time is manually set with "User" enabled in the Reference table.

NOTE: When using "User" with another higher priority reference (such as GNSS or IRIG) being enabled (so that it could become an available reference if it's declared valid), the System Time should be set as accurately as possible. If the input reference was to switch from "User" to another available reference (such as GNSS) and a large time correction was needed to be applied because the System Time error was too large, NTP will go out of sync.

If this time jump is excessive, (greater than 1000 seconds), NTP will exit synchronization and will not correct for the time jump until the NTP service is either stopped and then restarted or until the unit is rebooted. If the time difference between the "User" set time and the higher priority reference when its selected is less than 1000 seconds, NTP will remain in sync and will slew (over a period of time) to the new reference time.

Note: Selecting "Local System" as an Input Reference

"Local System" input reference is a unique input reference in that in can be used as either the Time input reference or the 1PPS input reference, but can never be both. It must be used in conjunction with another input reference (such as "GPS" or "IRIG" for example).

When the Time reference is configured as "Local System" (with the 1PPS reference configured as a different input reference), the Time that the unit powers up with is considered valid time, as long as the 1PPS input reference is valid.

When 1PPS reference is configured as "Local System" (with the Time reference configured as a different input reference), the unit's internal 1PPS will be used as a valid 1PPS input reference as long as the Time reference is valid.

Reference Priority Input USE CASE Examples:

Example 1—GNSS as Primary References, IRIG as Backup:
It is desired to have:

- GNSS as the primary time and 1PPS reference

- IRIG as the backup time and 1PPS time reference.

For this configuration:

1. Move the reference which has "GPS 0" in the **Time** column and "GPS 0" in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. Move the reference which has "IRIG 0" in the **Time** column and "IRIG 0" in the**1PPS** column to the second place in the table, with a **Priority** value of 2. Click the **Enabled** checkbox.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

   Because these are both default references, no additional references need to be added to the Reference Priority table.

Example 2—IRIG as Primary Reference, NTP Input as Backup:

It may be desired to have:

- IRIG as the primary reference input
- Another NTP server as backup reference, in case the IRIG input is lost.

For this configuration:

1. Move the reference which has "IRIG 0" in both the **Time** column and "IRIG 0" in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. Move the reference which has "NTP" in the **Time** column and "NTP" in the **1PPS** column to the second place in the table, with a **Priority** value of 2. Click the **Enabled**.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

   Because these are both default references, no additional references need to be added to the Reference Priority table.

Example 3—NTP Input as Only Available Input (also Referred to as "NTP Stratum 2 Synchronization"):

It may be desired to have:

- NTP provided by another NTP server as the only available reference input.

For this configuration:

1. Move the reference which has "NTP" in the **Time** column and "NTP" in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
2. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

Important Note: When selecting NTP as an input reference, do not select another reference (such as GNSS, IRIG, etc.) to work with NTP as a reference. NTP should always be selected as both the Time and1PPS input when it is desired to use NTP as an input reference.

Example 4—User Desires to Manually Set the Time. Other References May or May Not Be Available:

NOTE: In order for a manually set time to be considered valid and used to synchronize the unit, a "User" needs to be enabled in the Reference Priority table.

It may be desired to have a manually set the time reference.

For this configuration:

1. If necessary (see **NOTE** above), create a "User."
2. Move the reference which has "User 0" in the **Time** column and "User 0" in the **1PPS** column to the top of the table, with a **Priority** value of 1. Click the **Enabled** checkbox.
3. For all other references, uncheck the **Enabled** checkbox, so that they are all disabled.

If it is desired to use a manually set time as a backup to other references (such as GNSS or IRIG):

1. Move the reference which has “User 0” in both the **Time** column and “User 0” in the **1PPS** column to a place in the table with a lower priority than the references the manually set reference will be backing up. Click the **Enabled** checkbox.

   With “User” enabled, if no other higher priority references are enabled or available (or if the higher priority references have since been lost), you can simply set the System time to the desired value. The unit will go into synchronization using this set time.

   The time can be manually set through the **System Time** panel located in the **MANAGEMENT/OTHER/Time Management** page. When you have set the date and time, the front panel sync light will turn green.

NOTE: This process needs to be repeated each time the unit is power cycled (with no other references available) unless synchronizing to a battery backed time on startup is enabled or after each time all higher priority references are lost.

Example 5—User Desires to Use the Time that the NetClock Powers Up with (Local System) as the Valid Time. The 1PPS Input Reference Will Be Derived from GNSS Input):

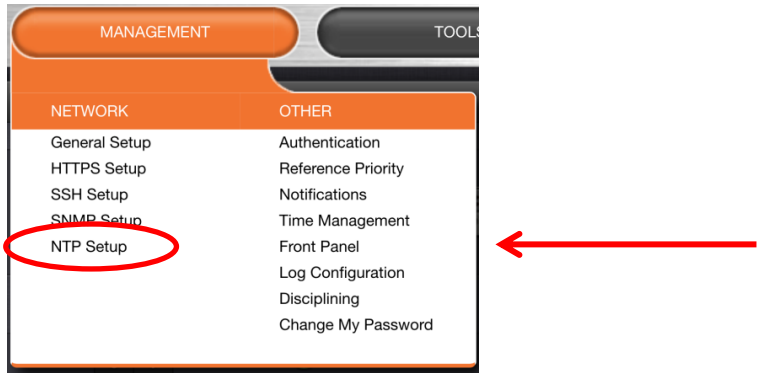
It may be desired to use the time that the NetClock powers up with (without the need for a user to manually set it, as would be done with “User” selected). This is referred to as “Local System.” Because “Local System” can’t be both Time and 1PPS input together, set GNSS as the 1PPS reference input. Because there is no default Index for “Local System” and “GPS”, a new Entry needs to be added to the Reference table in order to use this combination of references.
For this configuration:

1. Add a reference (see **0 Adding an Entry to the Reference Status Table**) with the following settings:
   - Check **Enabled** checkbox.
   - In the **Priority Level** text box, enter 1. This will give this reference the highest priority.
   - In the **Time** field, select “Local System”
   - In the **PPS** field, select “GPS”.
2. Confirm that the first reference in the Reference Priority table has “Local System” as the **Time** input and GNSS as the **1PPS** input.
3. After a power cycle or reboot, as soon as GNSS is declared valid, the System Time will automatically be used as-is, with no manual intervention required.

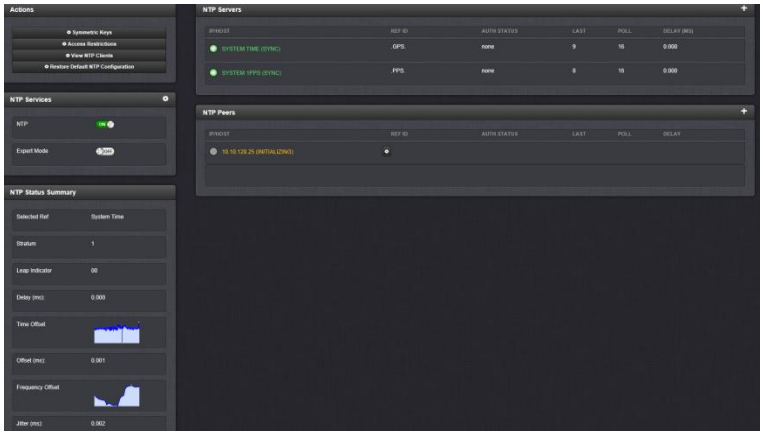
3.16.1 Configuring NTP

Accessing the NTP Setup Screen

To access the **NTP Setup** screen, choose **MANAGEMENT/NETWORK/NTP Setup**.

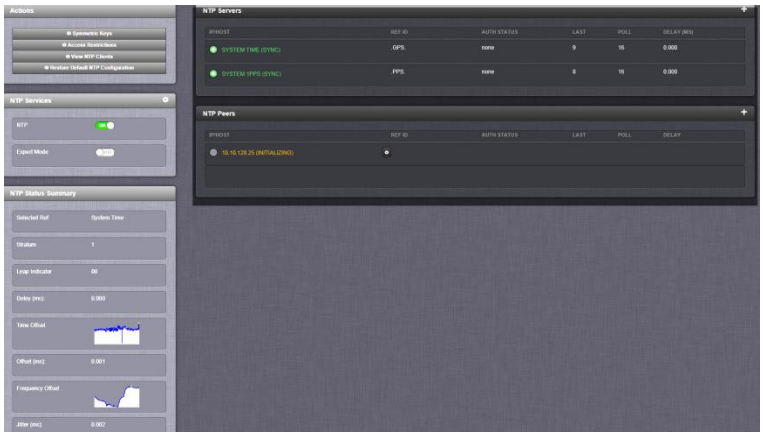


The **NTP** screen will display.



The **NTP** screen is divided into 4 panels:

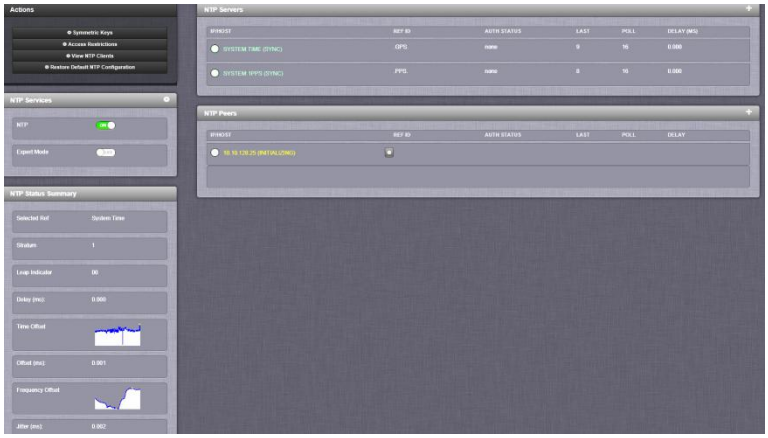
The main panel



The main panel is divided into 2 displays:

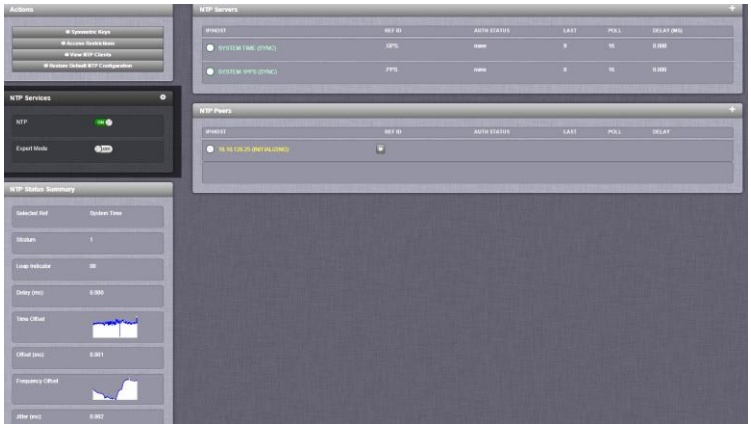
- **NTP Servers**—In this display you can view the NTP Servers you have set up in your network. It is through this display that you configure external NTP references.
- **NTP Peers**— In this display you can view the NTP Peers you have set up in your network. It is through this display that you configure NTP Peer reference inputs

The **Actions** panel



- **Symmetric Keys**—Click here to set up your symmetric keys for MD5 authentication. See **0 Symmetrical Keys (MD5 Authentication)**
- **Access Restrictions**—Click here to view, change or delete access restrictions to the NTP network. Fields in the NTP Access Restrictions table include
  - Type
  - IP Version
  - IP
  - IP Mask
  - Auth only
  - Enable Query
- **View NTP Clients**—Click here to reveal a table of all the clients the NTP server is servicing. Information for each client includes:
  - Client IP
  - Received Packets
  - Mode
  - Version
  - Restriction Flags
  - Avg Interval
  - Last Interval
- **Restore Default NTP Configuration**—Click here to restore the unit's NTP settings to the factory default. Any settings you have created will be lost.

The **NTP Services** panel



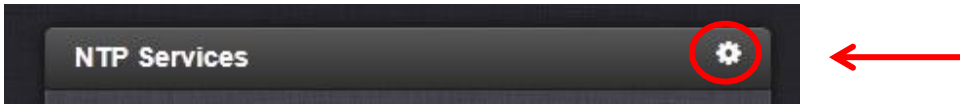
- **NTP ON/OFF—**This switch turns NTP on (enables NTP) and off (disables NTP).

NOTE: When the NTP timescale is changed or when you have changed any NTP configurations, use this switch to disable and then enable NTP.

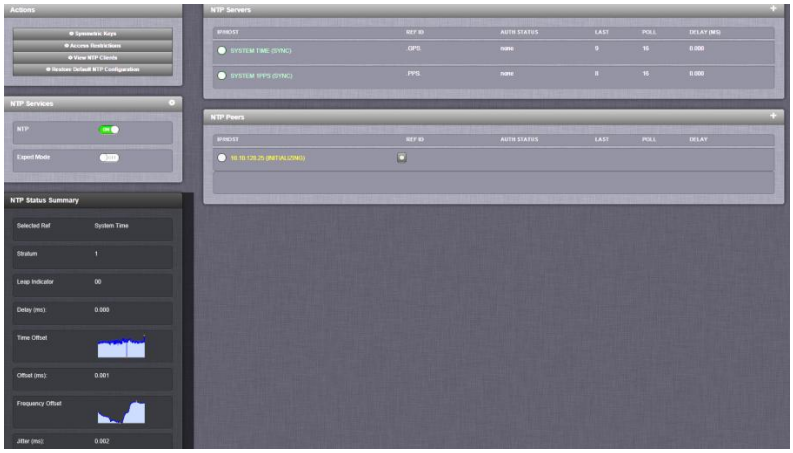
- **Expert Mode—**Turning this switch on enables direct access to the NTP.conf NTP configuration file, for when the user wishes to bypass the Web interface. The Expert Mode switch is set to OFF by default.

NOTE: Spectracom Tech Support does not support the editing of the NTP configuration files in Expert Mode. For additional information on editing the NTP.conf file, please refer to http://www.ntp.org.

- Other NTP Services that can be configured through the NTP Services panel are:
  - Broadcast
  - Autokey
  - Stratum 1
- These services are accessed by clicking the  button.



The **NTP Status Summary** panel



- The NTP Status Summary panel gives you a quick representation of the status of the NTP network. Information referenced in this panel includes:
  - **Selected Ref**—This is NTP server the unit is using as its selected reference
  - **Stratum**—This is the stratum level at which the unit is operating.
  - **Leap Indicator**—The leap indicator bits (usually 00). See **7.1.2 Leap Second Alert Notification**.
  - **Delay (ms)—**The measured one-way delay between the unit and its selected reference.
  - **Time Offset**—This is a graphical representation of the system time offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See **0 Inspecting the NTP Performance Graph—Time Offset**.
  - **Offset (ms)—**Displays the configured 1PPS offset values.
  - **Frequency Offset**—This is a graphical representation of the system frequency offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See **0 Inspecting the NTP Performance Graph—Frequency Offset.**
  - **Jitter (ms)—**Variance (in milliseconds) occurring in the reference input time (from one poll to the next).
  - **Jitter**—This is a graphical representation of the system jitter over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See **0 Inspecting the NTP Performance Graph—Jitter**.

NetClock and NTP

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.

When the NTP service is enabled, the unit will "listen" for NTP request messages from NTP clients on the network. When an NTP request packet is received, the unit will send an NTP response time packet to the requesting client. Under typical conditions, the unit can service at least 7,000 NTP requests per second without MD5 authentication enabled, and at a somewhat lower rate with MD5 authentication enabled.

The user can either enable or completely disable the NTP Service. When NTP is disabled, no NTP time packets will be sent out to the network. When NTP is 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.

Typically, the factory default configurations of the NTP settings do not need to be modified for NTP operation. However, NTP has configurations available that allow the normal operation of NTP to be altered for unique applications. These features include the ability to use either MD5 authentication or NTP Autokey, to block NTP access to parts of the network and to broadcast NTP data to the network's broadcast address.

NTP Peers and NTP Servers (Stratum Synchronization)

Other available NTP servers can be configured as potential input time references for System Time synchronization. A group of NTP servers at the same Stratum level (Stratum 1 time servers for example) are listed as NTP peers to each other. NTP Servers at a higher Stratum than another are configured as NTP Servers instead (Internet Time Servers should be configured as NTP Servers and not as NTP peers).

Important Note: In order for other NTP servers to be a valid reference, "NTP" must be enabled in the Reference Priority table.

It is recommended to use one or more NTP 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 clients on the network.

The unit can be configured to receive time from one or more available NTP servers (such as other NetClocks or Spectracom SecureSyncs). The other NTP servers can then be valid input references for System Time synchronization. This is commonly referred to as NTP Peering.

When the unit is configured to obtain time from other NTP servers at the same Stratum level (configured as NTP Peers) but is currently using another input reference other than the NTP server(s) as its selected reference, the unit will report to the network (in the NTP time stamps) that it is a Stratum 1 time server. But, at some point, if all other input references besides the other NTP server(s) become unavailable, the unit will then drop to a Stratum 2 time server (with System Time being derived from the NTP time packets being received from the other NTP Peers.

When the unit is configured to obtain time from other NTP servers at a higher stratum than it is (configured as NTP Servers) and is using the NTP server as its selected reference, the unit will report to the network (in the NTP time stamps) that it is one less Stratum than its selected reference NTP server (i.e., if the unit is configured to receive time from one or more Stratum 1

NTP Servers, with no other higher priority input references available, the unit will report to the network that it is a Stratum 2 time server).

In order for the unit to use other NTP servers as a valid time reference to synchronize the System Time, the input Reference Priority Setup table must be configured to allow NTP as an available reference.

If the unit is synchronized to another NTP server and the other NTP server subsequently loses sync or becomes unavailable (with no other higher priority input references being present and valid) the unit will then go into the Holdover mode until any enabled and valid input reference becomes available again (or until the Holdover period expires, whichever one occurs first). During Holdover mode, NTP will remain at the same Stratum level it was before entering the Holdover mode and can continue to be reference to the network. However, if no input reference becomes available before the Holdover period expires, Time Sync will be lost and shortly thereafter, NTP will report to the network that it is now at Stratum 15. A status of Stratum 15 will cause the network to ignore the unit as an NTP time reference. Refer to **3.15.1 Holdover Mode** for information on obtaining or configuring the allowable Holdover period.

NTP Output Timescale

The timescale for the time that is provided to the network nodes via the NTP time stamps is determined by the Timescale selected in the unit's System Time Setup Page, accessed through the Web interface at **MANAGEMENT/OTHER/Time Management**. If the Timescale in System Time Setup is selected as "UTC", the network PCs will receive UTC time via NTP. If "GPS" is selected instead, the network PCs will receive GPS time via NTP. When the Timescale is set to "GPS", the GPS-to-UTC offset on the Setup/Time Management page must be set correctly. Typically, UTC is the desired Timescale for network synchronization.

Important Note: Make sure the desired timescale for the NTP output is selected in the System Time Setup. Having the incorrect timescale selected can result an undesired time error in the NTP clients that are synchronizing to the unit via NTP. As of September 2013, the offset between UTC and GPS time is 16 seconds.

Important Note: Configuration changes made to unit's NTP configurations do not take effect until the NTP Service is Disabled and then Enabled (or until the unit is rebooted/power cycled). The NTP service can be stopped and started from the **MANAGMENT/NTP Setup** in the NTP Services panel. Once NTP has been re-enabled, NTP will be available again for network synchronization within a few minutes.

The **MANAGEMENT/NETWORK/NTP Setup** page allows NTP broadcast capability to be enabled (this feature very rarely needs to be enabled) and allows the network access of the NTP time stamps to be limited to only certain clients on the network (this feature is also rarely used).

Timing System Reference Preferred and Enable Timing System 1PPS Reference

If desired, Time and PPS References for the NTP service can be configured as "Preferred". This provides additional "weighting" to that particular NTP input reference during the selection process, while NTP is deciding which reference it should select as its source (though "prefer" does not guarantee that reference will become the selected reference).

- The Timing System Reference/Preferred (Enabled/Disabled) option configures NTP to "weight" the Timing system input heavier than input from other NTP servers for its selection (The Timing System inputs are normally more accurate than other NTP servers). However, if the Timing System inputs are not normally available (such as with intermittent GNSS reception or no other inputs are available), it may be desired not to prefer the Timing System over an NTP reference, in which case this box should not be checked.

- The Timing System 1PPS Reference (Enabled/Disabled) option determines whether or not NTP uses the 1PPS input from the Timing System. The 1PPS input to NTP needs to correlate with its "Time" input. If the Time and PPS inputs are originating from the same source, they will be correlated. However, if the time is originating from another NTP server, but the 1PPS is being derived by the Timing System, the two inputs may not always correlate. Without this correlation, NTP performance will be degraded. In this scenario, it is best not to use the System Time's 1PPS as a reference.

Normally, the NTP service will obtain its Time and PPS reference inputs from the Timing System (the Timing System is the time as derived from the GNSS, IRIG, ASCII data inputs, etc.). However, if desired, NTP can also obtain time from other NTP server(s). When the Timing System references are normally available to the unit, the "Timing System 1PPS reference" should be enabled and the "Timing System Reference" should be Preferred (both of the boxes at the top of the page enabled). This provides NTP with the most accurate references.

In the case of Stratum synchronization (only syncing the unit to other NTP servers, instead of the Timing System, so that is can operate as a Stratum 2 time server, for example), the Timing System inputs are not going to be available, as the only available input will be other configured NTP servers. In this scenario, it is best to uncheck both options at the top of the page so that the Timing System is not preferred over a configured NTP server and to keep the Timing System's 1PPS from affecting the operation of NTP (as its 1PPS will not correlate with the NTP time input being received from the other NTP servers).

NOTE: It is not normally recommended to enable the "Timing System Reference Preferred" checkbox in addition to enabling any of the "Preferred" boxes in the NTP Servers table. Normally, either select the "Prefer Timing System Reference" and none of the Preferred boxes in the NTP servers table (if the Timing System inputs are normally available) Or De-select the "Prefer Timing System Reference" and enable "Preferred" on one of the NTP servers in the NTP Servers table (if the Timing System inputs are not normally available).

It is not normally recommended to select more than one NTP Server in the NTP Servers table as being "Prefer." Typically, only one NTP server in the table should be selected as "Prefer" (and should only be selected if the "Prefer Timing System Reference: box is not checked).

The maximum number of NTP Peers (or NTP Servers) that can be configured as time references is twelve (12). For best results, more than four NTP time servers are recommended. As few as one NTP time server may be used, however, depending on your needs and network timing architecture. A specific NTP server is recommended to be configured as the preferred time reference by selecting the preferred checkbox.

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 unit 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 selecting the Clear checkbox and pressing Submit.

The grids on the NTP Peers and Servers tabs allow the user to define, by IP address or hostname, the locations of other NTP servers to use as time references (instead of, or in addition to, the configured unit's primary reference) and the locations of other NTP servers to use as peers. The maximum number of Peers allowed is twelve (12).

NTP Autokey—Overview

The unit provides an NTP version 4.2.6p5 which supports the Autokey Protocol. The Autokey Protocol uses the OpenSSL library which provides security capabilities including message digests, digital signatures and encryption schemes. The Autokey Protocol provides a means for NTP to authenticate and establish a chain of trusted NTP servers.

NTP Autokey—Support & Limitations

Currently, the unit supports only the IFF (Identify Friend or Foe) Autokey Identity Scheme. The user web interface automates the configuration of the IFF using the MD5 digests and RSA keys and certificates. At this time the configuration of other key types or other digests is not supported.

NOTE: When you configure NTP Autokey, you must disable the NTP service first, and then re-enable it after Autokey configuration is completed.

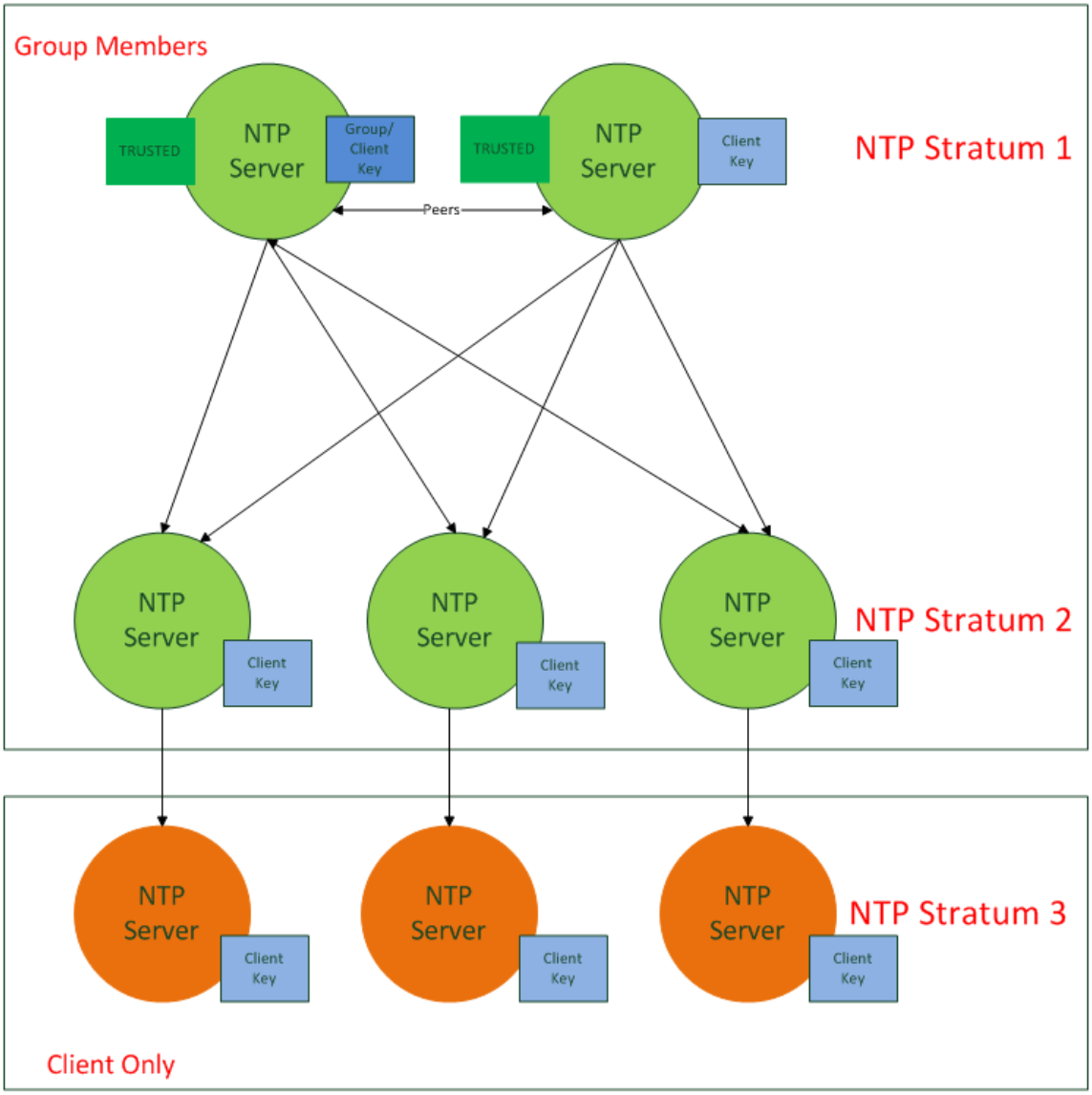
NTP Autokey—IFF Autokey Support

The IFF Autokey Support is demonstrated in the figure below. The IFF identity scheme is used with Multiple Stratum NTP Time Servers. The example below shows 3 Stratum layers. Stratum 1 NTP Servers are closes to the physical time references. All Stratum 1 servers can be Trusted Hosts. One of them is used to generate the IFF Group/Client Key. This defines the IFF Group.

All other group members generate Group Certificate and RSA public/private keys using MD5 digest. Each group member must share the common IFF Group/Client Key (**recommended**). Stratum 2 NTP servers are also members of the Group. All NTP Stratum 1 servers are Trusted Hosts. The NTP servers closest to the actual time reference (Stratum 1) should be designated trusted. A single Stratum 1 NTP server generates the IFF Group/Client Keys. There is NO group name feature supported. The Group can use the same passphrase (password) or different passphrases for each client.

A NTP Server Group member is configured by enabling Autokey and creating certificate and public/private key pair while not enabling the Client Only selection. A Client Only NTP server is configured by enabling Autokey and creating certificate and public/private key pair and enabling the Client Only selection.

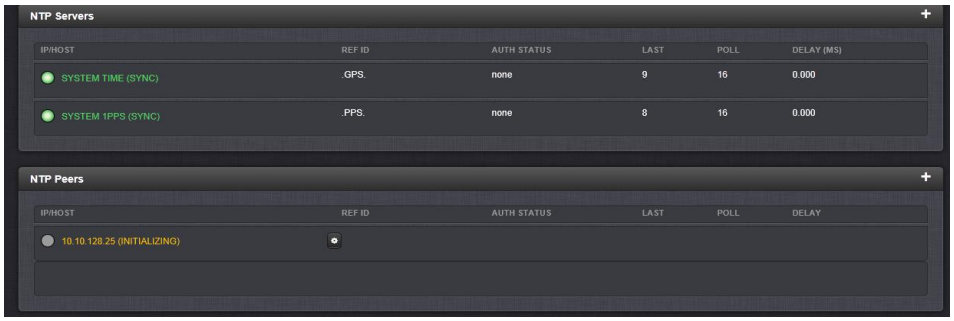
NOTE: Passphrases can be identical for all group members and Client NTP Servers. Or passphrases can be the same for group members and a different passphrase shared between the Client Only NTP Servers.



IFF Autokey Configuration Example

Symmetrical Keys (MD5 Authentication***)***

The unit 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. The Symmetrical Keys tab allows NTP to be configured to use MD5 authentication. See **0 Creating Symmetrical Keys (MD5 Authentication).** The **NTP Servers** and **NTP Peers** panels.



The **NTP Servers** and **NTP Peers** panels display which servers in the network are set up at a higher stratum (Servers) or at an equal stratum (Peers).

The **NTP Servers** panel and **NTP Peers** panel display the following information:

- **IP/HOST**
- **REF ID—**The type of input reference (for example, “GPS” indicates the reference can use GPS for its synchronization). Below is a list of potential REF IDs reported by the timing system (others may be reported by other NTP peers or servers):
  - **GPS**—GNSS reference
  - **IRIG**—IRIG reference
  - **HVQ—**HAVE QUICK reference
  - **FREQ**—Frequency reference
  - **PPS**—External 1PPS reference
  - **PTP**—PTP reference
  - **ATC**—ASCII time code reference
  - **USER**—User provided time
  - **LOCL**—Local reference (synced to itself)
  - **INIT**—NTP on server/peer is initializing
  - **STEP**—NTP on server/peer is performing initial synchronization step and restarting
- **AUTH STATUS—**Indicates if the selected reference is using MD5 authentication. “None” indicates authentication not being used.
- **LAST—**The number of seconds it’s been since this reference was last polled for its time.
- **POLL—**The poll interval, how often the unit is polling this NTP reference for its time.
- **DELAY (MS)—**The measured one-way delay between the unit and its selected reference.

NOTE: NTP clients of the unit are viewable through the **View NTP Clients** option In the Actionsl panel of the NTP Setup screen.

NOTE: In order for other NTP servers to be a valid reference, “NTP” must be enabled as both the Time and 1PPS references in the Reference Priority table.

To remove a server (and its associated configurations), select the “**Clear**” option at the end of its row to “Enabled” and click Submit. That particular row will then be immediately cleared.

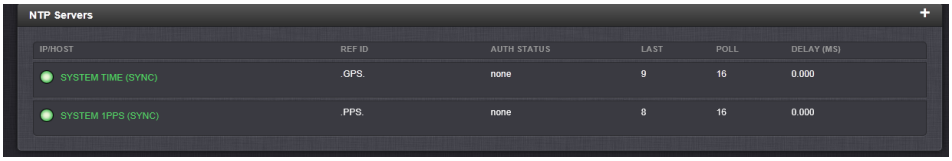
NOTE: In order for NTP configuration changes to take effect, NTP should be disabled and then enabled after any configurations changes have been made. NTP can

be stopped and restarted from the **MANAGEMENT/NETWORK/NTP Setup** page, in the **NTP Service** panel on the left-hand side of the page. See **0 Accessing the NTP Setup Screen, 0 Enabling and Disabling NTP**. In the "NTP service" field, select "Disabled', then click Submit to disable NTP, then Select "Enabled" and click Submit again to re-enable NTP. Changes made will now take effect and NTP operation will be restored shortly after this operation is performed.

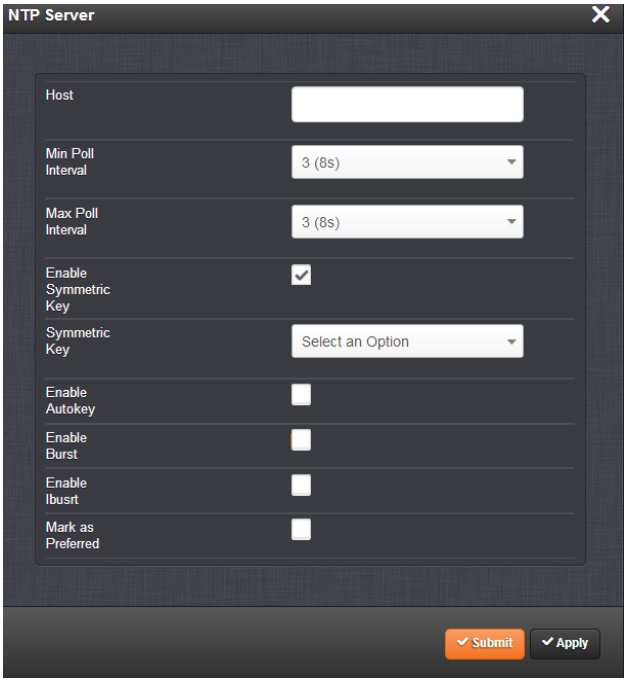
If the unit has no valid Timing System Reference, NTP Server or NTP Peers, the NTP Stratum value is automatically increased to Stratum 15. This ensures no NTP clients can use it as a time reference when unsynchronized. This feature utilizes automatic enabling and disabling of the Local Clock Reference driver to force Stratum 15. The automatic Local Clock Reference mode is disabled in NTP Expert mode if the user configures a Local Clock Reference Driver, or if the comment "`# DISABLE_AUTO_LOCAL`" is added to the NTP configuration file.

Configuring NTP Servers

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Servers** panel click on the "**+**" button.



3. The **NTP Server** window will display.



4. Enter the required information in the text fields.

- **Host**—Enter is the IP address for the server to be used as host.
- **Min Poll Interval**—Select a value from the drop down.
- **Max Poll Interval**—Select a value from the drop down.
- **Enable Symmetric Key**—Click to enable Symmetric Key, and then select an option from the drop down that displays.

NOTE: Before you can choose an option in the Key field, you must first set up symmetric keys through the Actions Panel. See **0 Symmetrical Keys (MD5 *Authentication)***. Conversely, you may check the **Autokey** box below the Key field.

- **Enable Autokey**—Click here if you want to use Autokey with this server. See **0 NTP Autokey—Overview** for more information about using Autokey.

NOTE: When you configure NTP Autokey, you must first disable the NTP service in the **NTP Services** panel, and then re-enable it after Autokey configuration is completed.

- **Enable Burst**—This tells NTP to send a burst to the remote server when the server is reachable.
- **Enable Iburst**—This tells NTP to send a burst to the remote server when the server is not reachable.
- **Mark as Preferred**—Click here to make this server the preferred server. See **0 Timing System Reference Preferred and Enable Timing System 1PPS Reference.**

NOTE: It is not normally recommended to select more than one NTP Server in the NTP Servers table as being preferred. Typically, only one NTP server should be selected as preferred.

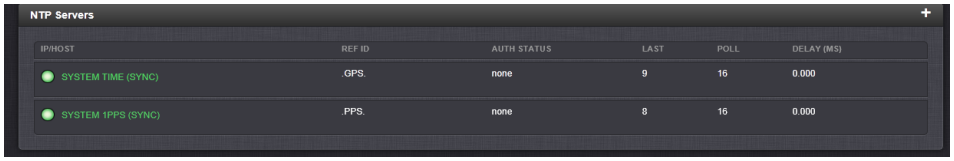
5. Click the **Apply** or **Submit** button at the bottom of the window.

NOTE: Clicking the **Apply** button will apply the settings and will not close the NTP Server window.
Clicking the **Submit** button will close the **NTP Server** window.
Clicking the **Apply** button allows the user to set up multiple servers without needing to constantly reopen the **NTP Server** window. Simply enter a new IP address in the Host field, enter the desired settings and click the **Apply** button for each new host. When you are done, click the **Submit** button.

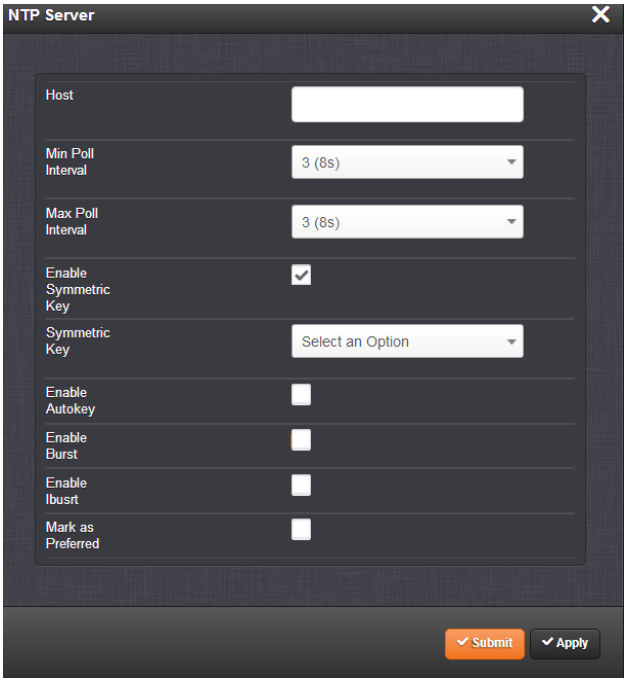
The NTP Server you have set up will appear in the **NTP Servers** panel.

Editing/Deleting NTP Servers

1. Navigate to the **NTP Setup** page through the **MANAGEMENT/NETWORK/NTP** menu.
2. In the **NTP Servers** panel. Double click anywhere on the row displaying the information for the NTP server you wish to edit/delete.



3. The **NTP Server** window will display.



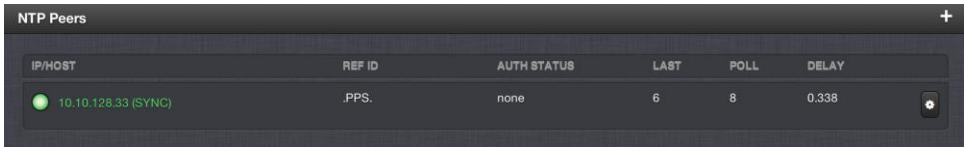
4. Enter the required information in the text fields. See **0 Configuring NTP Servers**.
5. Click the **Submit** or **Apply** button to apply the edited settings.

NOTE: Clicking the **Apply** button will apply the settings and will not close the **NTP Server** window.
Clicking the **Submit** button will close the **NTP Server** window.

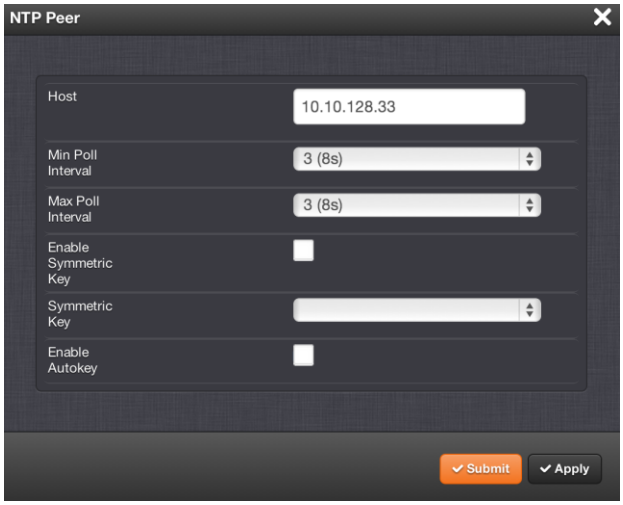
6. To delete a server, click the **Delete** button at the bottom of the window.

Configuring NTP Peers

1. Navigate to the **MANAGEMENT NTP Setup** screen.
2. In the **NTP Peers** panel click on the "+" button.



3. The **NTP Peer** window will display.



4. Enter the required information in the text fields:
   - **Host**—Enter is the IP address for the server to be used as host.
   - **Min Poll Interval**—Select a value from the drop down.
   - **Max Poll Interval**—Select a value from the drop down.
   - **Key**—Select an option from the drop down.

NOTE: Before you can choose an option in the **Key** field, you must first set up symmetric keys through the Actions Panel. See **0 Creating Symmetrical Keys (MD5 Authentication)**. Conversely, you may check the **Autokey** box below the **Key** field.

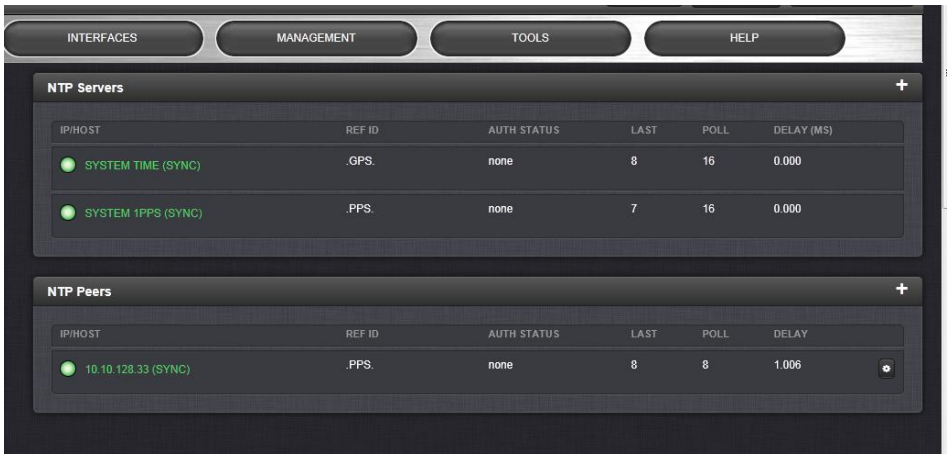
- **Autokey**—Click here if you want to use Autokey with this server rather than setting up MD5 Authentication. See **0 NTP Autokey—Overview** for more information about using Autokey.

NOTE: When you configure NTP Autokey, you must first disable the NTP service in the **NTP Services** panel, then re-enable it after Autokey configuration is completed.

5. Click the **Submit** button.

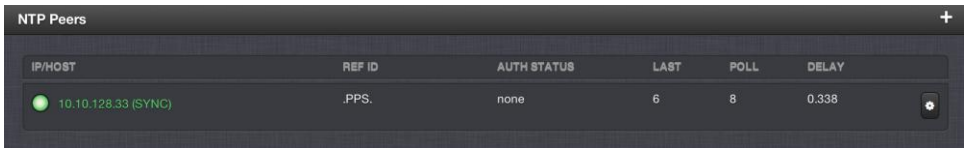
NOTE: Clicking the **Apply** button will apply the settings and will not close the **NTP Peer** window.
Clicking the **Submit** button will close the **NTP Peer** window.
Clicking the **Apply** button allows the user to set up multiple servers without needing to constantly reopen the **NTP Peer** window. Simply enter a new IP address in the Host field, enter the desired settings and click the **Apply** button for each new host. When you are done, click the **Submit** button.

The NTP Peer you have set up will appear in the **NTP Peers** panel.

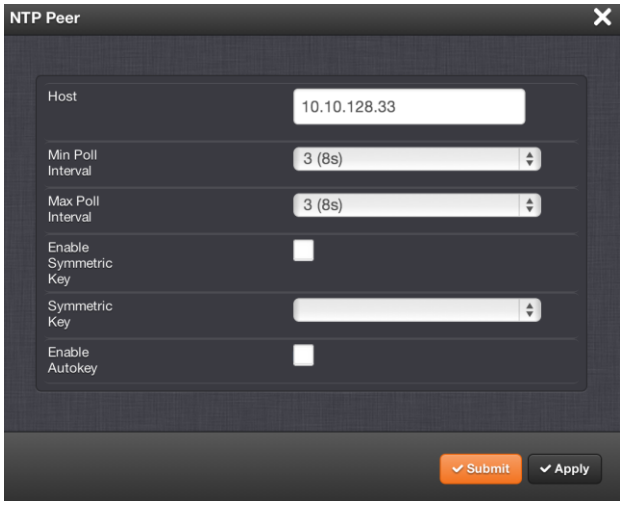


Editing/Deleting NTP Peers

1. Navigate to the **MANAGEMENT NTP Setup** screen.
2. In the **NTP Peers** panel, double click anywhere on the row displaying the information for the NTP server you wish to edit/delete.



3. The **NTP Peer** window will display.



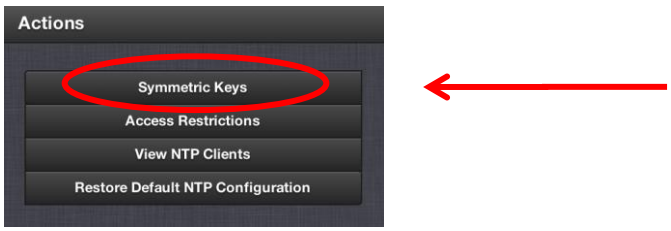
4. Enter the required information in the text fields. See **0 Configuring NTP Servers**.
5. Click the **Submit** or **Apply** button to apply the edited settings.

NOTE: Clicking the **Apply** button will apply the settings and will not close the **NTP Peer** window.
Clicking the **Submit** button will close the **NTP Peer** window.

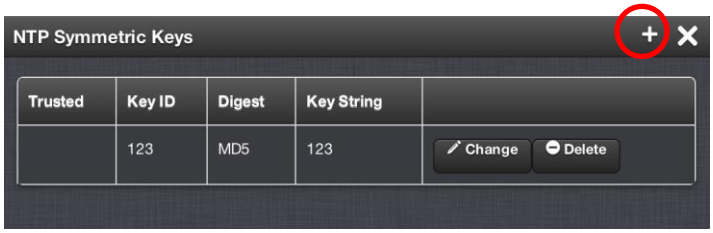
6. To delete a server, click the **Delete** button at the bottom of the window.

Creating Symmetrical Keys (MD5 Authentication)

1. Navigate to the NTP setup screen through the **MANAGEMENT/NETWORK/NTP Setup** menu.
2. In the **Actions** panel, click on the Symmetric Keys button

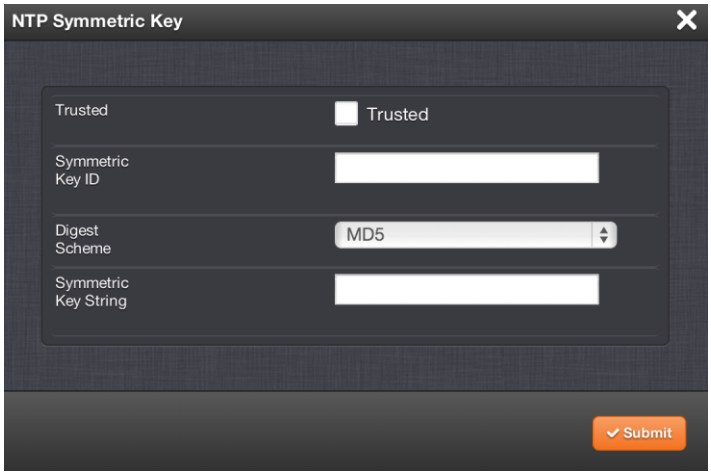


3. The **NTP Symmetric Keys** window will display.



4. To add a Symmetric Key, click on the "+" button.

5. The **NTP Symmetric Key** window will display.

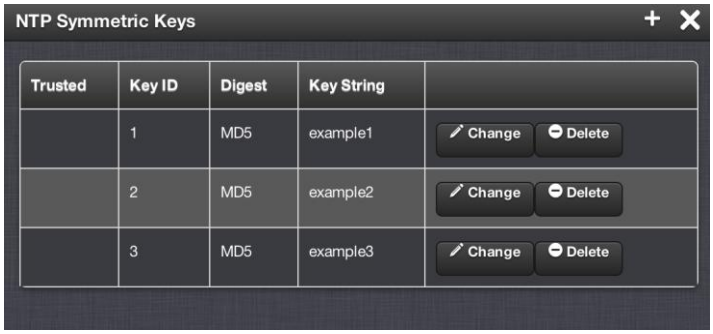


6. Fill in the fields:
    - **Trusted** (checkbox)—Check this box to use MD5 authentication with trusted key ID.

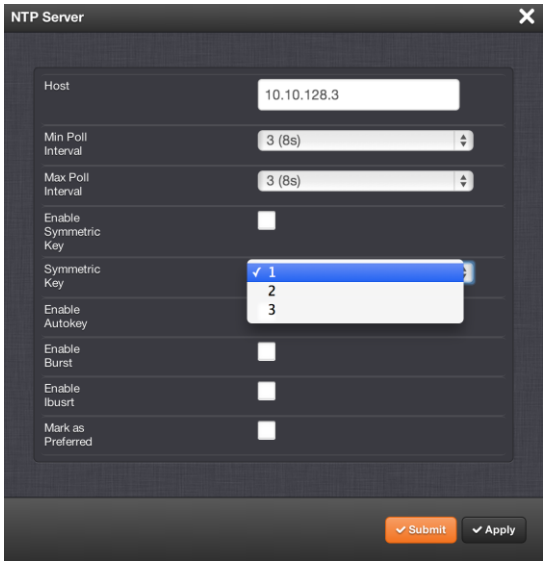
NOTE: To use the MD5 authentication with trusted key ID, both the NTP client and the unit must contain the same key ID/key string pair and the client must be set to use one of these MD5 pairs.

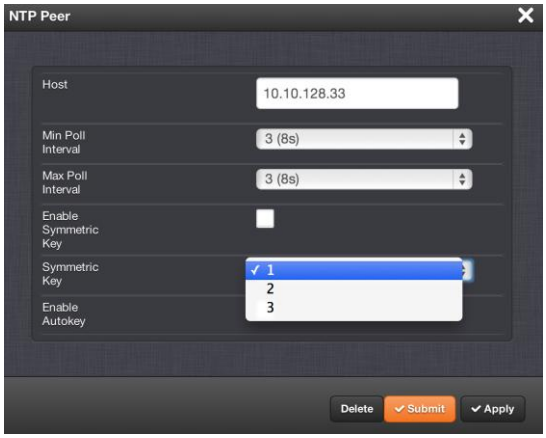
- **Key ID**—The key ID must be a number between 1 and 65532.
- **Digest Scheme**—Choose one of the options from the drop-down list. The available options are:
    - MD5 (the default)
    - SHA1
    - SHA
    - MDC2
    - MDC2
    - RIPEMD160
    - MD4
- **Key Str**—The key string must be readable ASCII and between 1 and 16 characters long.

7. Click the **Submit** button.
8. The key pair you entered will appear in the table in the **NTP Symmetric Keys** window.


NTP Symmetric Keys
Trusted
Key ID
Digest
Key String
1
MD5
example1
Change
Delete
2
MD5
example2
Change
Delete
3
MD5
example3
Change
Delete

9. The key(s) you have set up will now appear as options in the **Key** field in both the **NTP Server** screen and the **NTP Peer** screen.





Duplicate key IDs are not permitted. NTP requests received by unit 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. An NTP request with valid authenticators results in a valid NTP response with its own valid authenticator using the same Key ID provided in the NTP request.

The user may define the trusted symmetrical keys that must be entered on both the unit and any network client with which the unit 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.

NOTE: In order for NTP configuration changes to take effect, NTP should be disabled and then enabled after any configurations changes have been made. NTP can be enabled and disabled through the NTP Services panel on the **MANAGEMENT/NETWORK/NTP Setup** page. See **0 Enabling and Disabling NTP**. Changes made will take effect and NTP operation will be restored shortly after this operation is performed.

Editing/Deleting Symmetrical Keys

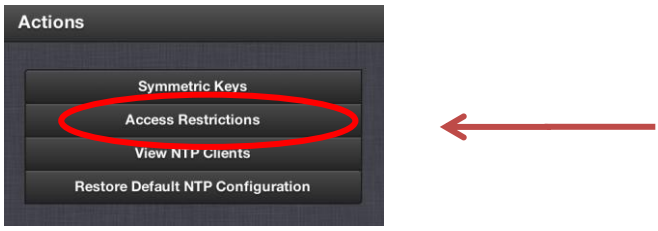
1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **Actions** panel, click on the Symmetric Keys button.
3. In the **NTP Symmetric Keys** window locate the key pairing you would like to edit or deleted.
4. To edit a key pair, click on the Change button in the right-hand column and edit the fields as desired in the NTP Symmetric Key window.
5. Click the **Submit** button.

NOTE: Clicking the **Apply** button will apply the settings and will not close the **NTP Symmetric Key** window.
Clicking the **Submit** button will close the **NTP Symmetric Key** window.

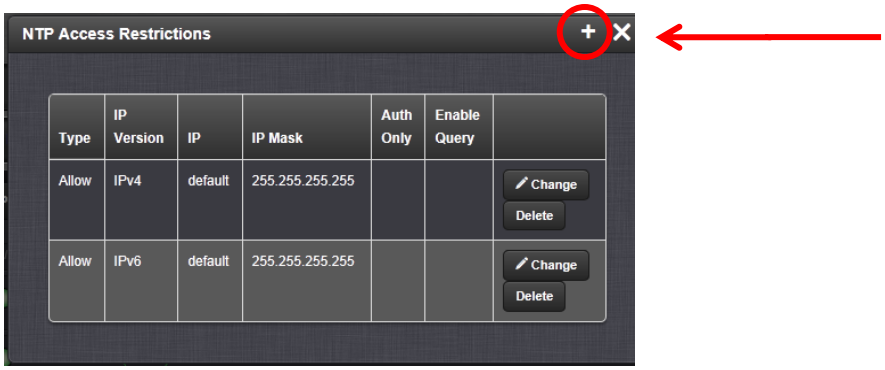
6. Do delete a key pair, click on the Delete button in the right-hand column.
7. Click **OK** in the dialogue box that displays.

Adding NTP Access Restrictions

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **Actions** panel, click on the **Access Restrictions** button.



3. The **NTP Access Restrictions** status window will display.



4. To add a Symmetric Key, click on the "+" button.

5. The **NTP Access Restrictions** edit window will display.

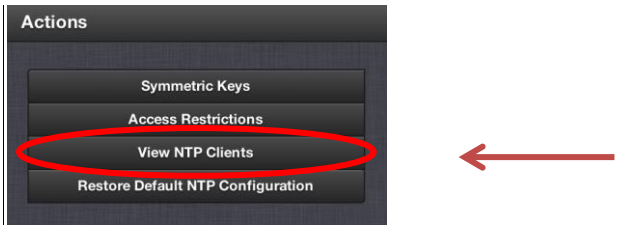
6. Fill in the fields:
   - **Restriction Type**—Choose either Allow or Deny.

   If you select “Deny”, the configured portion of the network will not have NTP access to the unit, but the rest of the network will have access to it. If you select “allow”, the configured portion of the network will have NTP access to unit, but the rest of the network will not have access to it.
   - **IP Version**—Choose IPv4 or IPv6
   - **IP Address**—Enter the appropriate hostname.
   - **Subnet Mask**—Enter the appropriate IP mask.
   - **Require Authentication** (checkbox)—Check this box if you want the additional security of authorized access. The unit is to accept only authenticated requests (MD5 or Autokey) from this user or network segment.
   - **Allow NTP Queries** (checkbox)—Check this box if you would like to allow NTPDC or NTPQ client access. NTPDC and NTPQ are utilities for controlling NTP servers and gathering performance data from NTP servers. Modification or control of the unit’s NTP service through NTPDC or NTPQ is not supported.
7. Click the **Submit** button.

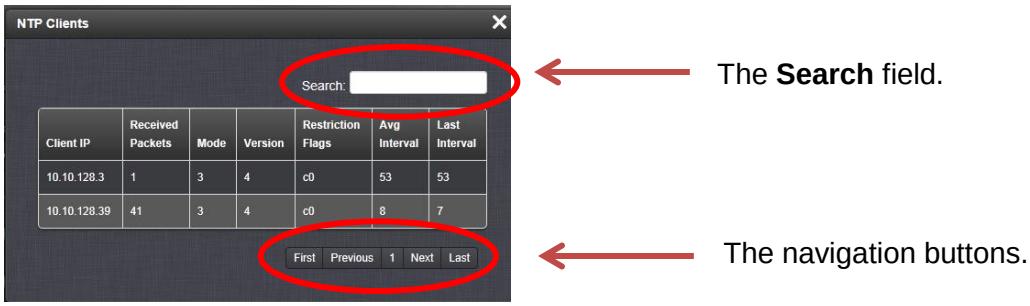
Viewing NTP Clients

To view the NTP clients being served by unit:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Actions** panel click on the **View NTP Clients** button.



3. The NTP Clients window will display, showing a table of the clients that are synchronizing to unit via NTP.

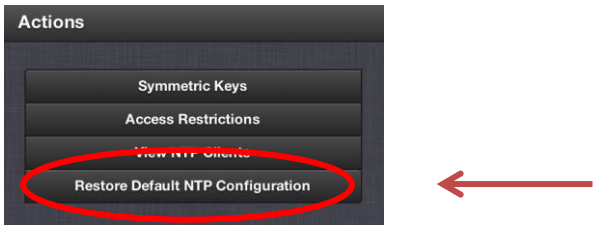


- You can search any of the fields for specific information in the Search field at the top of the window.
- A limit of 10 entries will appear on the screen at any one time. If you have more than 10 clients, you can move through the table using the **First**, **Previous**, **Next** and **Last** navigation buttons at the bottom of the screen.

Restoring the Default NTP Configuration

To restore the unit to its default NTP configuration:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Actions** panel click on the **Restore Default NTP Configuration** button.



3. In the dialogue window that displays, click on the **OK** button.

Enabling and Disabling NTP

After changing any NTP configurations, the NTP daemon needs to be disabled and then enabled for the changes to take effect.

Changes made to NTP configurations will also take effect after the unit is either rebooted or power cycled. To enable or disable NTP:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Services** panel locate the ON/OFF switch.

3. Click **OK** in the dialogue box that displays.

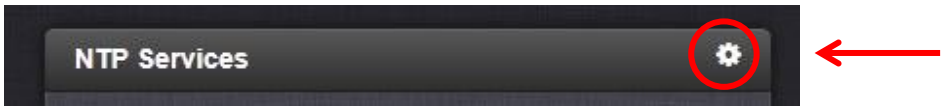
When enabled, the NTP Service operates in Unicast mode. In Unicast mode, the NTP Service responds to NTP requests only. The NTP Service supports a broadcast mode in which it sends a NTP time packet to the network broadcast address.

Enabling/Disabling NTP Broadcasting

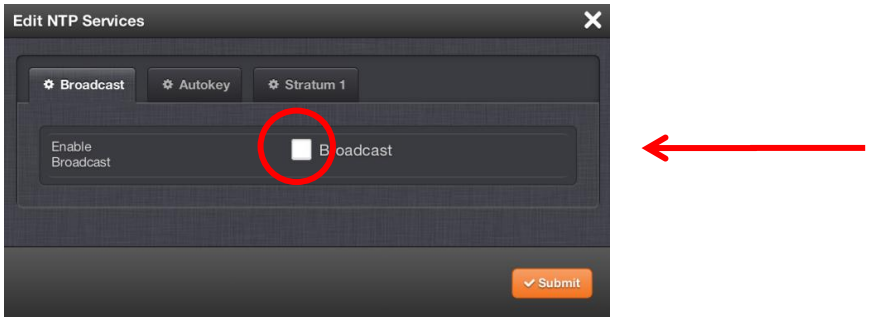
The unit allows NTP service to be configured to broadcast the NTP time to the network's broadcast address at scheduled intervals. To enable NTP broadcasting:

NOTE: The NTP Broadcast mode is intended for one or a few servers and many clients. As most NTP clients do not normally just "listen" for NTP data on the broadcast address (because NTP broadcast isn't as accurate as requesting time), this capability is seldom required and rarely used.

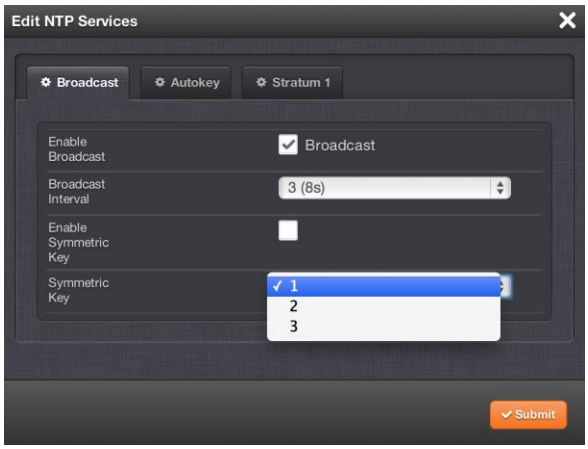
1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. These services are accessed by clicking the  button.



3. The **Edit NTP Services** window will display.



4. Check the **Broadcast** box.



5. Select a Broadcast Interval. When NTP broadcasting is selected, in addition to still responding to NTP time requests sent from network appliances, the unit will also send unsolicited NTP time packets to the local broadcast address at a user-specified interval.
6. To utilize MD5 authentication, select a Symmetric Key (to create symmetric keys, see **0 Symmetrical Keys (MD5 Authentication)**.
7. Click the **Submit** button.
8. To disable NTP broadcasting, click the **Broadcast** box to remove the check and click the **Submit** button.

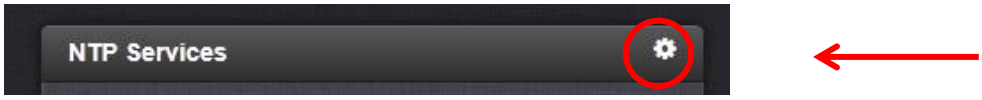
Configuring NTP Autokey

To configure NTP Autokey:

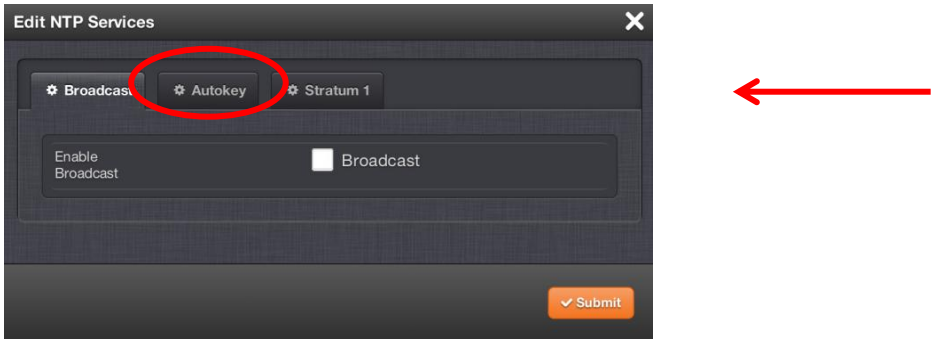
NOTE: Configuration changes made to the unit's NTP configurations do not take effect until the NTP Service is Disabled and then Enabled (or until the unit is rebooted/power cycled). The NTP service can be stopped and started from the **MANAGMENT/NTP Setup** in the **NTP Services** panel.

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.

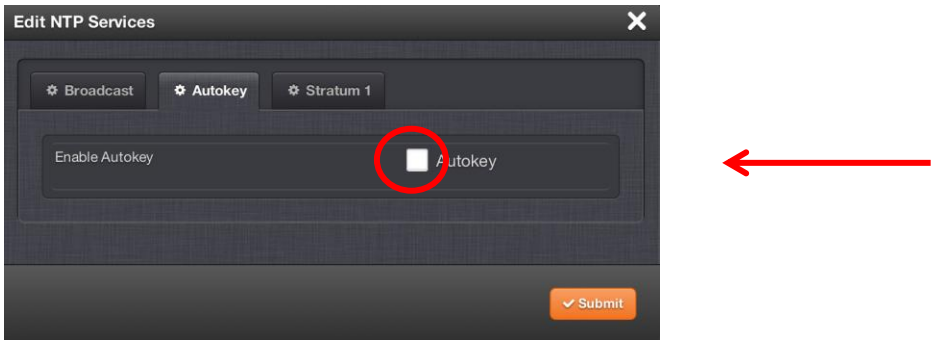
2. Click on the  button.



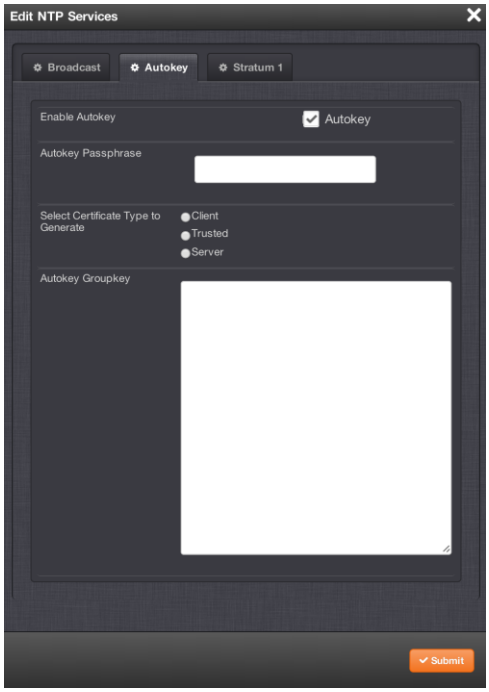
3. The **Edit NTP Services** window will display.
4. Click on the **Autokey** tab.



5. Click on the **Autokey** box.



6. Fill in the **Passphrase** field. The passphrase is your NTP server's password.

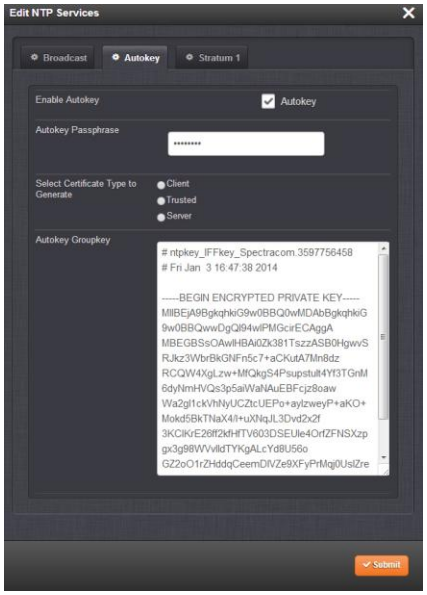


7. Designate whether the server's status as client, trusted or a server by clicking one of the radio buttons.

NOTE: Before a server can be designated Client or Server status, one server must be designated as Trusted. When designating a server as Trusted:

1. Choose the **Trusted** radio button.
2. Click the **Submit** button.

A Groupkey is then generated for the network. This Groupkey will be pasted into the **Groupkey** box to designate another server on the network as Client or Server.



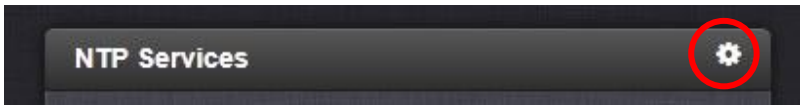
8. To designate a unit as Trusted, click the **Submit** button. This will generate a new Groupkey.
9. To designate a unit as a Client or a Server, paste the generated Groupkey into the **Groupkey** box and click the **Submit** button.

Configuring the Unit's Stratum 1 status.

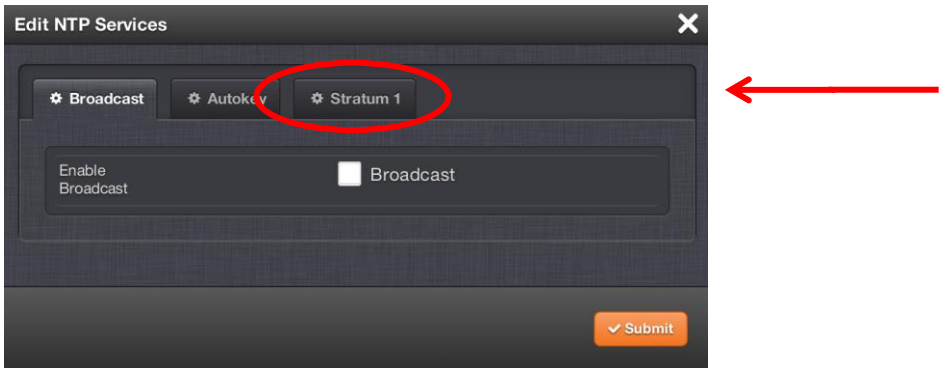
To designate the unit's Stratum 1 status:

NOTE: Configuration changes made to the unit's NTP configurations do not take effect until the NTP Service is Disabled and then Enabled (or until it is rebooted/power cycled). The NTP service can be stopped and started from the **MANAGMENT/NTP Setup** in the **NTP Services** panel.

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. Click on the  button in the **NTP Services** panel.

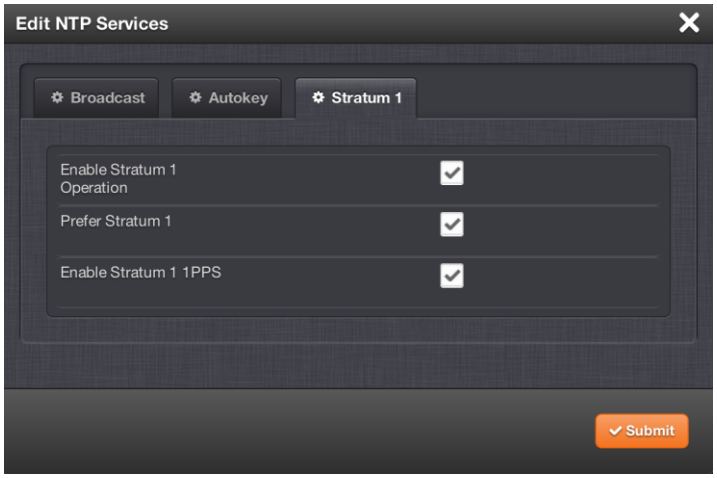


3. The **Edit NTP Services** window will display.
4. Click on the **Stratum 1** tab.



5. Choose among 3 options:
   - Enable Stratum 1 Operation
   - Prefer Stratum 1
   - Enable Stratum 1 1PPS.

   You may choose combination of 1, 2 or three settings. See **0 Timing System Reference Preferred and Enable Timing System 1PPS Reference** for information on timing systems in NTP networks.



6. Click the **Submit** button to confirm your setup.

Configuring an NTP Stratum 1 Server as Trusted Host with IFF Group/Client key.

1. Define the Hostname of all NTP servers before proceeding.
2. Disable NTP.
   Ensure the time is accurate to a few seconds. Use NTP or manually set the clocks to set the system time.
3. Verify this unit is NTP Stratum 1 and is in Time/1PPS Sync.
4. Under the **Autokey** tab of the **Edit NTP Services** window:
   a. **Enable Autokey**—Check the box.
   b. **Autokey Passphrase**—Enter your Group members NTP Autokey password.
   c. **Select Certificate Type to Generate**—Do NOT enable **Client**.
   d. Select **Trusted**.
   e. Click **Submit**.
5. Observe the IFF Group/Client Key appearing.
   a. This is the common IFF Group/Client Key. This key is shared between all Group members using this NTP Servers passphrase for ALL group members.
6. Configure NTP as requiring authentication.
7. Enable NTP in the **NTP Services** panel.
8. Verify NTP reaches occur and NTP eventually reaches Stratum 1.

Creating an NTP Stratum 1 Group Member Server with a Client Key

The steps to configure a NTP Stratum 1 Server which is a Group Member using a Client key are detailed below.

1. Define the Hostname, making sure it is not the same as the trusted root server.
   1. Disable NTP if enabled.
   2. Manually set the time or use NTP to set the system time.
   3. Under the **Autokey** tab of the **Edit NTP Services** window, enable:
      a. **Enable Autokey**—Check the box.
      b. **Autokey Passphrase**—Enter your Group members NTP Autokey password.
      c. **Select Certificate Type to Generate**—Do NOT enable **Client**
   4. Using the NTP Server containing the IFF Group/Common Key generate a Client Key using this NTP Server's passphrase.

5. Cut and paste the Client Key into the **Autokey Groupkey** text box.
6. For all NTP Stratum 2 servers and higher stratum numbers, disable the following items under the **Stratum 1** tab in the **Edit NTP Services** window:
   a. Prefer Stratum 1.
   b. Enable Stratum 1 1PPS.
7. In the **NTP Servers** panel of the main window, add an NTP server and enable the **Autokey** option box. See **0 Configuring NTP Servers**.
8. Enable NTP in the **NTP Services** panel.
9. Wait for NTP to synchronize to the NTP References provided.

Create a NTP Stratum 1 Client Only Server with a Client Key

1. Define the Hostname, making sure that it is different from its trusted group server. See **3.3.5.4 Configuring NTP Servers**.
2. Disable NTP if enabled.
3. Manually set the time or use NTP to set the system time.
4. Under the **Autokey** tab of the **Edit NTP Services** window, enable:
   a. **Enable Autokey**—Check the box.
   b. **Autokey Passphrase**—Enter your Group members NTP Autokey password.
   c. **Select Certificate Type to Generate**—Select **Client** to enable Client only.
5. Using the NTP Server containing the IFF Group/Client Key, copy the Group/Client key.
6. Paste this Group/Client key into the **Autokey Groupkey** text box.
7. For all NTP Stratum 2 servers and higher stratum numbers, under the **Stratum 1** tab in the **Edit NTP Services** window configure the NTP Stratum 1 references:
   a. Disable Enable Stratum 1 Operation.
   b. Disable Enable Stratum 1 1PPS.
8. In the **NTP Servers** panel of the main window, add an NTP server and enable the Autokey option box. See **0 Configuring NTP Servers**.
9. Wait for NTP to synchronize to the NTP References provided.

3.16.2 Working in Expert Mode

The unit also offers an "**Expert Mode**" for NTP configuration. NTP utilizes the "`NTP.conf`" file for its configuration. Normally, configuration of the `NTP.conf` file is indirectly performed by a user via the supplied configuration pages of the web UI. However, it may be desired in certain circumstances to edit this file directly, instead of using the web-based setup screens. When Expert mode is enabled, the user has direct access to the `NTP.conf` file.

Important Note: The Expert Mode should only be used by those individuals that are extremely familiar with NTP operation, including the `NTP.conf` file settings. Incorrectly altering the `NTP.conf` file can cause NTP to stop working (if NTP is configured as an input reference, the unit could lose synchronization).

Important Note: Spectracom Tech Support does not support the editing of the NTP configuration files while in the Expert Mode. For additional information on editing the `NTP.conf` file, please refer to http://www.ntp.org/.

Important Note: If an undesirable change is made to the `NTP.conf` file that affects the NTP operation, the `NTP.conf` file can be manually changed back as long as the previous configuration was known. The `NTP.conf` file can be reset back to the factory default values by either using the procedure to restore all of the factory default settings (see **3.3.5.19 Restoring**

the Default NTP Configuration) or editing the file back to the original configuration as shown in the factory default configuration below.

Important Note: If changes are made to the `NTP.conf` file while in the Expert mode, Expert mode should remain enabled from that point forward. Disabling Expert mode after changes being made to this file may result in loss of this configuration information.

Factory default NTP.conf file:

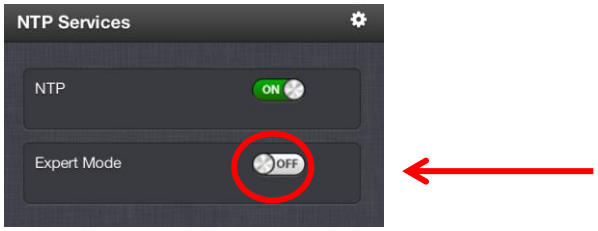
```
restrict 127.0.0.1
restrict ::1
restrict default noquery nomodify
restrict -6 default noquery nomodify
keys /etc/ntp/keys/ntp.keys
controlkey 65533
requestkey 65534
trustedkey 65533 65534
server 127.127.45.0 prefer minpoll 4
server 127.127.22.0 minpoll 4
fudge 127.127.22.0 stratum 0
peer 10.10.128.35 minpoll 3 maxpoll 3 autokey
keysdir /etc/ntp/keys/
crypto pw admin123 randfile /dev/urandom
driftfile /etc/ntp/ntp.drift
logfile /home/spectracom/log/ntp.log
statsdir /home/spectracom/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats  file loopstats  type day enable
filegen peerstats  file peerstats  type day enable
filegen clockstats file clockstats type day enable
```

Prior to Expert mode being enabled, the **Network/NTP Setup** page will contain various tabs for configuring different options of the NTP Service. To prevent inadvertent changes from being made to a user-edited `NTP.conf` file via the web pages, these NTP configuration tabs are removed from the web browser view as long as the Expert mode remains enabled (only the **Expert Mode** tab is visible in Expert Mode; all other tabs will no longer be present). Disabling the Expert mode restores these tabs to the **Edit NTP Services** window.

To enable the Expert Mode to edit the NTP.conf file directly:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.

2. In the **NTP Services** panel locate the **Expert Mode** switch.

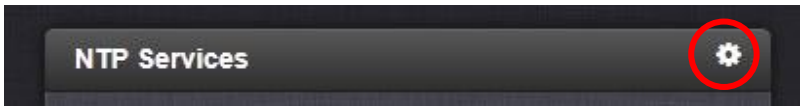


When enabled, the NTP Service operates in Unicast mode. In Unicast mode, the NTP Service responds to NTP requests only. The NTP Service supports a broadcast mode in which it sends a NTP time packet to the network broadcast address.

3. Click on the **Expert Mode** switch.

4. Click **OK** in the dialogue box that displays.

5. .Click on the  button.



6. In the **Edit NTP Services** window, edit the file as desired in the text box under **the Expert Mode** tab.

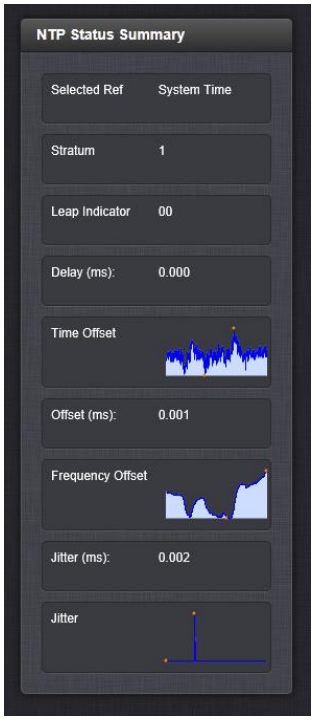
7. Click the **Submit** button to save any changes that were made.

8. First disable and then re-enable the NTP service using the **NTP ON/OFF** switch in the **NTP Services** panel. The unit will now use the new NTP configuration per the manually edited file.

3.16.3 Monitoring System Status Using the NTP Status Summary

A Status summary for monitoring the status of your NTP network is provided.

1. To access the NTP Status Summary, navigate to the Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.



2. The **NTP Status Summary** panel is at the lower left of the screen. The panel contains the following information:

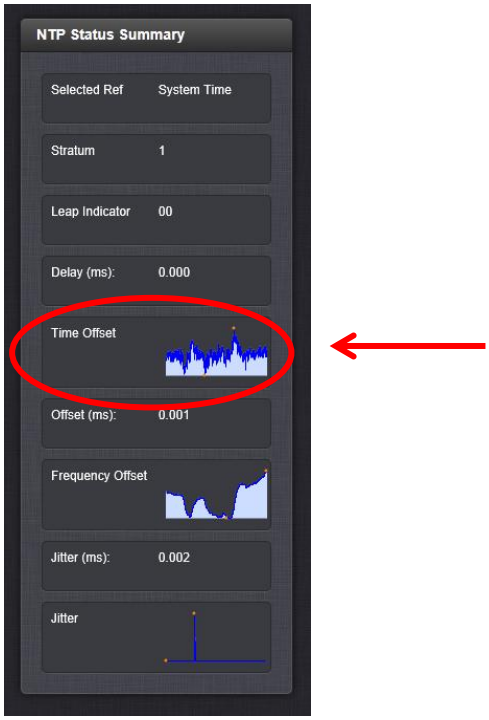
- **Selected Ref**—This is NTP server the unit is using as its selected reference.
- **Stratum**—This is the stratum level at which the unit is operating.
- **Leap Indicator**—The leap indicator bits (usually 00). See **7.1.2 Leap Second Alert Notification.**
- **Delay (ms)—**The measured one-way delay between the unit and its selected reference.
- **Time Offset**—This is a graphical representation of the system time offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See **0 Inspecting the NTP Performance Graph—Time Offset.**
- **Offset (ms)—**Displays the configured 1PPS offset values.
- **Frequency Offset**—This is a graphical representation of the system frequency offset over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel containing a larger, more detailed view of the graph. See **0 Inspecting the NTP Performance Graph—Frequency Offset.**
- **Jitter (ms)—**Variance (in milliseconds) occurring in the reference input time (from one poll to the next).
- **Jitter**—This is a graphical representation of the system jitter over time. Clicking on this graph in the NTP Status Summary panel will open a window in the main panel

containing a larger, more detailed view of the graph. See **0 Inspecting the NTP Performance Graph—Jitter**.

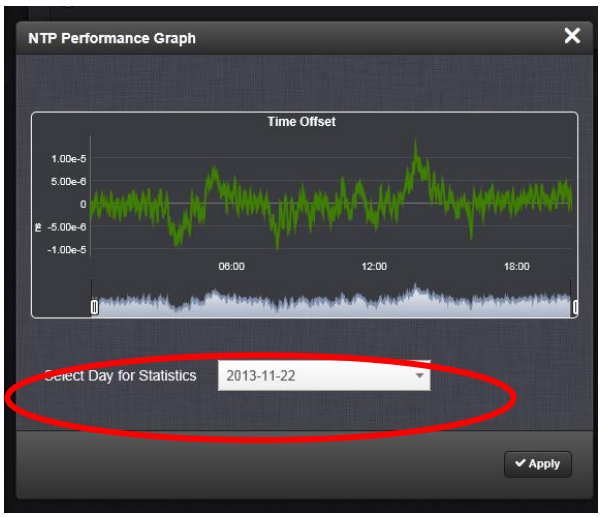
Inspecting the NTP Performance Graph—Time Offset

To view the NTP Performance Graph:

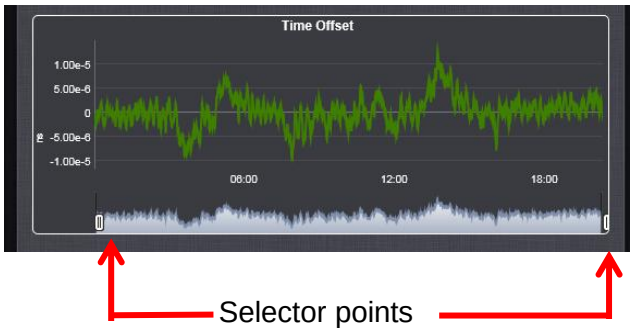
1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Time Offset** graph.



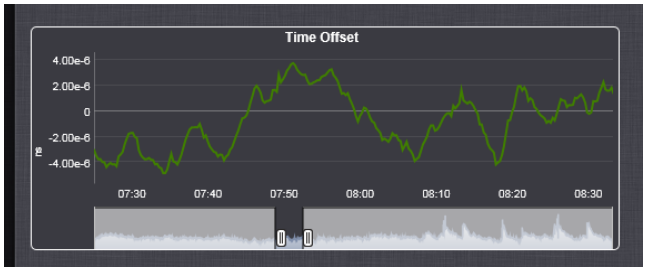
3. Click on the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



5. To select the statistics for a particular day, select a date from the drop-down list in the Select Day for Statistics field. The default date is the present date. Click **Apply**.
6. To see a closer representation of the data, move the selector points in the timeline at the bottom of the graph.



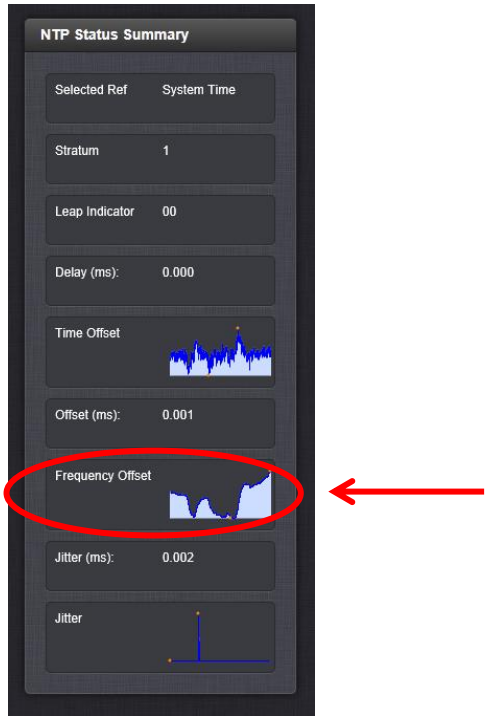
7. A more detailed graph will appear.



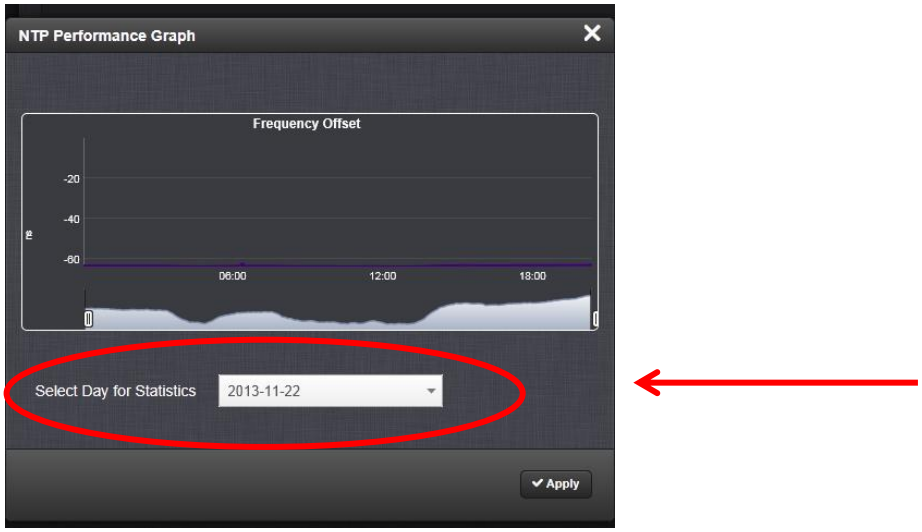
Inspecting the NTP Performance Graph—Frequency Offset

To view the **NTP Performance Graph:**

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Frequency Offset** graph.

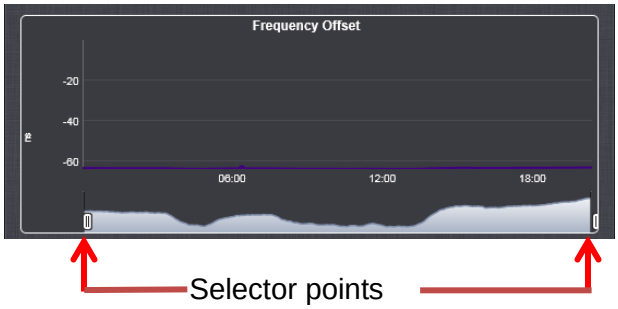


3. Click on the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.

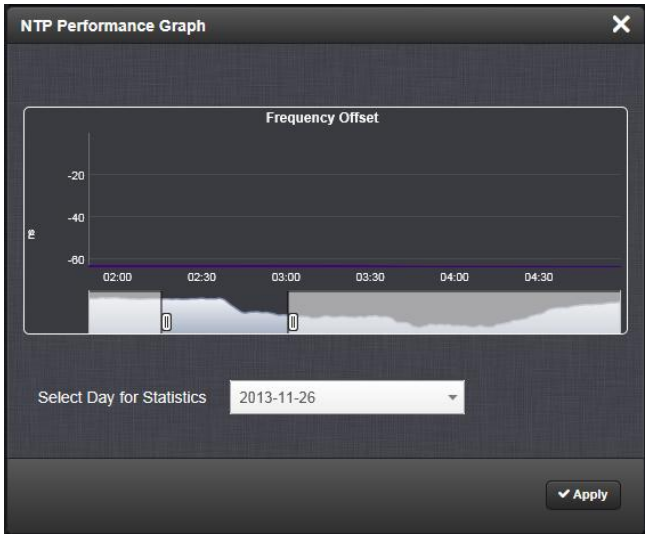


5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field. The default date is the present date. Click the **Apply** button.

6. To see a closer representation of the data, move the selector points in the timeline at the bottom of the graph.



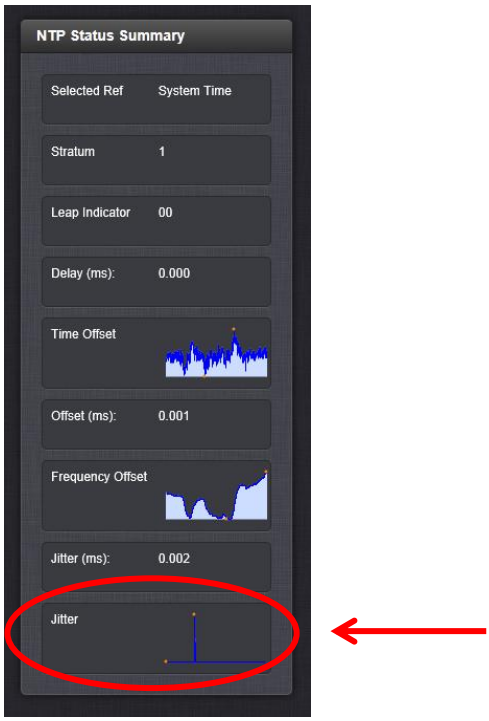
7. A more detailed graph will appear.



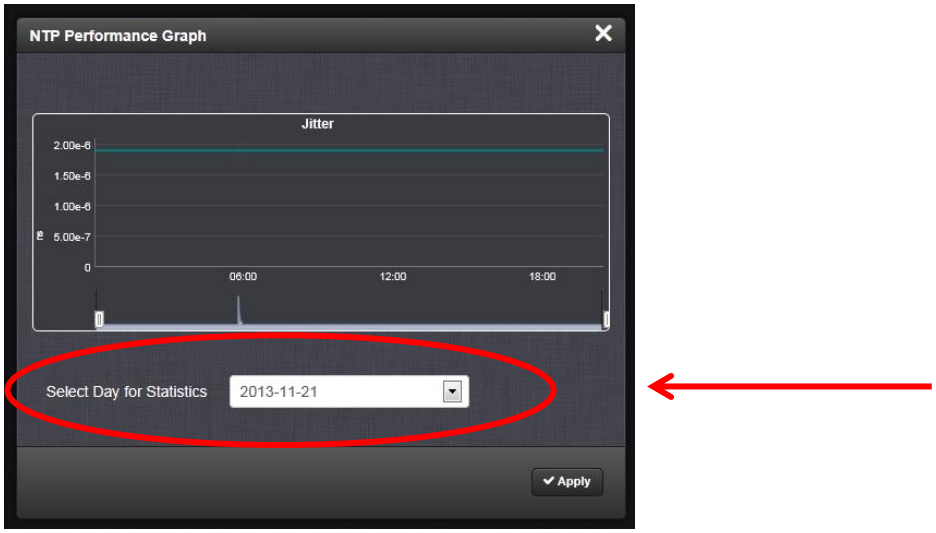
Inspecting the NTP Performance Graph—Jitter

To view the NTP Performance Graph:

1. Navigate to the **MANAGEMENT/NETWORK/NTP Setup** screen.
2. In the **NTP Status Summary** panel locate the **Frequency Offset** graph.

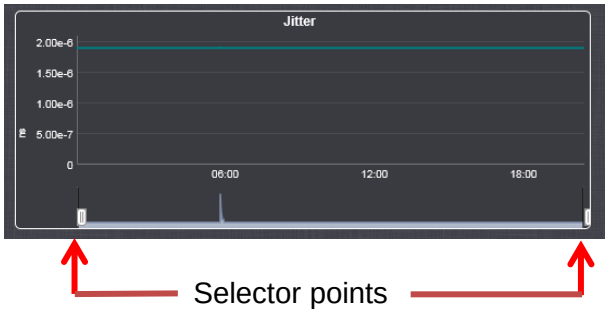


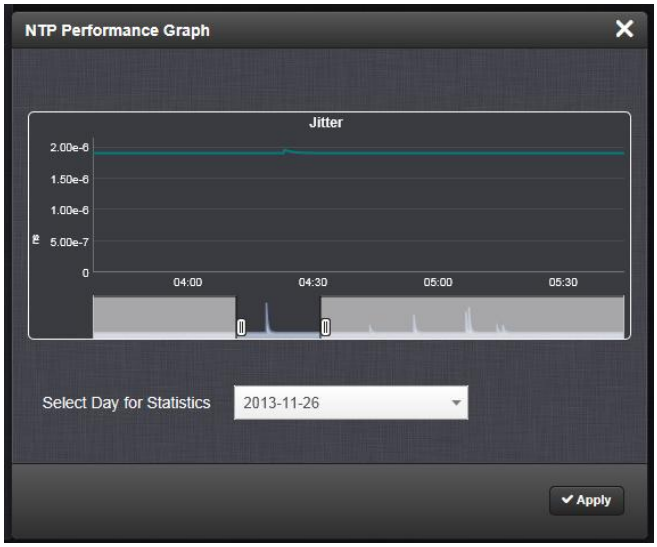
3. Click on the graph in the **NTP Status Summary** panel.
4. The **NTP Performance Graph** panel will appear.



5. To select the statistics for a particular day, select a date from the drop-down list in the **Select Day for Statistics** field. The default date is the present date. Click the **Apply** button.

6. To see a closer representation of the data, move the selector points in the timeline at the bottom of the graph.





3.16.4 NTP Support

Spectracom does not 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 Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2003/2008, and Windows 7 time synchronization. Refer to www.spectracomcorp.com for additional information, or contact Spectracom Technical Support.

Spectracom also offers an alternate Windows NTP client software package called PresenTense. PresenTense software provides many features and capabilities not included with the limited functionality of the Windows W32Time program, including alert notification and audit trails for the PC's time.

For more information on the PresenTense software, please visit www.spectracomcorp.com or contact our Sales department.

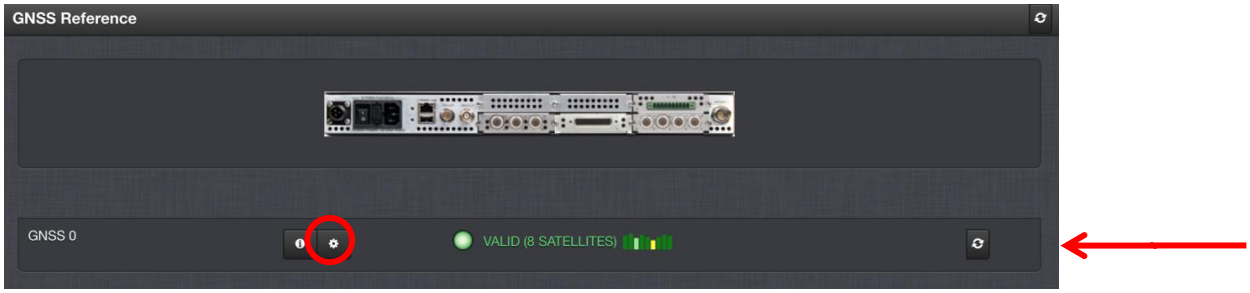
3.17 Configuring GPS/GNSS Input

NOTE: GPS, the Global Positioning System, is just one constellation of Global Navigation Satellite Systems (GNSS). The NetClock may be configured to receive signals from more than one GNSS system. For instance, many receivers can be configured to receive signals from GPS and GLONASS systems for redundancy and signal diversity improving the robustness of the application. This document will use GPS and GNSS interchangeably unless specifically mentioned.

When connected to a GPS antenna, NetClock can use GPS as one of its selected references. The factory default configuration allows GPS satellites to be received / tracked with no additional user intervention required. However, there are a few available user-configured settings for GPS that allow a user to alter the operation of the GPS receiver. These settings include the ability to place the GPS receiver in a mobile mode of operation (by default, NetClock is optimized to operate in a stationary environment), the ability to apply an offset to account for antenna cable delays and other latencies, as well as the ability to erase the stored GPS position information (latitude, longitude and antenna height).

1. Navigate to the GNSS Reference page through **REFERENCES/GNSS** drop-down menu.

2. The **GNSS Reference** page will display.

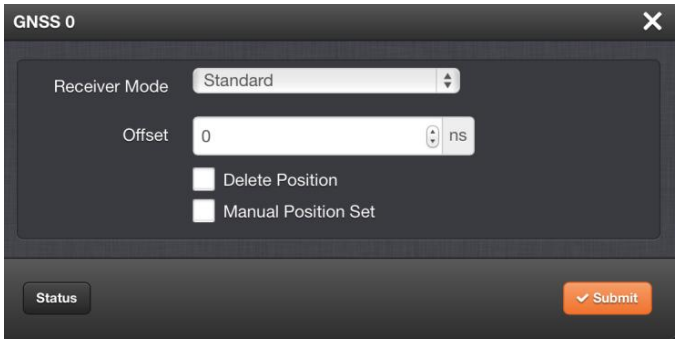


3. Click on the  button for the GNSS Reference you wish to configure.

NOTE: If you choose the individual GNSS Reference directly through the **INTERFACES/REFERENCES** drop-down menu, the GNSS status window will open directly. In this case, click the **EDIT** button at the bottom of the GNSS status window.

NOTE: If you have only one GNSS reference, the unit will number that card 0. Additional references will be numbered 1 or above.

4. The **GNSS 0** edit window will appear.



The **Receiver Mode** option allows the GNSS receiver to operate in either a stationary mode ("Standard" or "Single Satellite" modes) or in a mobile mode environment (such as in an automobile, boat, airplane, etc.).

The available selections are detailed herein:

Standard: This mode should always be selected if the GNSS receiver will remain stationary at all times and will be able to track at last four satellites at all times. In this mode, a GNSS survey, taking about 33 minutes, will initially be performed when at least four GNSS satellites become available. During the GNSS survey, the GNSS receiver must continuously track at least four satellites. Otherwise the GNSS survey will have to start over.

Upon completion of the GNSS survey, the unit will go into Time Sync. Also, the GNSS receiver will lock-in the calculated GNSS position and will enter the "Stationary" mode. Once in Stationary mode, the GNSS survey will only be performed again if the equipment is then relocated to another location (or if the GNSS location is manually cleared by a user). Upon a power cycle, if the equipment has not been relocated, the unit will return to the Stationary mode without the need to perform another GNSS survey.

In this mode, the GNSS receiver will be considered a valid input reference as long as a valid location is entered (either automatically via the GNSS survey or manually entered by a user) and the GNSS receiver continues to track at least four qualified satellites from that point forward.

Mobile: This mode should only be selected if the unit will not remain stationary at all times (instead installed in a building, it is instead installed in a mobile platform; such as a vehicle, ship, plane, etc.). In this mode, the GNSS survey is not performed. the unit will go into synchronization shortly after tracking satellites.

NOTE: With the GNSS Receiver configured in "Continuous" (mobile) mode, the specified accuracies of the unit will be degraded to less than three times that of stationary mode.

Stationary mode accuracy of the receiver is less than 50ns to GPS/UTC (1 sigma), so mobile mode is less than 150ns to GPS/UTC time (1 sigma).

Single Satellite: This mode should only be used if the GNSS receiver will remain stationary at all times and it is impossible for the GNSS receiver to track at least four GNSS satellites for at least 33 minutes continuously (in order to complete the GNSS survey) and the current latitude and longitude is not known. As the GNSS receiver is designed to provide the best timing in the Stationary mode (stationary mode can only be achieved if the GNSS Survey can be completed or the location is manually entered) while tracking at least four satellites, "Single Satellite" mode should only be used if the GNSS survey cannot be completed and the current latitude and longitude are not known (and therefore, can't be manually entered by a user).

In this mode, the GNSS receiver will be considered a valid input reference as long as a valid location is entered (either automatically via the GNSS survey or manually entered by a user) and the GNSS receiver continues to track at least one qualified satellite from that point forward.

The **Offset** option allows a user to enter an offset to the GNSS time and 1PPS reference to account for antenna cable delays or other latencies (entered and displayed in nanoseconds).

By setting the correct **Offset** value (also known as "antenna cable delay"), you can offset the system's on-time point by the Offset value to compensate for the antenna and in-line amplifier delays. Under typical conditions, the expected cable and amplifier delays are negligible. You can calculate the delay based on the manufacture's specifications.

The range of the cable delay is ± 50,000,000 nanoseconds. The default value is 0 nanoseconds and the resolution is 1 nanosecond.

The following formula is used to calculate the cable delay:

D = (L * C)/V

Where:

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

When using LMR-400 or equivalent coax cable (such as the coax cable offered by Spectracom), this formula equates to approximately 1.2 nanoseconds of delay per every foot of cable. To calculate the Offset value (cable delay), multiply the length of the entire cable run by "1.2" and then enter this value into the Offset field.

Examples of LMR-400 (or equivalent) coax cable delays:

100 feet of cable = **120** nanoseconds of cable delay
200 feet of cable = **240** nanoseconds of cable delay
300 feet of cable = **360** nanoseconds of cable delay

The **Delete Position** option allows the user to delete the unit's GNSS position and restart the GNSS Self Survey on command. To ensure that no trace of position data remains on the unit, perform the following steps:

- Disconnect the unit's GNSS antenna.
- Change the **Delete Position** value to "Enabled" (the box is clicked).
- Click the **Submit** button. The unit will initiate a GNSS self-survey.

NOTE: You cannot delete position and restart the GNSS Self Survey when in the "Continue" (mobile) Receiver mode. This option is for use with "Standard" and "1 Satellite" Receiver modes ONLY.

The **Constellation Selection** option allows the user to select which GNSS constellations are used. This setting appears only when the NetClock is equipped with a Multi-GNSS receiver. In addition, the selection of constellations other than GNSS requires the Multi-GNSS option to be installed on the product.

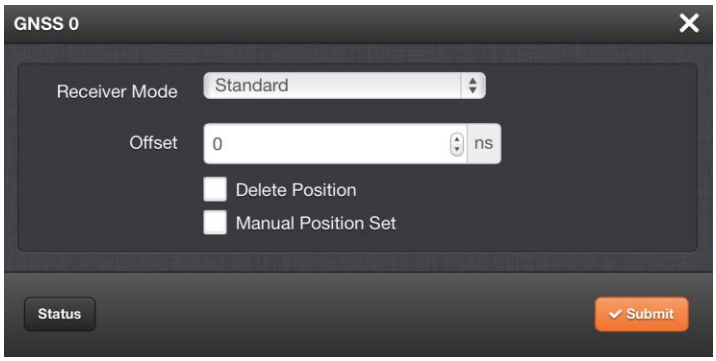
Configuring the GNSS Receiver

To configure the GNSS Receiver:

1. Navigate to the **GNSS 0** window.

NOTE: If you have only one card of any type, the unit will number that card 0. Additional cards will be numbered 1 or above.

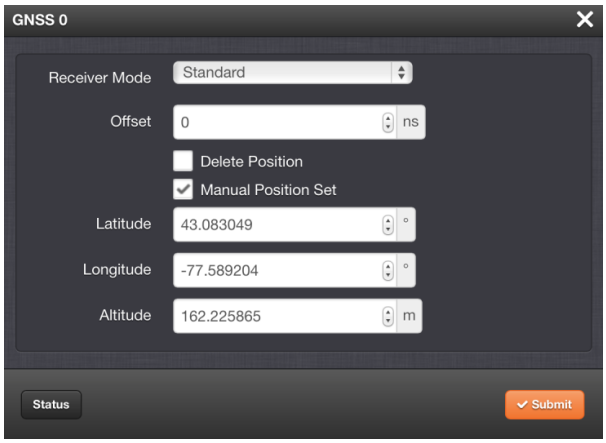
2. The **GNSS 0** edit window will display.



NOTE: If you choose the individual GNSS Reference directly through the **INTERFACES/REFERENCES** drop-down menu, the GNSS status window will open directly. In this case, click the **EDIT** button at the bottom of the GNSS status window.

3. Enter the information in the fields. The available fields are:
   - **Receiver Mode**—This is a drop-down list offering 3 choices:
     - Single Satellite
     - Standard
     - Mobile
   - **Offset**—The default value is 0 nanoseconds and the resolution is 1 nanosecond.

- **Delete Position**—Clicking this box allows the user to delete the unit's GNSS position and restart the GNSS Self Survey on command.
- **Manual Position**—Clicking this box will provide 3 additional fields that will allow the user to manual configure the unit's position by:
    - **Latitude**—In degrees, minutes, seconds.
    - **Longitude**—In degrees, minutes, seconds.
    - **Altitude**—In meters.



Manual Position Setup

The current latitude, longitude and antenna height can be either viewed or manually entered.

While in the Stationary mode of operation, the GNSS Survey is the best method for the GNSS receiver to accurately and automatically calculate the latitude, longitude and antenna height values. If the GNSS survey cannot be completed because less than four GNSS satellites can be received when a fairly accurate location is entered into the GNSS receiver, you can also place the unit into the "Stationary" mode of operation, thereby increasing the accuracy of the GNSS receiver.

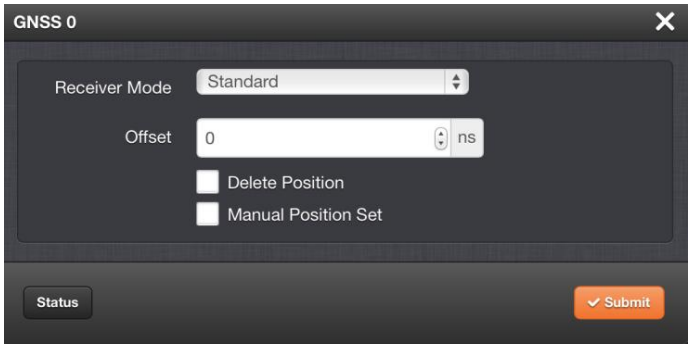
The location input by the user may only help to speed up the time to the first fix during the initial installation. The unit will automatically check the status of the GNSS receiver after receiving the location input from the user. Based on the status of the GNSS receiver, the unit will either tell the user that the GNSS receiver already has finished the first fix and the input was abandoned, or send the location to the GNSS receiver.

To manually enter the unit's position:

1. Navigate to the **GNSS 0** window.

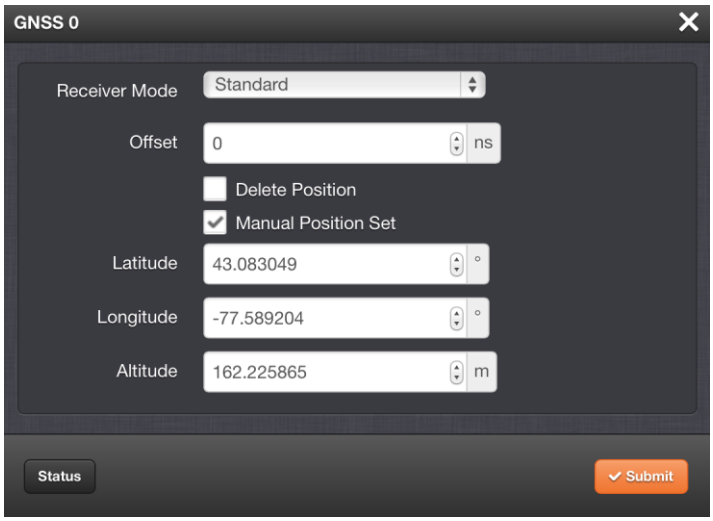
NOTE: If you have only one card of any type, the unit will number that card 0. Additional cards will be numbered 1 or above.

2. The **GNSS 0** edit window will display.



NOTE: If you choose the individual GNSS Reference directly through the **INTERFACES/REFERENCES** drop-down menu, the GNSS status window will open directly. In this case, click the **EDIT** button at the bottom of the GNSS status window.

3. Check the Manual Position Set checkbox. Entry fields for latitude, longitude and altitude are displayed.

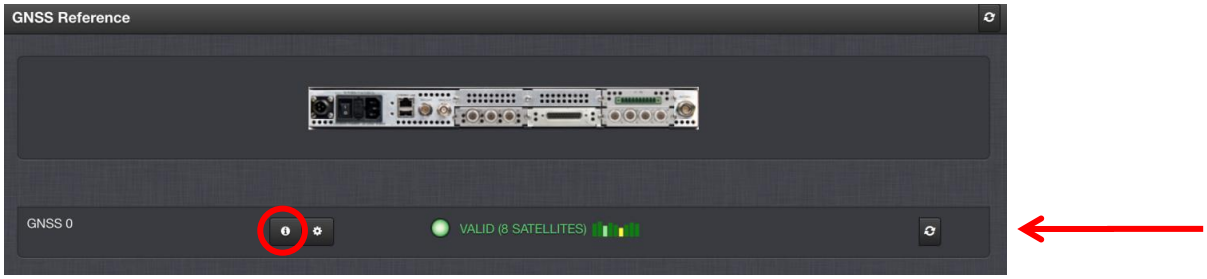


4. In the additional fields displayed, enter:
   - **Latitude**—In degrees, minutes, seconds.
   - **Longitude**—In degrees, minutes, seconds.
   - **Altitude**—In meters.
5. Click the **Submit** button at the bottom of the window.

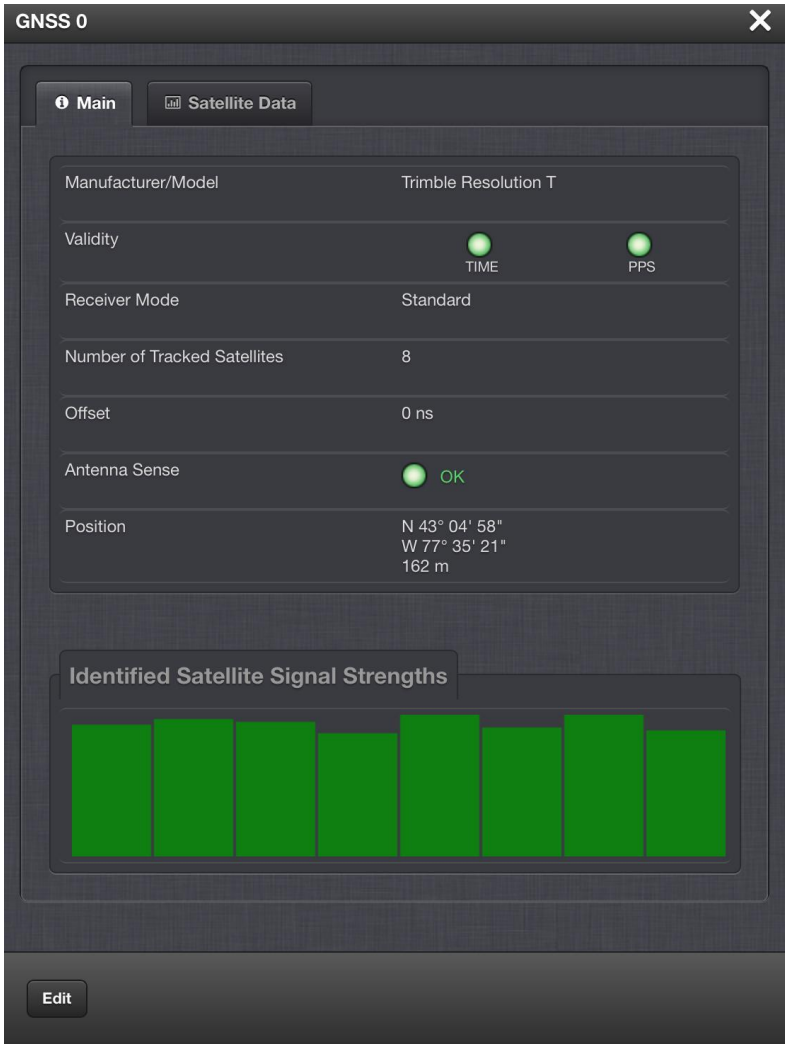
Viewing the Status of the GNSS Reference

To view the status of a GNSS reference:

1. Navigate to the **GNSS Reference** page through **INTERFACES/REFERENCES/GNSS Reference**.



2. Click on the  button for the GNSS Reference.
3. The **GNSS 0** status window will display.

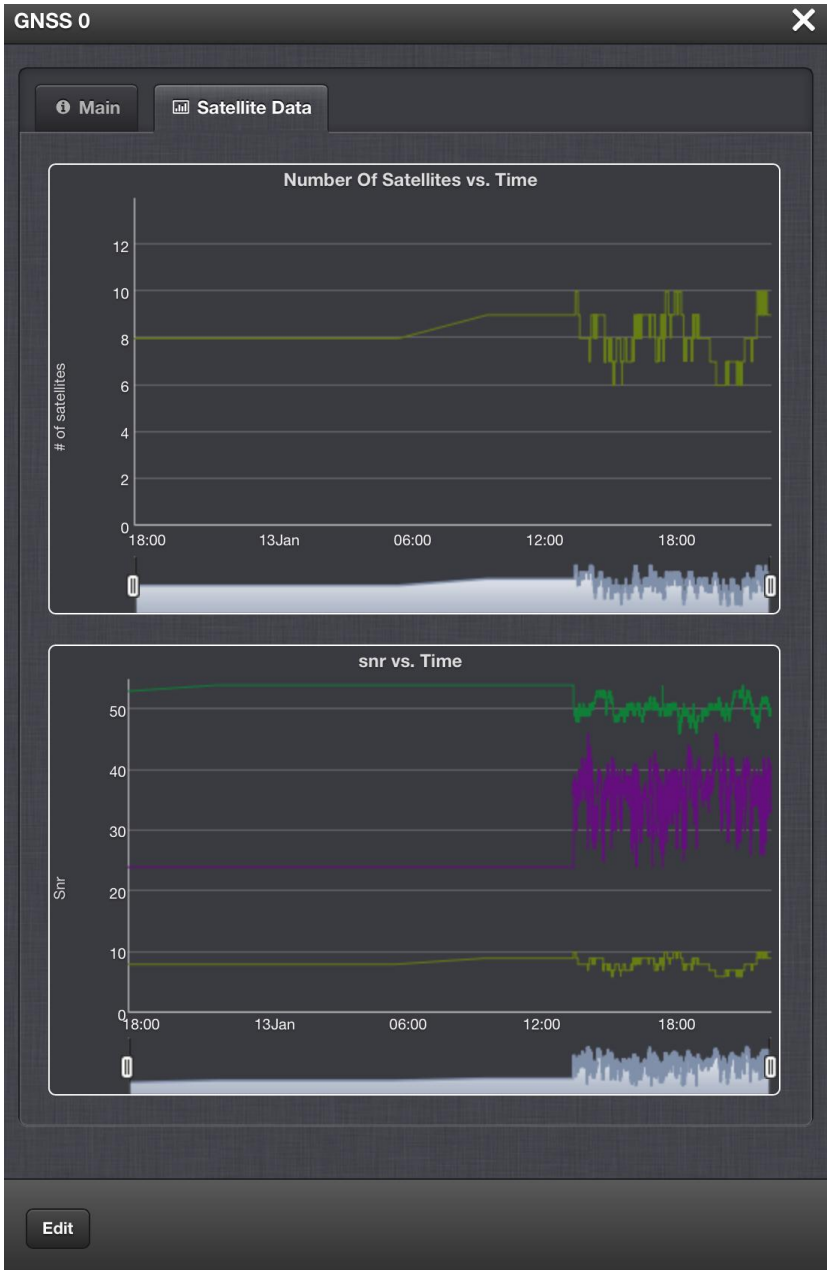


- The GNSS 0 window contains 2 tabs:
  - **Main** (the default)
  - **Satellite Data**
- Under the **Main** tab, the following information will display:
  - **Manufacturer/Model**—The manufacturer and/or model of the GNSS receiver.
  - **Validity**—The two "light" icons will indicate the validity of the available signals:
    - TIME.

        - 1PPS.
        - "On" (green) indicates a valid signal. "Off" indicates no valid signal.
    - **Receiver Mode**—One of:
        - Single Satellite.
        - Standard.
        - Mobile.
    - **Number of Tracked Satellites**—The number of satellites being tracked.
    - **Offset**—As set by the user, in ns.
    - **Antenna Sense**—This will display:
        - "OK" (green).
        - "Open"—Check the antenna for the presence of an open.
        - "Short"—Check the antenna for the presence of a short.
    - **Position**—The position by:
        - Latitude—In degrees, minutes, seconds.
        - Longitude—In degrees, minutes, seconds.
        - Altitude—In meters.
    - **Identified Satellite Signal Strengths**—Shows in bar graph form the strength of the signal from each tracked satellite. Each bar represents one satellite.

Under the **Satellite Data** table are two graphs:

- **Number of Satellites vs. Time**—A graphical track of how many satellites were being tracked over time.
- **snr vs. Time**—A graphical track of the maximum snr, the minimum snr and the number of satellites being tracked over time.



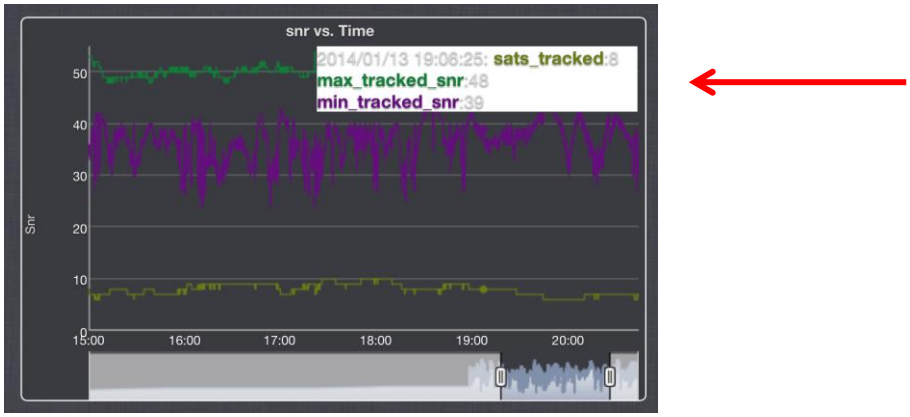
Satellites being tracked

Max snr

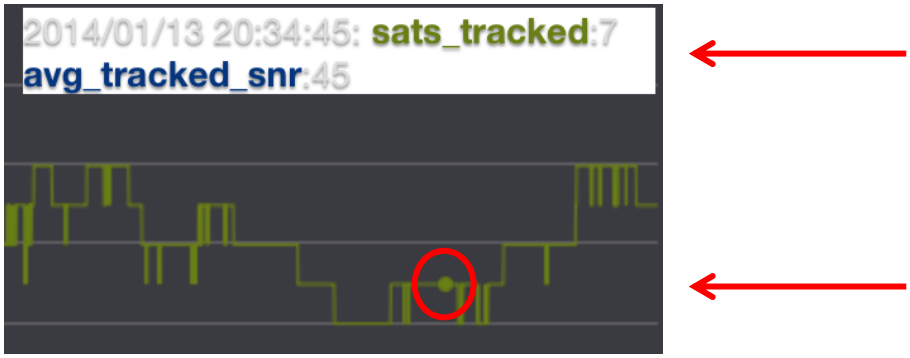
Min snr

Satellites being tracked

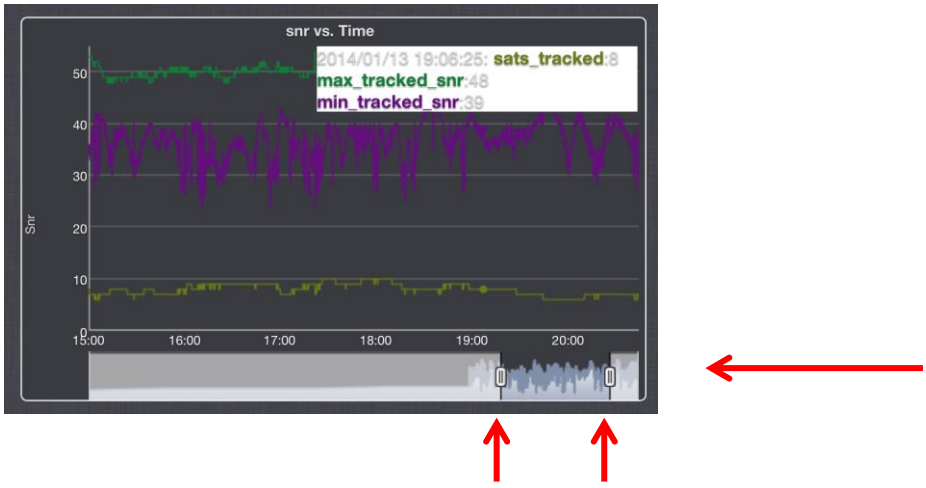
- In both graphs, to see a legend of the graphical data, click inside the graph. A pop-up window will display the legend for that graph.



a. In both graphs, to see the status of the data at any one time, click on the line on the graph at that time, and a pop-up legend will display the status of the antenna reference at that time.



b. In both graphs, to see a particular timeframe in more detail, move the sliders at the bottom of the graph to focus on the desired time frame.



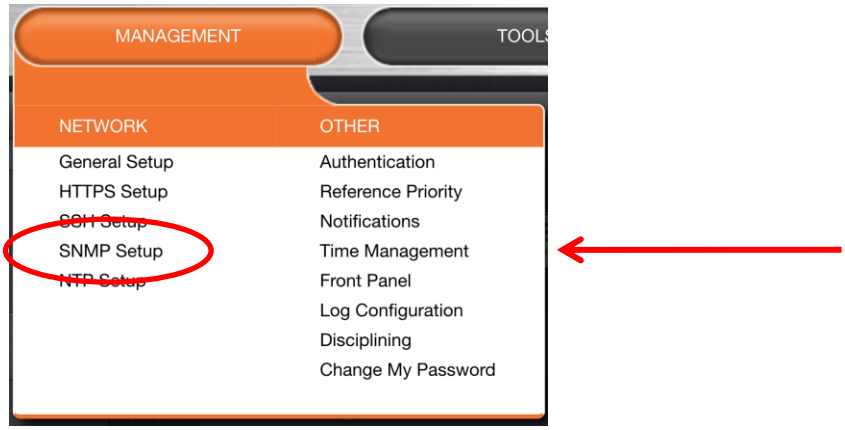
3.18 Configuring SNMP and Notifications

3.18.1 Configuring SNMP and Notifications

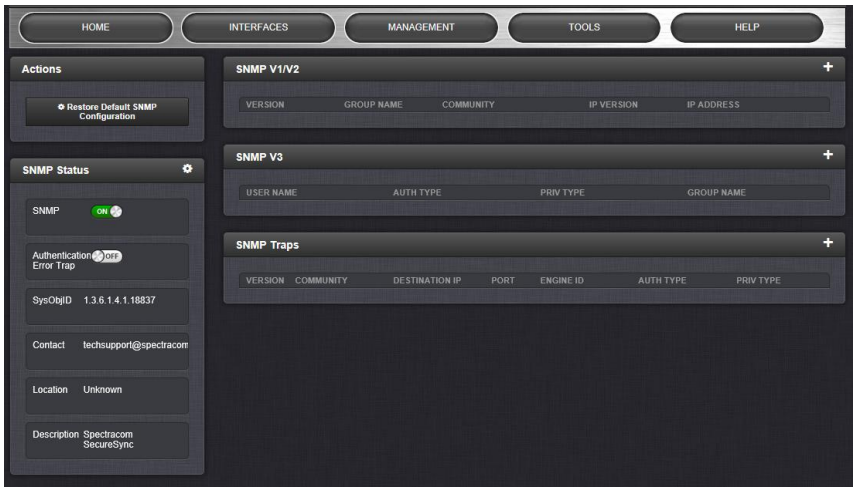
Accessing the SNMP Setup Screen

To access the **SNMP Setup** screen:

1. Choose **MANAGEMENT/NETWORK/SNMP Setup**.

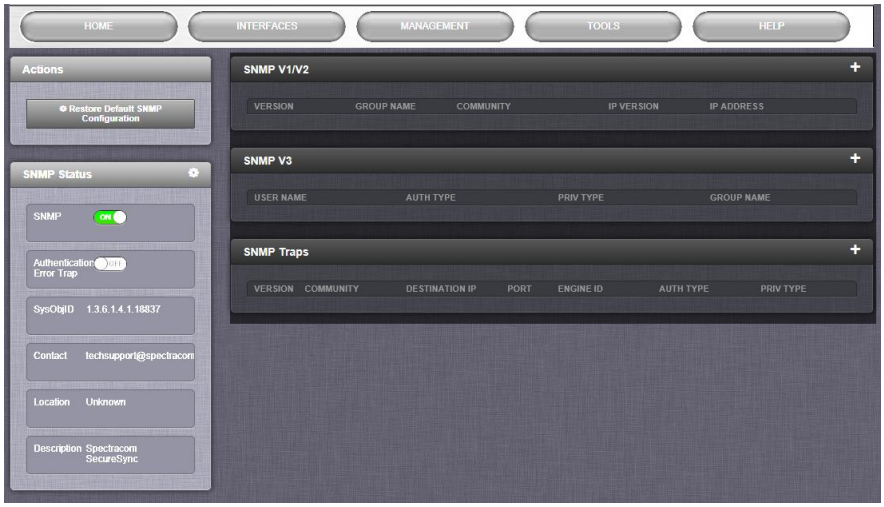


2. The **SNMP** screen will display.



The SNMP screen is divided into 3 Panels:

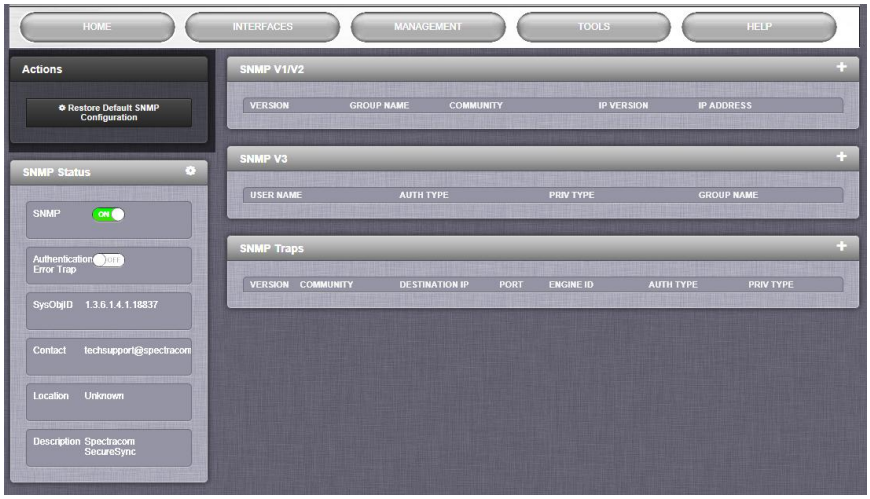
The main panel



The main panel is subdivided into 3 displays:

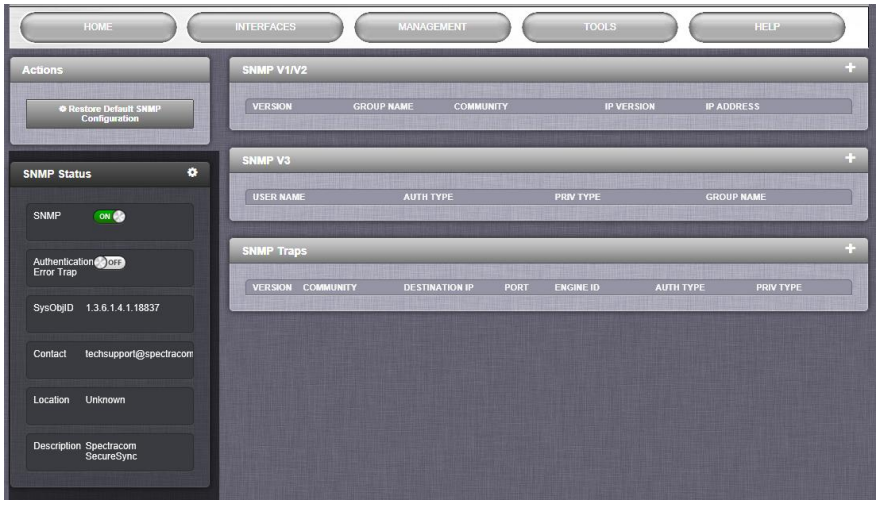
a. **SNMP V1/V2—** This panel allows configuration of SNMP v1 and v2c communities (used to restrict or allow access to SNMP). This tab allows the configurations for SNMP v1 and v2c, including the protocols allowed, permissions and Community names as well as the ability to permit or deny access to portions of the network.
   Clicking on the "+" symbol in the top-right corner opens the SNMP V1/V2c Settings for Access Screen. See **0 Configuring SNMP V1/V2 Communities**.
b. **SNMP V3—** This panel allows configuration of SNMP v3 functionality, including the user name, read/write permissions, authorization passwords as well as privilege Types and Passphrases.
   Clicking on the "+" symbol in the top-right corner opens the SNMP V3 Screen. See **0 Configuring SNMP V3 Users**.
c. **SNMP Traps—**This panel allows the ability to define up to five different SNMP Managers that SNMP traps can be sent to over the network. This allows for SNMP Managers in different geographical areas to receive the same SNMP traps and Managers in other areas also receive.
   Clicking on the "+" symbol in the top-right corner opens the SNMP Traps Settings Screen. See **0 Defining SNMP Traps (Notifications)**.

The **Actions** panel



The **Actions** panel contains the **Restore Default SNMP Configuration** button.

The **SNMP Status** panel



The **SNMP Status** panel provides:

- An **SNMP** ON/OFF switch.

d. An **Authentication Error Trap** ON/OFF switch.

e. **SysObjID**—The System Object ID number. This is editable in the **SNMP Status** panel (see **0 Configuring the SNMP System Object ID**).

f. **Contact Information**—The email to contact for service. This is editable in the **SNMP Status** panel (see **0 Configuring SNMP System Contact Information**).

g. **Location**—The system location. This is editable in the **SNMP Status** panel (see **0 Configuring SNMP System Location**).

h. **Description**—A simple product description. This is not editable in the **SNMP Status**.

NetClock and SNMP

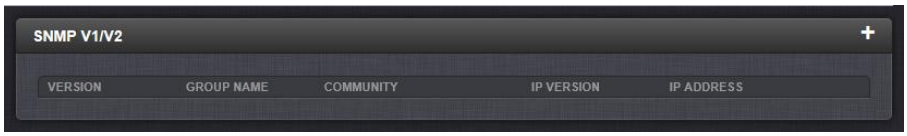
SNMP (Simple Network Management Protocol) is a set of standards for managing network devices, which includes a protocol, a database structure specification, and a set of data objects. The communication protocol involves one or more network management stations monitoring one or more network devices. SNMP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

NetClock's SNMP functionality supports SNMP versions V1, V2c and v3 (with SNMP version 3 being a secure SNMP protocol).

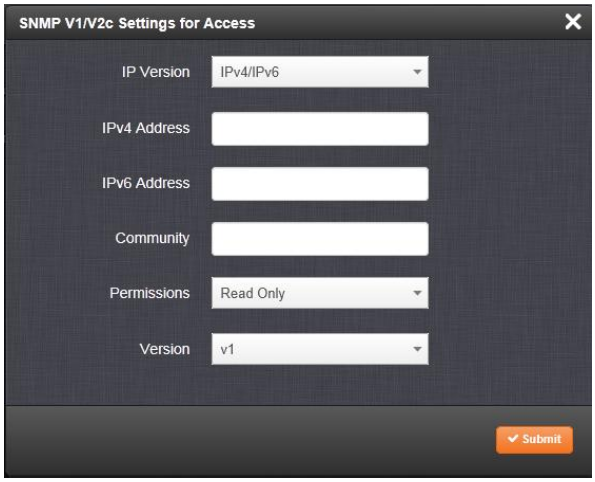
Configuring SNMP V1/V2 Communities

Creating Communities

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **SNMP V1/V2** panel click on the "+" button.



3. The **SNMP V1/V2c Settings for Access** window will display.



4. Enter the required information in the fields provided
    - The IP Version field provides a choice of IPv4, IPV6 or both IBv4 and IPv6 (the default).
    - The choices offered below will change in context with the choice made in the IP Version field.
    - If no value is entered in the IPv4 and/or IPv6 field, the unit uses the system default address.

- SNMP community names should be between 4 and 32 characters in length.
- Permissions may be Read Only or Read/Write
- The version field provides a choice of V1 or V2c.

5. Click the **Submit** button at the bottom of the window.

NOTE: You can exit the window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the window before you have clicked the **Submit** button, any information you entered will not be retained.

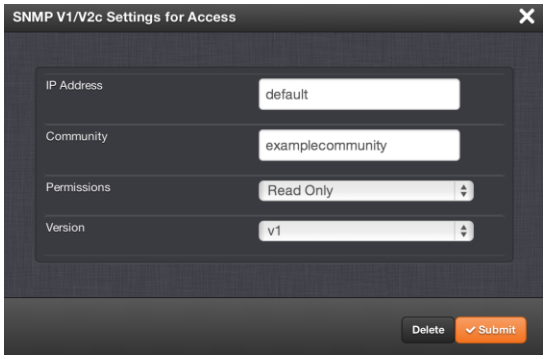
6. The created communities will appear in the SNMP V1/V2 panel.

Editing and Deleting Communities

To edit or delete a community you have created:

1. Click on the row of the **SNMP V1/V2** panel that displays the community you wish to edit or delete. The cursor will change from an arrow icon to a pointing finger to indicate that the entry is clickable.
2. The **SNMP V1/V2c Settings for Access** window will display.

NOTE: The options available for editing in the **SNMP V1/V2c Settings for Access** window will vary contextually according to the information in the entry chosen.

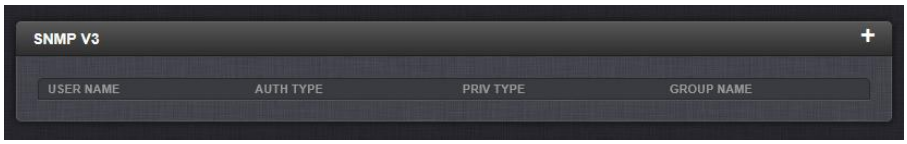


3. To edit the settings, enter the new details you want to edit and click the **Submit** button.
OR
To delete the entry, click on the **Delete** button.

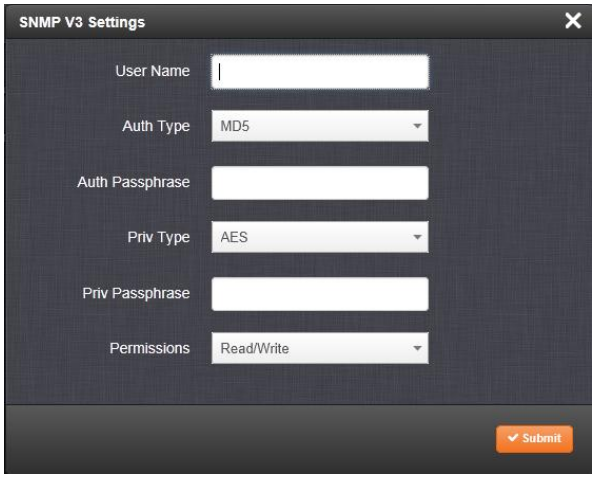
Configuring SNMP V3 Users

Creating Users

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **SNMP V3** panel click on the "+" button.



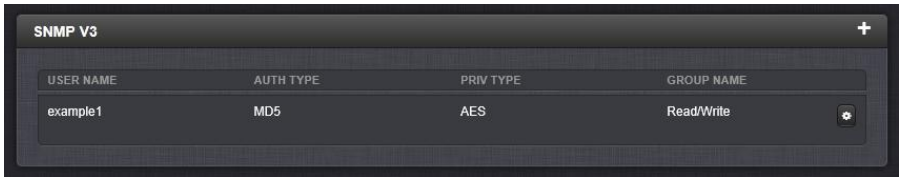
3. The **SNMP V3 Settings** window will display.



4. Enter the required information in the fields provided.
   - SNMP user names and passwords are independent of users that are configured on the **Tools/Users** page.
   - User names are arbitrary. SNMP user names should be between 4 and 32 characters in length.
   - The user name must be the same on the unit and on the management station.
   - The **Auth Type** field provides a choice between MD5 and SHA.
   - The **Auth Password** must be between 8 and 32 characters in length.
   - The **Priv Type** field provides a choice between AES and DES.
   - The **Priv Passphrase** must be between 8 and 32 characters in length.
   - The **Permissions** field provides a choice between Read/Write and Read Only.
5. Click the **Submit** button at the bottom of the window.

NOTE: You can exit the window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the window before you have hit the **Submit** button, any information you entered will not be retained.

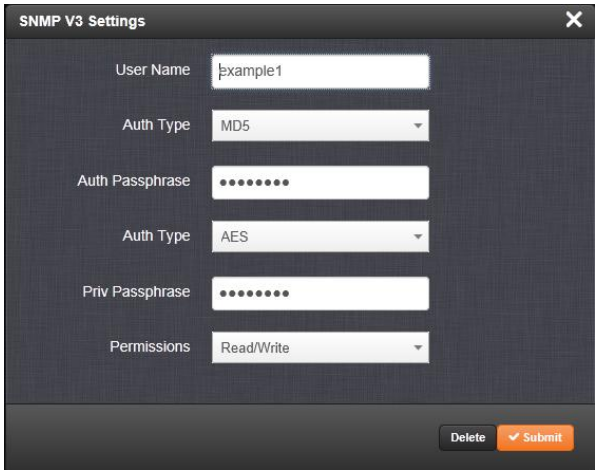
6. The created user will appear in the **SNMP V3** panel.



Editing and Deleting Users

To edit or delete a user you have created:

1. Click on the row of the **SNMP V3** panel that displays the community you wish to edit or delete. The cursor will change from an arrow icon to a pointing finger to indicate that the entry is clickable.
2. The **SNMP V3 Settings** screen will display.

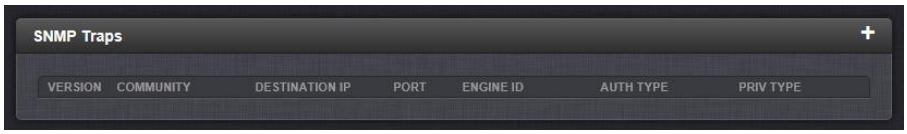


3. To edit the settings, enter the new details you want to edit and click the **Submit** button.
   OR
   To delete the entry, click on the **Delete** button.

NOTE: You can exit the window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the window before you have hit the **Submit** button, any information you entered will not be retained.

Defining SNMP Traps (Notifications)

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the **SNMP Traps** panel click on the "+" button.



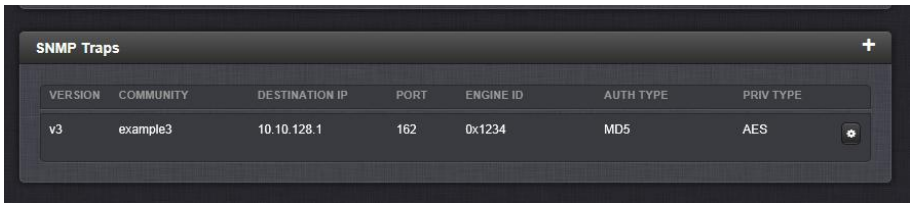
3. The **SNMP Traps Settings** window will display.

4. Enter the required information in the fields provided.
    - The **Version** field provides a choice between v1, v2c and v3 (the default)

NOTE: The options available for editing in the **SNMP Traps Settings** window will vary contextually according to the user's choice in the **Version** field.

- SNMP user names should be between 4 and 32 characters in length.
- **Destination IP Version** is a choice between IPv4 and IPv6.
- **Destination IP** is destination address for the notification to be sent.
- The default **Port** is 162**.**
- **Engine Id** must be a hexadecimal number (such as 0x1234).
- **Auth Type** provides a choice between MD5 (the default) and SHA.
- The **Auth Password** must be between 8 and 32 characters in length.
- The **Priv Type** field provides a choice between AES and DES.
- The **Priv Passphrase** must be between 8 and 32 characters in length.

5. Click the **Submit** button at the bottom of the window.
6. The SNMP trap you create will appear in the SNMP Traps Panel.



NOTE: You can exit the **SNMP Traps Settings for Access** window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **SNMP Traps Settings for Access** window before you have hit the **Submit** button, any information you entered will not be retained.

Each row of the **SNMP Traps** panel includes the version of the SNMP functionality, the User/Community name for the trap, the IP address/Hostname of the SNMP Manager and values applicable only to SNMP v3, which include the Engine ID, the Authorization Type, the Privilege Type.

You may define up to five different SNMP Managers to whom SNMP traps can be sent over the network. This allows for SNMP Managers in different geographical areas to receive the same SNMP traps.

NOTE: Spectracom has been assigned the enterprise identifier 18837 by the IANA (Internet Assigned Numbers Authority). Spectracom's product MIBs reside under the enterprise identifier @18837.3.

For detailed descriptions of the objects and traps supported by the unit, please refer to the Spectracom MIB files.

About SNMP Traps:

NetClock can provide SNMP traps when events occur to provide remote indications of status changes. SNMP Traps are one way to remotely monitor NetClock status.

The SNMP traps indicate the status change that caused the trap to be sent and may also include one or more objects, referred to as variable-bindings, or "varbinds." A varbind provides a current NetClock data object that is related to the specific trap that was sent. For example, when a Holdover trap is sent because the NetClock either entered or exited the Holdover mode, the trap varbind will indicate that the NetClock is either currently in Holdover mode or not currently in Holdover mode.

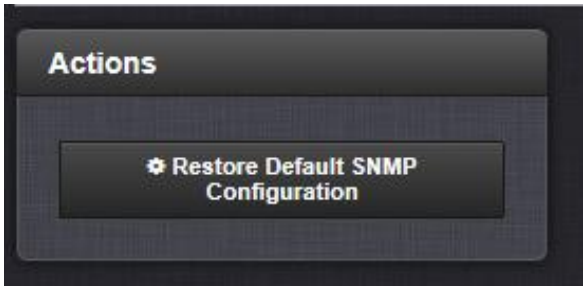
For testing purposes, a command line interface command is provided. This command, **`testevent`**, allows one, several, or all of the traps defined in the MIB to be generated.

Restoring the Default SNMP Configuration

To restore the unit to its default SNMP configuration:

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.

2. In the **Actions** panel, click the **Restore Default SNMP Configuration** button.

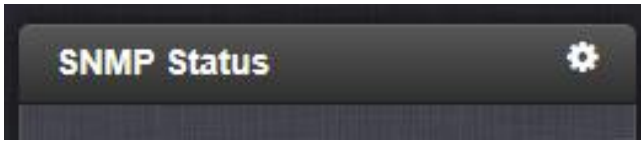


3. Confirm in that you want to restore the default settings in the pop-up message.

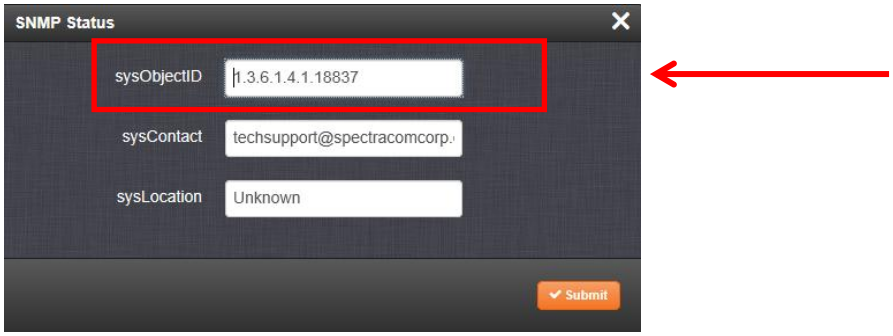
Configuring the SNMP System Object ID

To configure the SNMP System Object ID:

1. Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.
2. In the panel click on the  button.



The **SNMP Status** pop-up window will display.



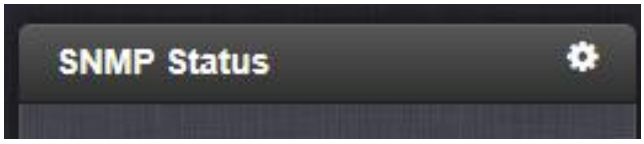
3. In the **sysObjectID** field, enter the SNMP system object ID.
4. Click the **Submit** button at the bottom of the window.

NOTE: You can exit the **SNMP Status** Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **SNMP Status** window before you have hit the **Submit** button, any information you entered will not be retained.

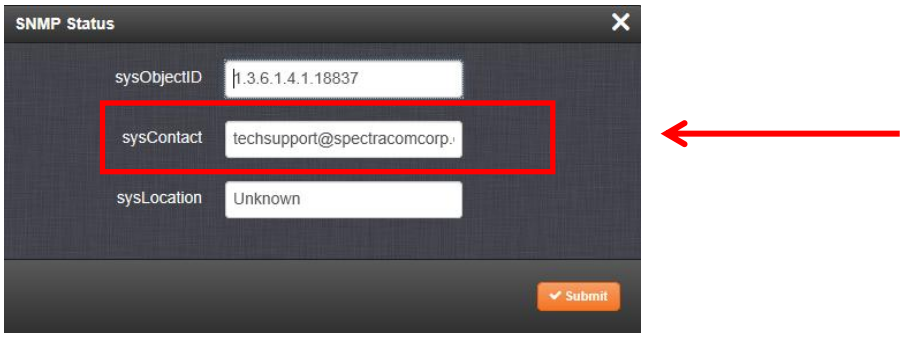
Configuring SNMP System Contact Information

To configure the SNMP system contact information:
Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.

1. In the **SNMP Status** panel click on the button.



2. The **SNMP Status** pop-up window will display.



3. In the **sysContact** field, enter the email information for the system contact you wish to use.

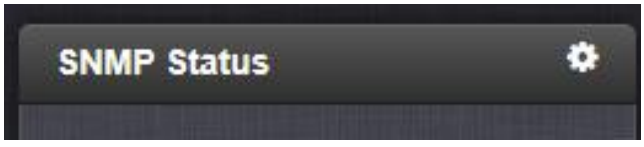
4. Click the **Submit** button at the bottom of the window.

NOTE: You can exit the **SNMP Status** Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **SNMP Status** window before you have hit the **Submit** button, any information you entered will not be retained.

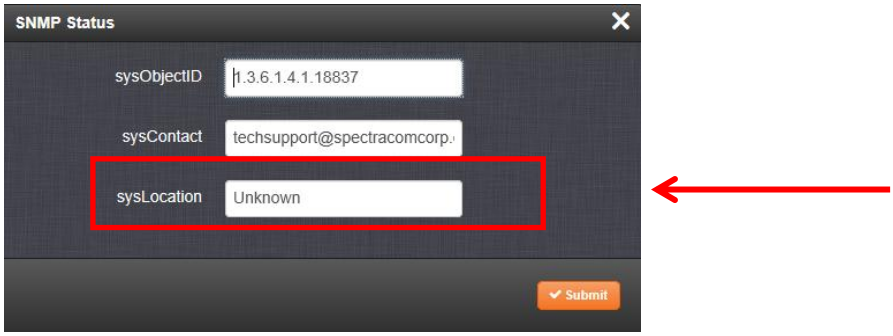
Configuring SNMP System Location

To configure the SNMP system location:
Navigate to the **MANAGEMENT/NETWORK/SNMP Setup** screen.

1. In the **SNMP Status** panel click on the button.



2. The **SNMP Status** pop-up window will display.



3. In the **sysLocation** field, enter the system location of the unit.
4. Click the **Submit** button at the bottom of the window.

NOTE: You can exit the **SNMP Status** Window by clicking on the X at the top right of the window or by clicking anywhere outside the window.
If you exit the **SNMP Status** window before you have hit the **Submit** button, any information you entered will not be retained.

Accessing the SNMP Support MIB Files Provided on the NetClock

Spectracom's private enterprise MIB files can be extracted via File Transfer Protocol (FTP) from the unit using an FTP client such as Microsoft FTP, CoreFTP, or any other shareware/freeware FTP program.

To obtain the MIB files from the unit via FTP/SFTP:

1. Using an FTP program, log in as an administrator.
2. Through the FTP program, locate the Spectracom MIB files in the **`/home/spectracom/mibs`** directory.
3. FTP the files to the desired location on your PC for later transfer to the SNMP Manager.
4. Compile the MIB files 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 names for the files**.** The MIB file names 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.

NOTE: In addition to the Spectracom MIB files, there are also some net-snmp MIB files provided. Net-snmp is the embedded SNMP agent that is used in the NetClockc and it provides traps to notify the user when it starts, restarts, or shuts down. These MIB files may also be compiled into your SNMP manager, if they are not already present.

Spectracom's private enterprise MIB files can be requested and obtained from the Spectracom Customer Service department via email at techsupport@spectracomcorp.com.

NOTE: By default, techsupport@spectracomcorp.com is the address in the **sysContact** field of the SNMP Status panel of the SNMP Setup page.

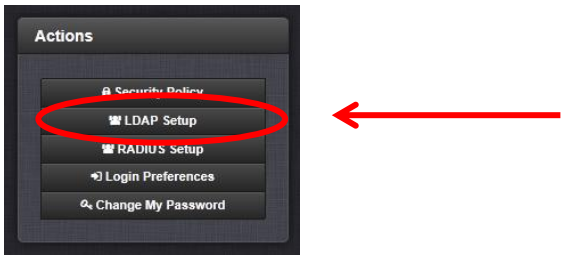
3.19 Configuring LDAP Authentication

LDAP (Lightweight Directory Access Protocol) authentication provides the means to use an external LDAP server to authenticate the user account credentials when logging in to the unit. LDAP allows the login password for user-created accounts to be stored and maintained in a central LDAP or server on the network. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the LDAP server, it automatically changes the login password for all of the appliances that are using the LDAP server to authenticate a user login.

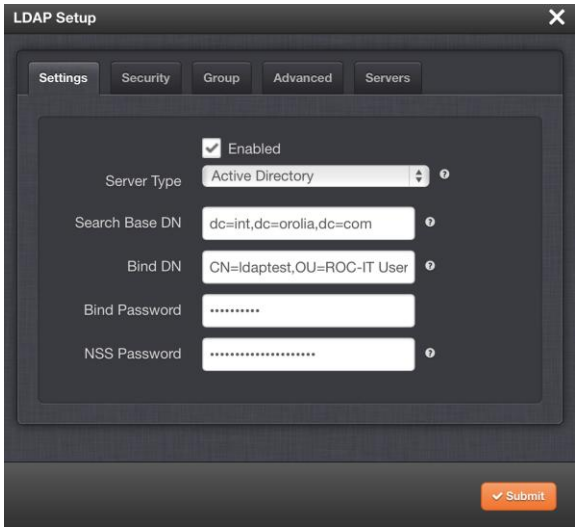
In order to use the LDAP authentication capability of the NetClock, it needs to first be configured with the appropriate settings in order to be able to communicate with the LDAP server(s) on the network.

To configure LDAP authentication:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the LDAP Setup button.



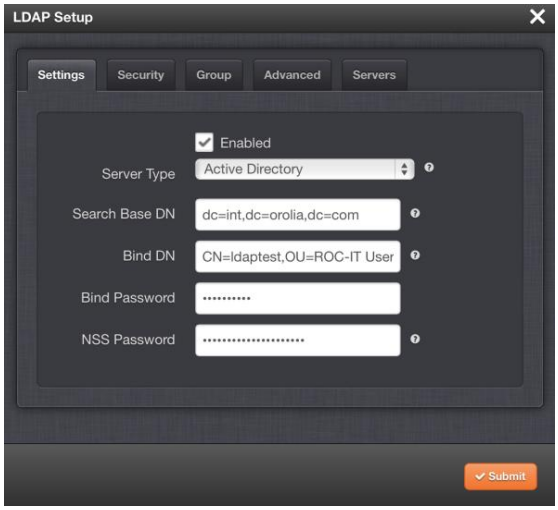
3. The **LDAP Setup** window will display.



4. There will be 5 tabs from which to choose:
   - **Settings**—This is where you set up the general LDAP Distinguished Name and Bind settings.

- **Security**—This is where you upload and manage the CA server certificate, CA client certificate and CA client key.
- **Group**—This is where you enable/disable group-based authentication.
- **Advanced**—This is where you set up your search filter(s) and login attribute.
- **Servers**—This is where you identify the LDAP server to be used.

5. Under the **Settings** tab, set:



- **Server Type**—This must be the correct type—check with your LDAP server administrator if you are not sure which you are using. You have a choice of:
  - **Active Directory**—This will be used when the LDAP server is a Windows server.
  - **Open LDAP**—This will be used when the LDAP server is a Linux/UNIX server.
- **Server Base DN**—Specifies the default base distinguished name to use for searches. This is the base name to use in the database search. Typically, this is the top-level of the directory tree structure. Your LDAP server administrator will provide this information.
- **Bind DN**—Enter the Distinguished Name used to bind to (this is an optional field if the database allows anonymous simple authentication). You are able to use any same level of the tree and everything below.
  The bind DN is the user that is permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter (as specified under the **Advanced** tab) and search base for the DN for authenticating users. When the DN is returned, the DN and password are used to authenticate the user.
- **Bind Password**—Enter the password to be used to bind with the LDAP Server. Leave this field empty for anonymous simple authentication.
- **NSS Password**—Enter the password to be used for nss_base and nss_shadow. Example: ou=People,dc=example,dc=com?one.

6. Under the **Security** tab, you can upload and install the SSL required certificates and NTP client key.

You may upload:

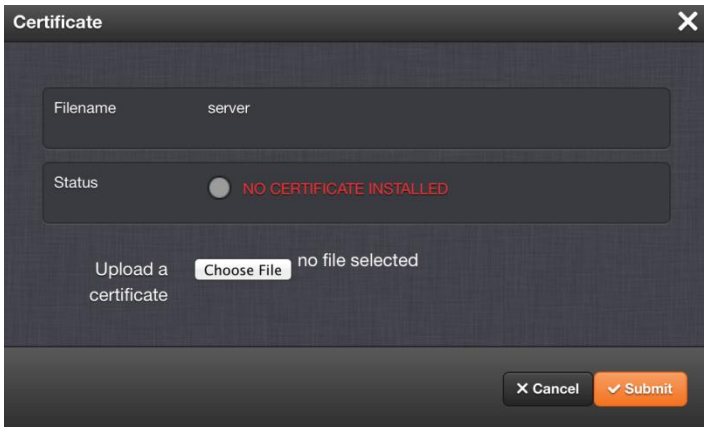
- A server certificate
- A client certificate
- A client key

For each:

a) If necessary, create the desired certificate or client key. See **0 Creating an HTTPS Certificate Request** for information on creating certificates and **0 NTP Autokey—IFF Autokey Support** for information on client keys.

b) Under the Security tab, click on the  button for the certificate you wish to upload.

c) In the window, click on the **Choose File** button.

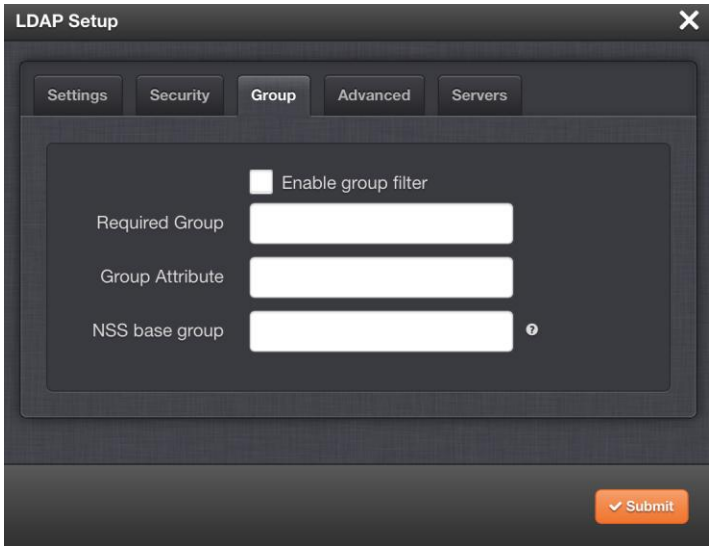


d) Locate and upload the certificate or client key file.

e) Click the **Submit** button.

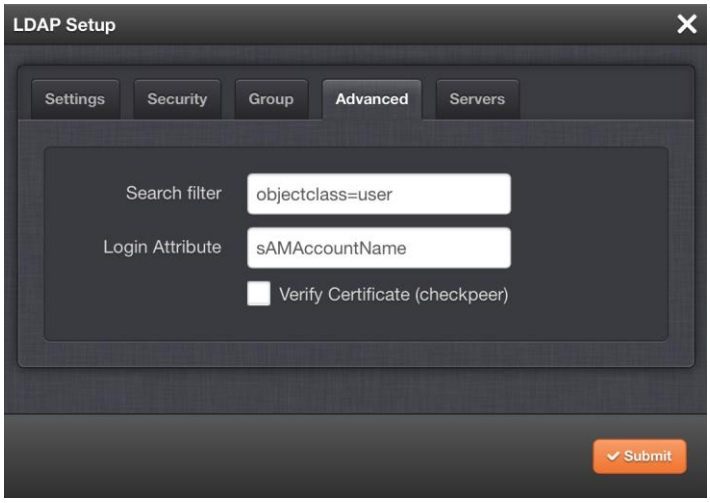
The SSL certificates and/or client key you upload will be installed in the `/home/spectracom/xfer/cert/` directory.

7. Under the **Group** tab, you can filter access by group.



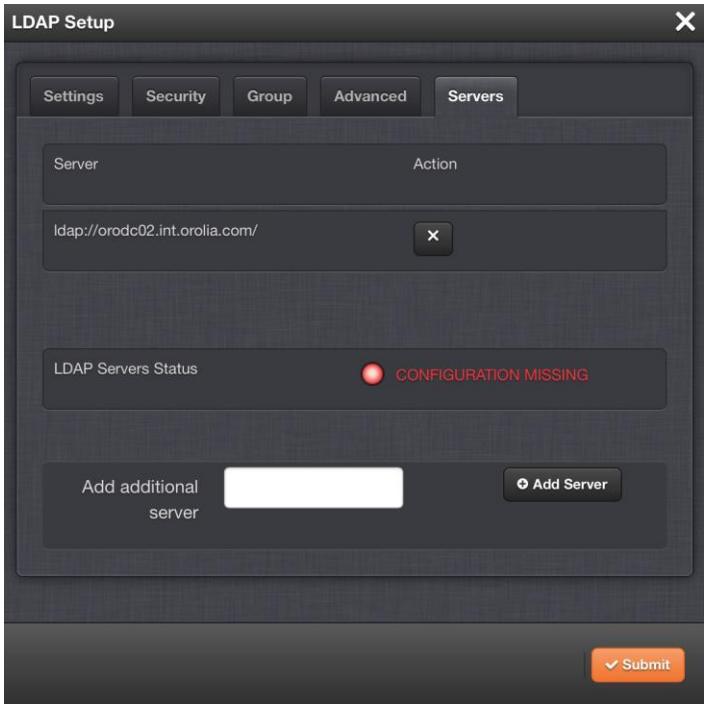
- To enable group authentication:
  a) Select the **Enable group filter** checkbox.
  b) Enter information for
     - **Required Group**—Enter the required group. Example. : `ou=Group, dc=example, dc=com.`
     - **Group Attribute**—Enter the group attribute. Example: `member.`
     - **NSS base group**—Enter the `nss_base` group. Example: `ou=Group, dc=example, dc=com?one.`
  c) Click on the **Submit** button.

9. Under the **Advanced** tab, you can set the search filter and the LDAP login attribute.



- Fill in the following fields, as desired:
  - **Search filter**—This is the LDAP search filter. Example: objectclass=user.
  - **Login Attribute**—This is the LDAP login attribute. Example: sAMAccountName.
  - **Verify Certificate (checkpeer)—**Select this checkbox if you wish to turn on checkpeer authentication.

10. Under the **Servers** tab, you manage the LDAP server(s) to be accessed:



Under the **Servers** tab, the window displays:

- **Server**—The hostname(s) or IP address(es) of the LDAP server(s) that have been added.
    - **Action**—After a server has been listed, it can be removed by clicking the ✕ button.
- **LDAP Server Status**—This will display one of the following states:
    - **PASS** (Green)—An LDAP server that has been set up is available and is able to pass data.
    - **CONFIGURATION MISSING** (Red)—No configuration files are available.
    - **FAILED TO READ DATA** (Red)—An LDAP server is available but no data was passed.
    - **FAILED NOT REACHABLE** (Red)—No LDAP server could be reached.
    - **LDAP DISABLED**—The Enabled checkbox under the Settings tab as not been selected.
- **Add additional server**—Enter the hostname or IP address of the LDAP server to be queried. You may list multiple servers.

3.19.1 RADIUS Authentication

RADIUS authentication provides the means to use an external RADIUS server to authenticate the user accounts when logging in to the unit. RADIUS allows the login password for user-created accounts to be stored and maintained in a central RADIUS or server on the network. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the RADIUS or RADIUS server, it automatically changes the login password for all of the appliances that are using the RADIUS server to authenticate a user login.

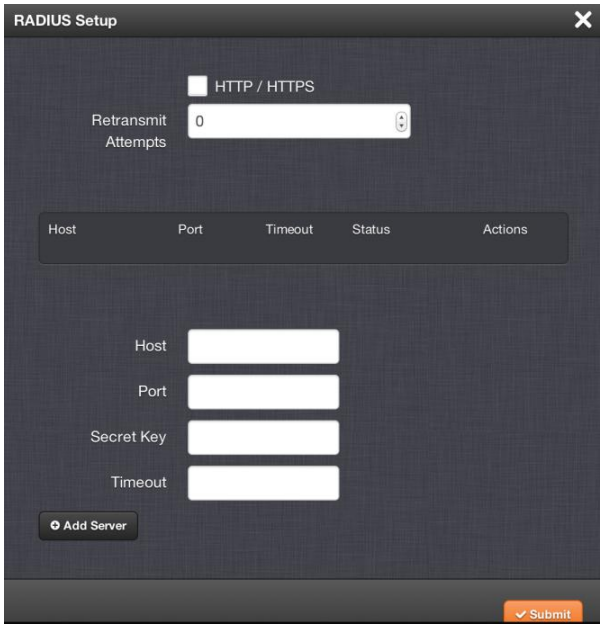
In order to use RADIUS authentication capability of the unit, it needs to first be configured with the appropriate settings in order to be able to communicate with the RADIUS server(s) on the network.

Configuring RADIUS authentication

To configure RADIUS authentication:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button

3. The **Radius Setup** window will display.



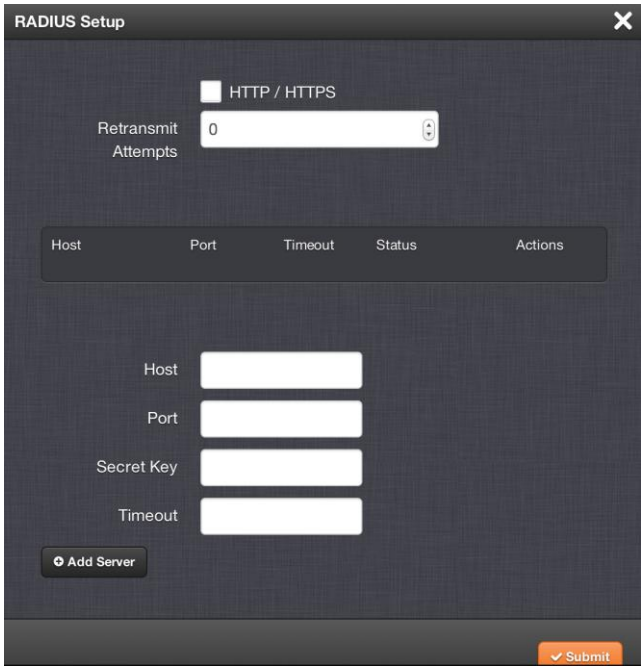
- If desired, select the **HTTP/HTTPS** checkbox to enable HTTPS.
- In the **Retransmit Attempts** field, select the number of retries for unit to communicate with the RADIUS server.

Adding a RADIUS server.

To add a RADIUS server:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button

3. The **Radius Setup** window will display.



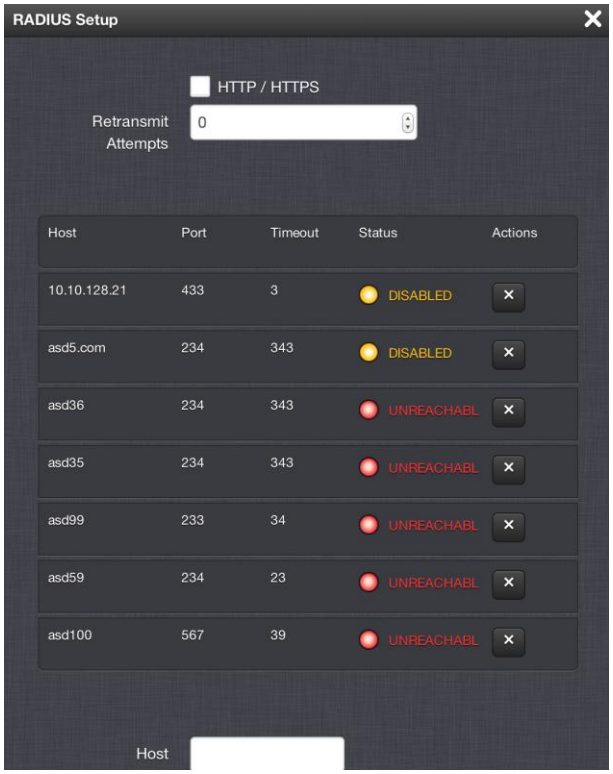
4. Populate the following fields as needed:
   - **Host**—Enter either the hostname or IP address of the RADIUS server on the network with which you wish the unit to authenticate.
   - **Port**—Defines the RADIUS Port to use. The default RADIUS Port is 1812, but this can be changed, as required.
   - **Secret key**—Enter the secret key which is shared by the unit and the RADIUS server (the key is used to generate an MD5 hash).
   - **Timeout**—Defines the Timeout that the unit will wait to communicate with the RADIUS server.
5. Click the **Add Server** button.

Viewing the status of a RADIUS server

To view the status of a RADIUS server:

1. Navigate to **MANAGEMENT/OTHER/Authentication**.
2. In the **Actions** panel, click the **RADIUS Setup** button

3. The **Radius Setup** window will display.



For each RADIUS server, the following information will display:

- **Host**—The hostname or IP address of the RADIUS server.
- **Port**—The RADIUS port used to access the RADIUS server.
- **Timeout**—The timeout that has been set for the RADIUS server.
- **Status**—One of the following statuses will display:
  - **UNREACHABLE** (red, blinking)—The server is not available on the network.
  - **UNAUTHORIZED** (red)—The server is available on the network but access was denied.

- **REACHABLE** (green)—The server is available on the network and access was allowed.
- **DISABLED** (yellow)—The server is available on the network but RADIUS authentication is disabled on the server.

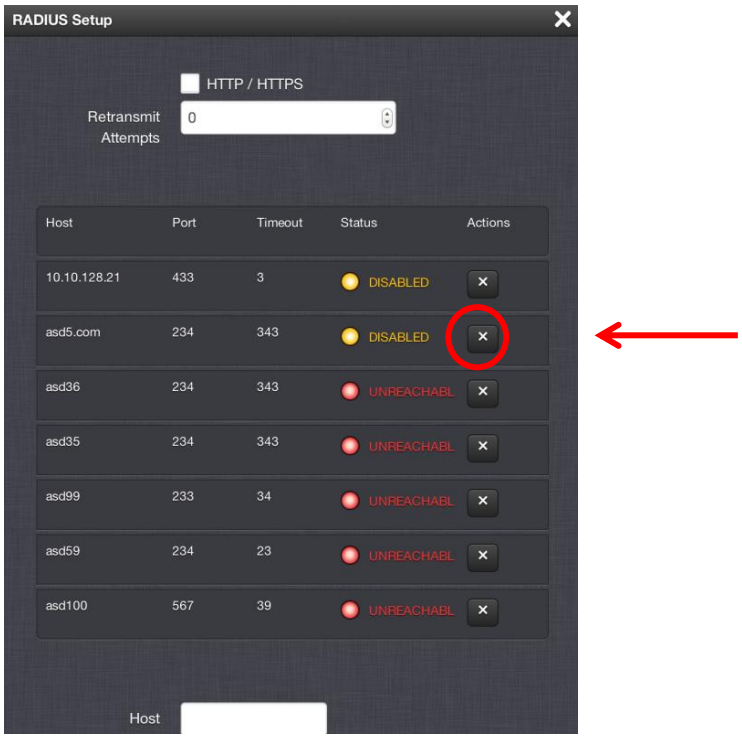
- **Actions**—Click the ✕ button to remove a server.

Removing a RADIUS server

To remove a RADIUS server:

2. Navigate to **MANAGEMENT/OTHER/Authentication**.
3. In the **Actions** panel, click the RADIUS Setup button

4. The **Radius Setup** window will display.



5. For the RADIUS server you wish to remove, click on the ✕ button.

Section 4: NetClock Status Indications

In addition to the available NetClock logs, status information about the unit can be viewed and monitored several ways. These status indications include the time synchronization with its selected references, GPS satellites currently being tracked, estimated time errors, oscillator disciplining, NTP sync status and current Stratum level, status of outputs and presence of DC input power.

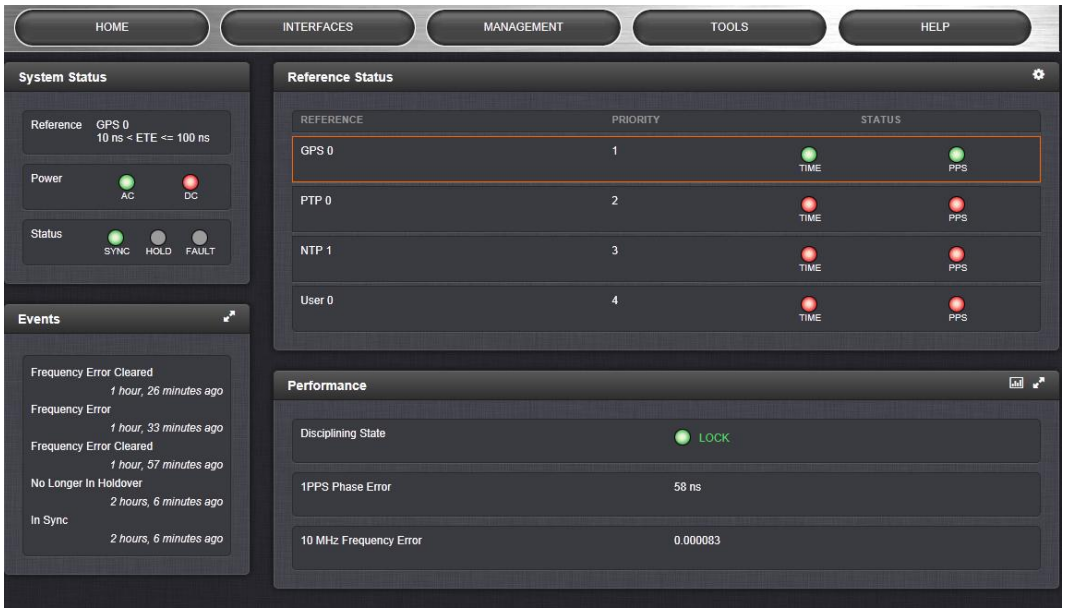
4.1 Front Panel LED Status Indications

The NetClock front panel status LEDs are one indication of the current operational status. For detailed information, refer to the table in Section *1.7*: "*NetClock 9400 Series Front Panel LED Status Indicator Lights*".

4.2 Web Interface Status Indications

4.2.1 Using the HOME Page to Monitor Status Indications

The NetClock Web interface is designed to give immediate and easy access current status information directly from the interface's **HOME** page.



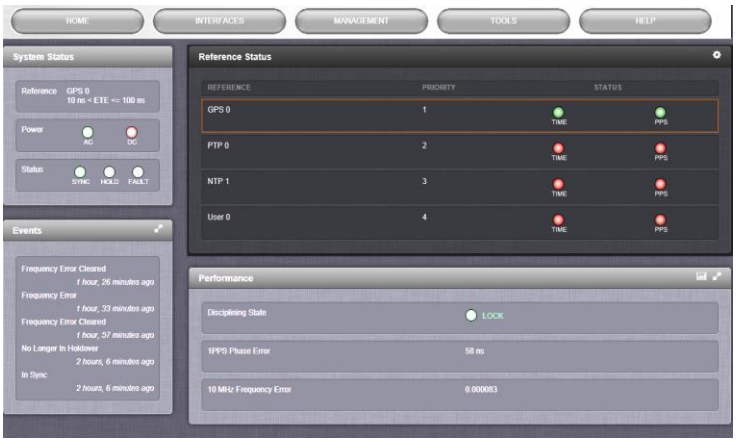
The **HOME** page is divided into 4 panels:

The **System Status** panel

The **System Status** panel provides information on:

- **Reference**—Indicates the status of the current synchronizing reference, if any.
- **Power**—Indicates whether the power is on and which type of power is being used. If the unit is configured for AC power, AC will appear in this panel. If the unit is configured for DC power, DC will appear in this panel. If the unit is configured for both AC and DC, AC and DC will appear in this panel.
- **Status**—Indicates the status of the network's timing. There are three indicators in the Status field:
  - **Sync**—Indicates whether the unit is synchronized to its selected input references.
    - Green indicates it is currently synchronized to its references (The front panel Sync light will also be green).
    - Orange indicates it is not currently synchronized to its references (The front panel Sync light will be red).
  - **Hold**—When lit, indicates that the unit is in holdover mode.
  - **Fault**—Indicates a fault in the operation of the unit.

The **Reference Status** panel



The **Reference Status** panel provides information on the status of the network's references. The panel provides information on:

1. **Reference**—Indicates the name type of each reference. These are determined by the inputs set up for the unit.
2. **Priority**—Indicates the priority of each reference. This number will be between 1 and 15. References in this panel appear in their order of priority.
3. **Status**—Indicates which available input reference is acting as the Time reference and which available input reference is acting as the 1PPS reference.
    - Green indicates that the reference is present and has been declared valid.
    - Orange indicates the input reference is not currently present or is not currently valid
4. See the appropriate section for information on setting reference priority.

The **Performance** panel

The **Performance** panel provides information on:

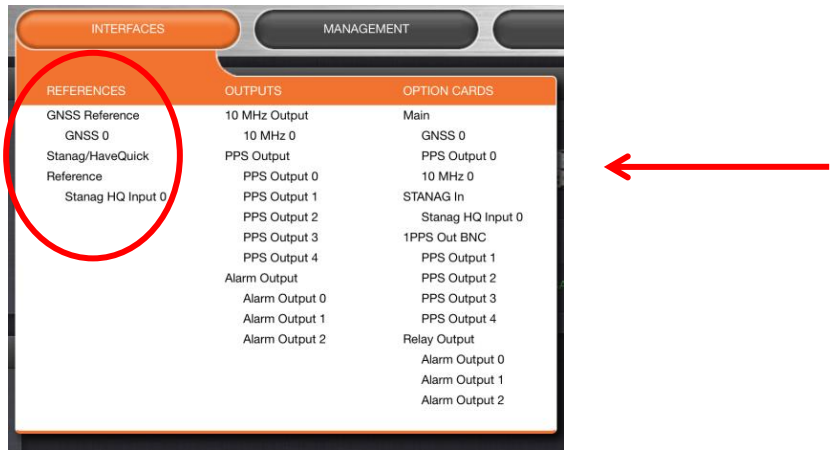
- **Disciplining State**—Indicates whether or not the internal oscillator is currently being disciplined (steered to an input reference).
- **1PPS Phase Error**—An internal measurement (in nanoseconds) of the internal 1PPSs' phase error with respect to the selected input reference (if the input reference has excessive jitter, phase error will be higher)
- **10MHz Frequency Error—**An internal estimated calculation (in Hertz) of the internal oscillator's frequency error, based on the phase accuracy error at the beginning and end of a frequency measurement window (the length of this window will vary depending upon the type of oscillator installed and the oscillator adjustment algorithm).

The **Events** panel.

The **Events** panel is a log of theNetClock's recent activity. It updates in real time.

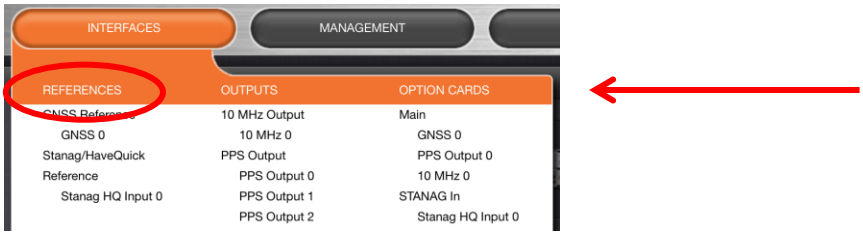
4.2.2 Monitoring the Status of Input References

The NetClock's input references can be monitored in real time through the **INTERFACES** drop-down menu. The menu will populate dynamically, according to which references are available.



Monitoring All Input References

To monitor all references, click on **REFERENCES** in the **INTERFACES** menu.

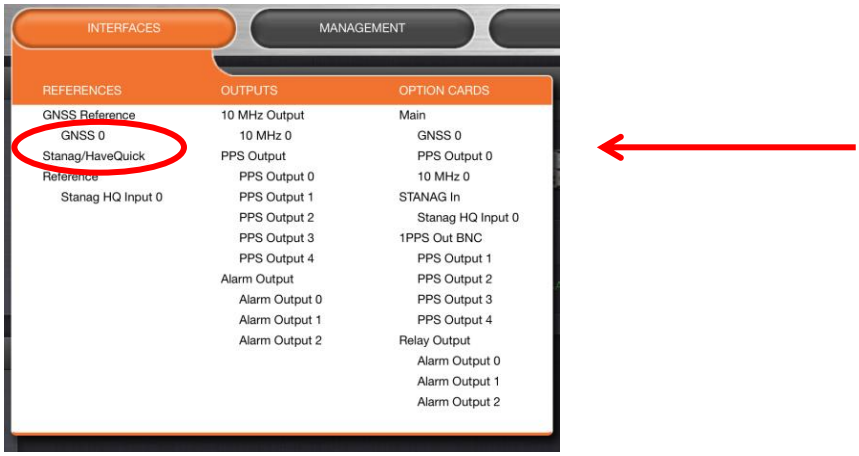


The resulting screen will display all the system references.

Monitoring All of a Specific Type of Input Reference

To monitor all a specific type of reference, click on general entry for that type of reference in the menu.

1. In the **INTERFACES/REFERENCES** column, select the type of reference you wish to monitor.



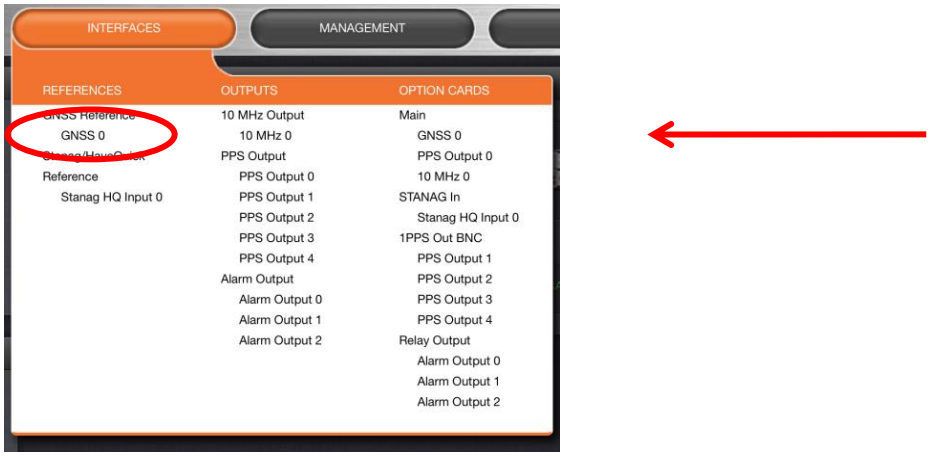
2. The resulting screen will display all the system references of your chosen type.

Viewing the Status of an Individual Input Reference

There are methods to reach the status window for a specific reference:

Method 1

1. Click on the specific entry for that reference in the menu.

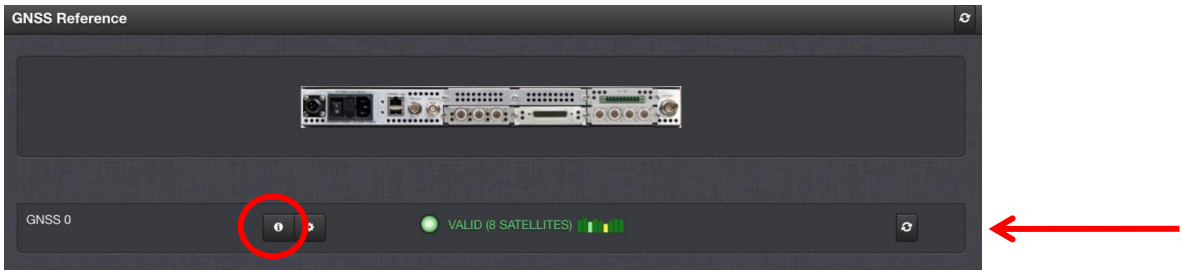


2. The resulting screen will display the status window for the specific reference you selected.

Method 2

1. Navigate to the Reference page for the reference type you want to monitor through the **INTERFACES/REFERENCES** drop-down menu.
2. Click on the  button located in that output's status.

NOTE: A particular option card might have more than one setting that can be viewed. See the appropriate section for the settings of any particular output or card.



The settings status window will display.

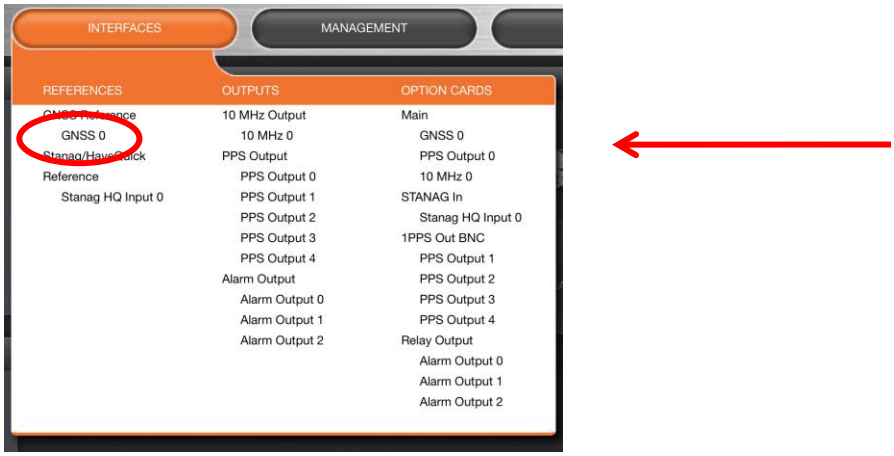
NOTE: You can access the option card's edit window directly from the settings detail window by clicking on the **Edit** button.

Editing the Settings of an Input Reference

There are methods to reach the status window for a specific reference:

Method 1

1. Click on the specific entry for that reference in the menu.



2. The resulting screen will display the status window for the specific reference you selected.

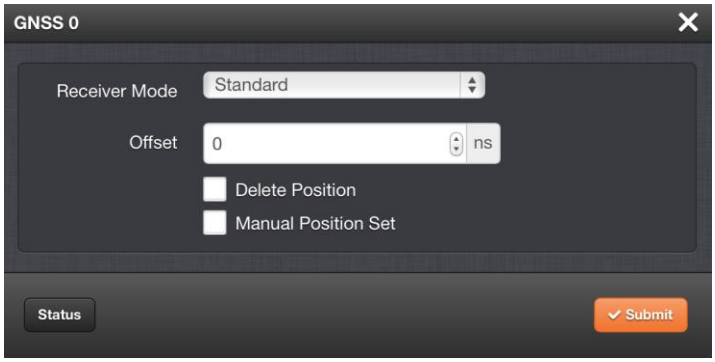
3. Click on the **Edit** button at the bottom of the window.

Method 2

1. Navigate to the Reference page for the reference type you want to monitor through the **INTERFACES/REFERENCES** drop-down menu.
2. Click on the  button located in that option card's status.

NOTE: A particular option card might have more than one setting that can be adjusted. See the settings of any particular output or card.

3. The edit window will display.

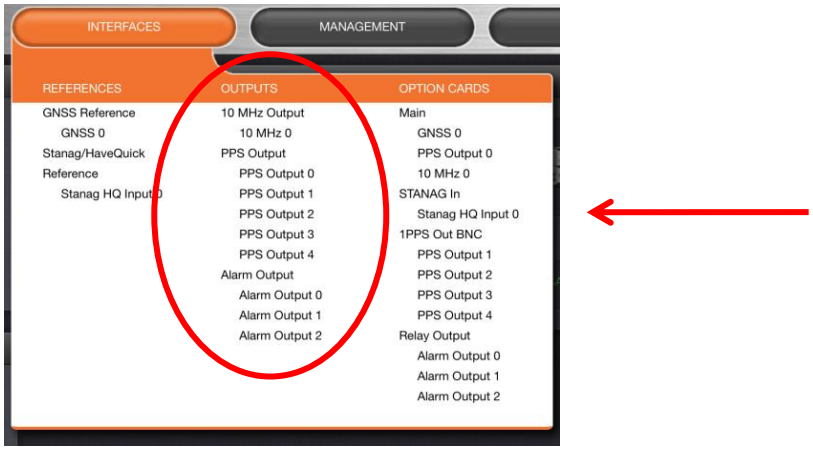


Edit the field(s) as desired.

NOTE: You can access the reference's settings window directly from the edit detail window by clicking on the **Status** button.

4.2.3 Monitoring the Status of Outputs

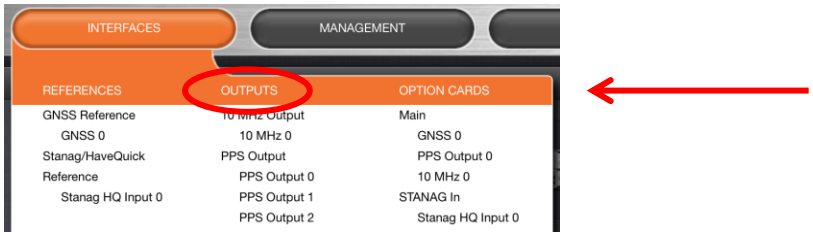
The NetClock's installed outputs can be monitored in real time through the **INTERFACES** drop-down menu. The menu will populate dynamically, according to which outputs are available.



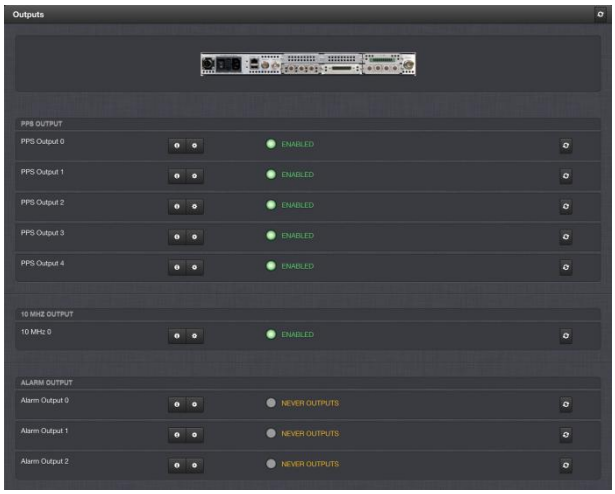
Monitoring the Status of all Outputs

To monitor all outputs:

1. Click on **OUTPUTS** in the menu.



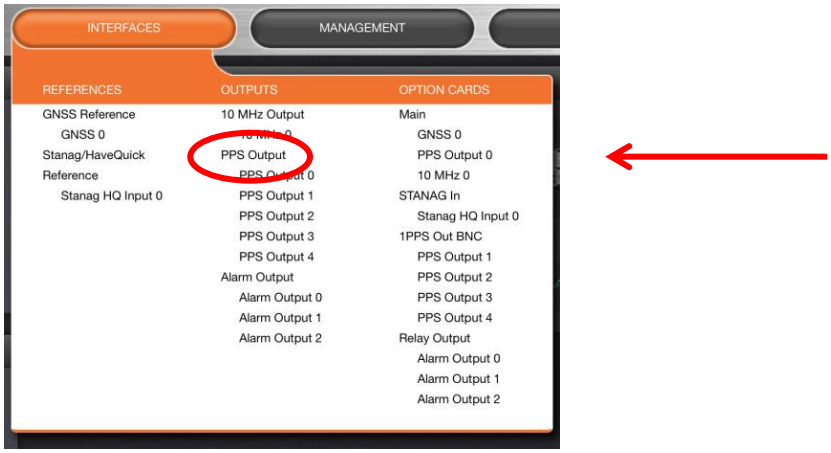
2. The resulting screen will display all outputs.



Monitoring All of a Specific Type of Outputs

To monitor all outputs of a specific type:

1. Click on the specific type of output in the **INTERFACES/OUTPUTS** drop-down menu.

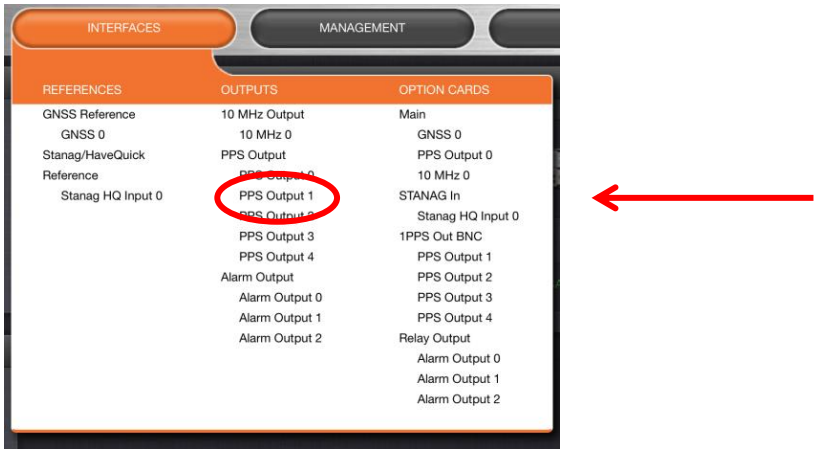


2. The panel will display for the specific type of output you selected.

Viewing the Status of an Individual Output

To view the settings of an individual output:

1. Click on the individual output in the **INTERFACES/OUTPUTS** drop-down menu.



2. The status window will display for the specific output you selected.

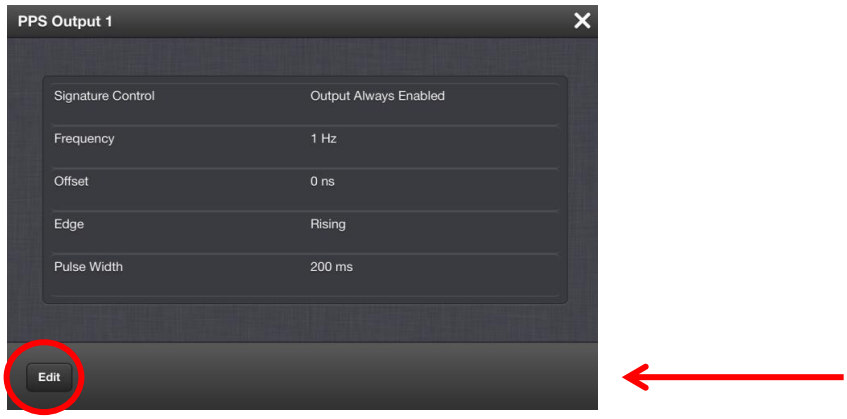
NOTE: You can access the output's edit window directly from the settings detail window by clicking on the **Edit** button.

Editing the Settings of an Individual Output

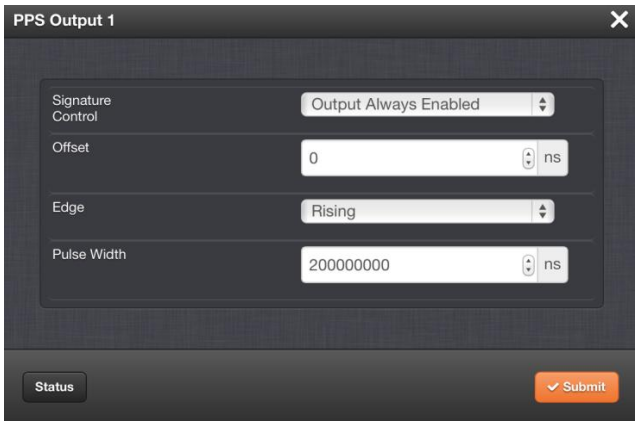
To edit the settings of an individual output:

1. Click on the individual output in the **INTERFACES/OUTPUTS** drop-down menu.

2. The status window will display for the specific output you selected.



3. Click on the **Edit** button at the bottom of the status window.
4. The edit window will display for the specific output.

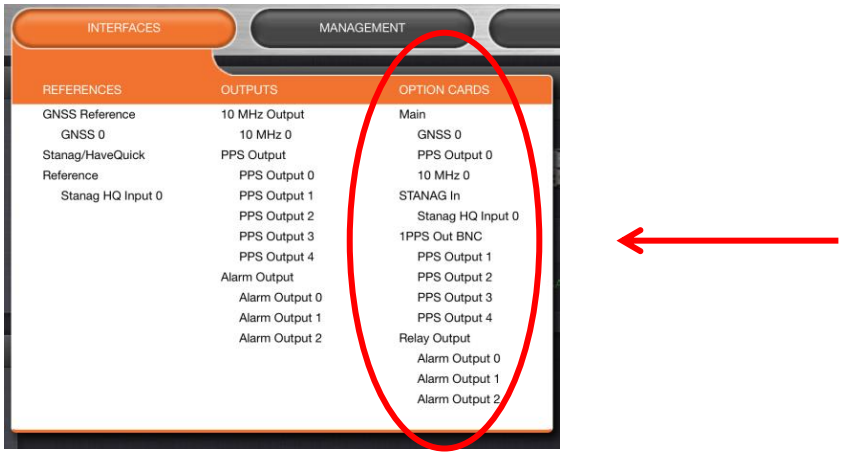


NOTE: See the options section for information specific to a particular output or card.

NOTE: You can access the output's settings window directly from the edit window by clicking on the **Status** button.

4.2.4 Monitoring the Status of Installed Option Cards

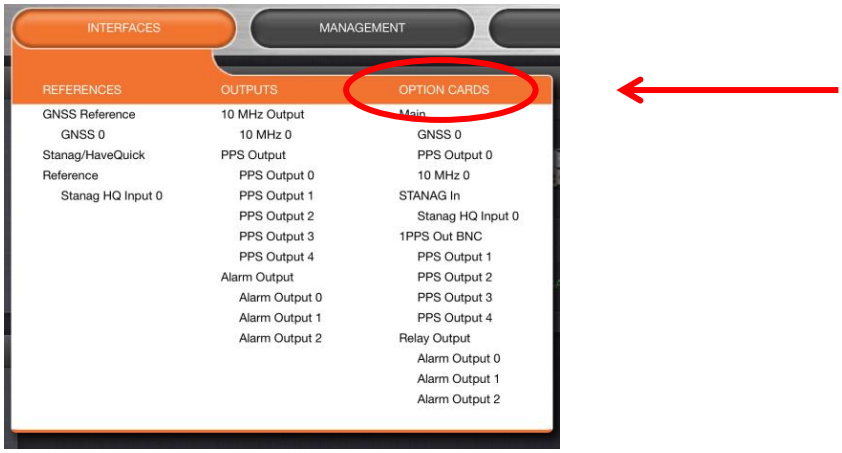
NetClock's installed option cards, if any, can be monitored in real time through the **INTERFACES/OPTION CARDS** drop-down menu. The menu will populate dynamically, according to which option cards are installed.



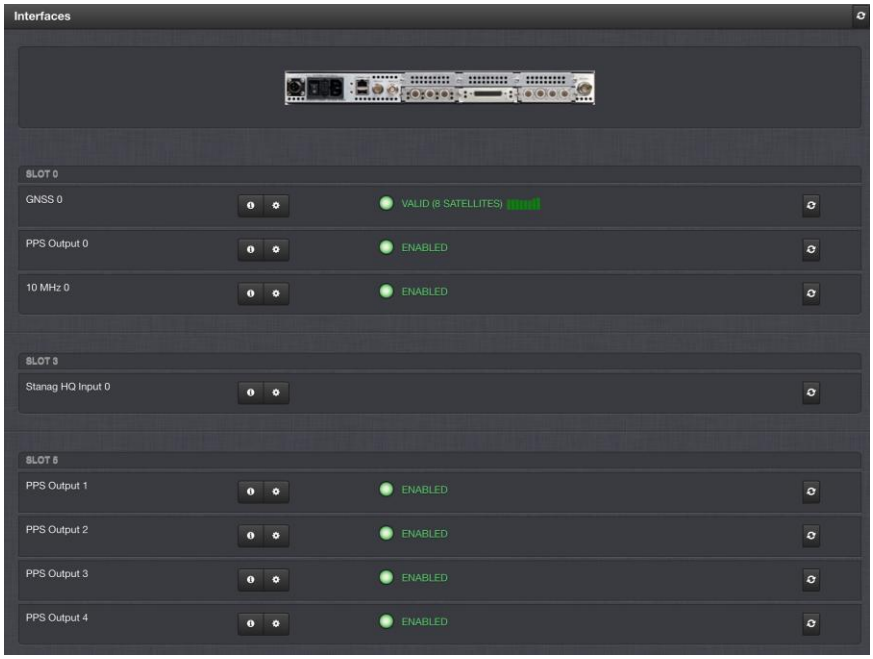
Viewing the Status of All Installed Option Cards

To monitor all option cards:

1. Click on **OPTION CARDS** in the menu.



2. The resulting screen will display all installed option cards.



Viewing the Status of Individual Installed Option Cards

To monitor a specific option card:

1. Navigate to the specific option card in the **INTERFACES/OPTION CARDS** drop-down menu.

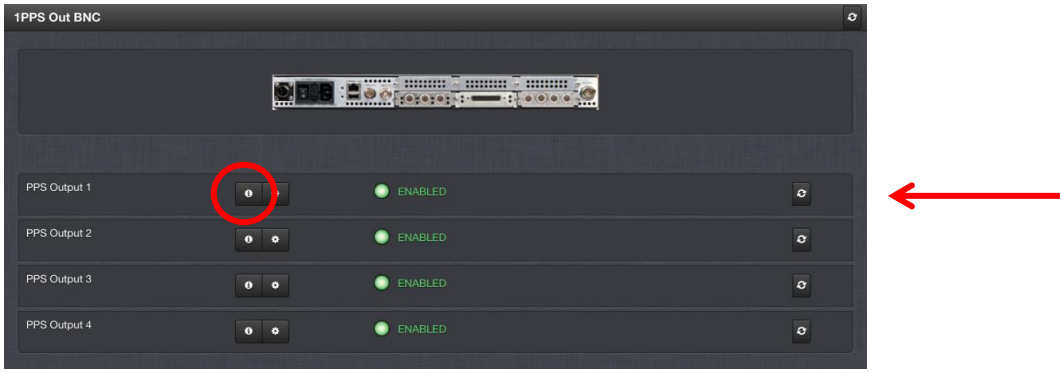
2. The options window will display for the specific option card you chose.

Viewing the Status of an Option Card's References and Outputs

To view the status of an option card's references and outputs:

1. Navigate to the specific option card in the **INTERFACES/OPTION CARDS** drop-down menu.
2. Click on the  button for the reference or output whose status you wish to see.

NOTE: A particular option card might have multiple references and/or outputs that can be viewed. See the section on option cards for the settings of any particular option card.



3. A status window for that reference or output will display.

NOTE: If you know the individual reference or output whose status you wish to see, you can access the status window of that reference or output directly through the **INTERFACES/REFERENCES** or **INTERFACES/OUTPUTS** drop-down menu. See **0 Viewing the Status of Individual Installed Option Cards** or **0 Monitoring All of a Specific Type** of Outputs.

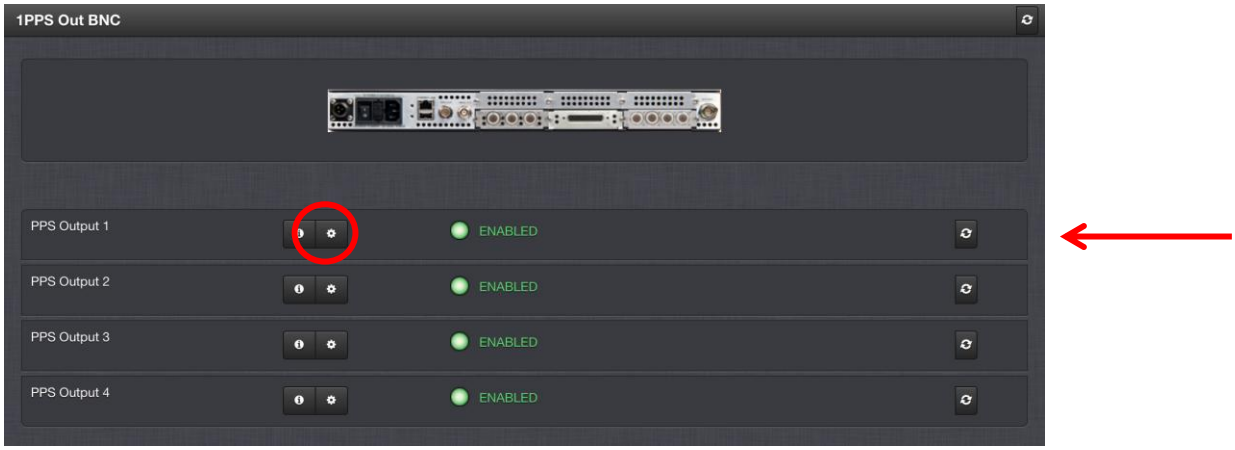
Editing the Settings of an Option Card's References or Outputs

To edit the settings of an option card's references or outputs:

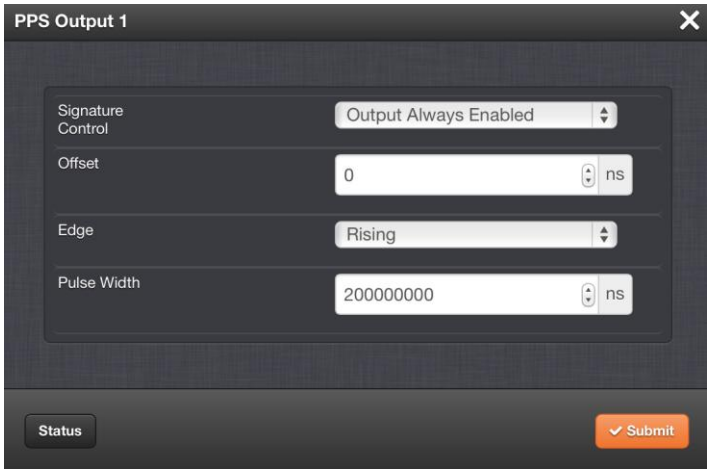
To view the status of an option card's references and outputs:

1. Navigate to the specific option card in the **INTERFACES/OPTION CARDS** drop-down menu.
2. Click on the  button for the reference or output you wish to edit.

NOTE: A particular option card might have multiple references and/or outputs that can be viewed. See the settings of any particular option card.



3. The edit window for that reference or output will display.



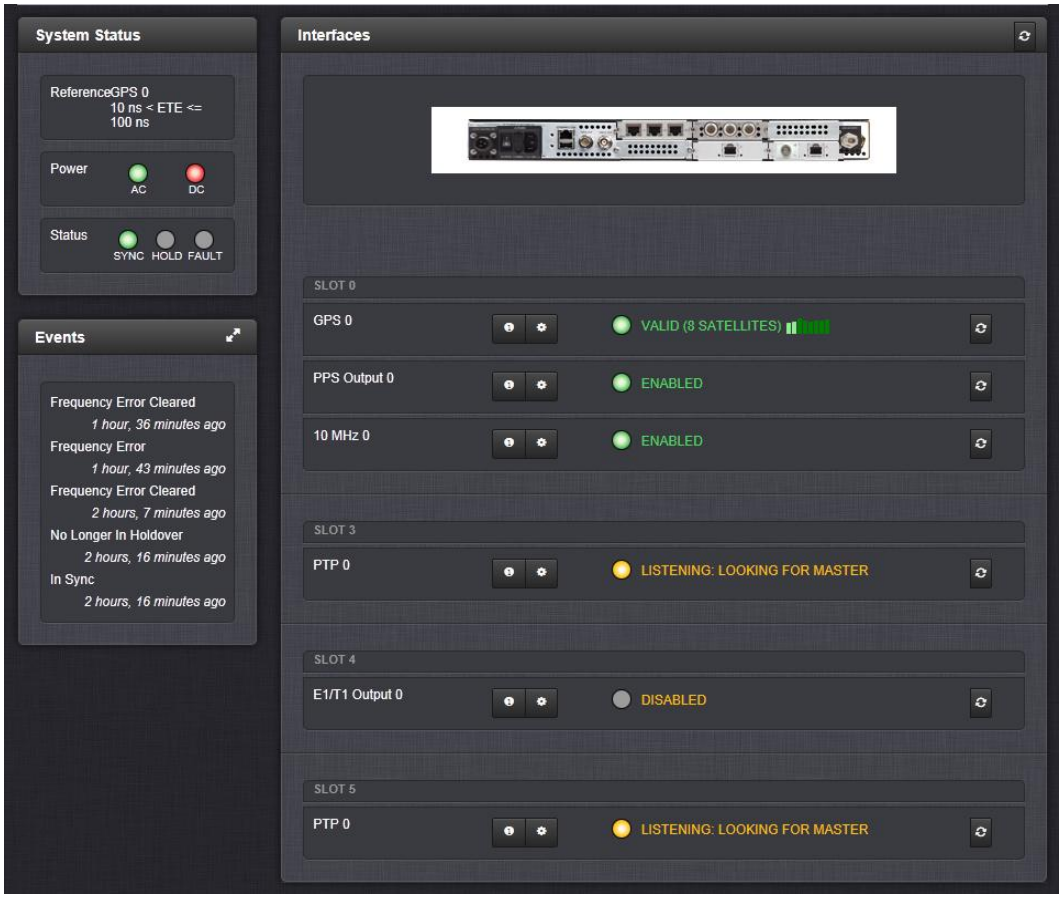
4. Edit the field(s) as desired.

NOTE: If you know the individual reference or output whose status you wish to see, you can access the status window of that reference or output directly through the **INTERFACES/REFERENCES** or **INTERFACES/OUTPUTS** drop-down menu.

4.2.5 Monitoring the Status of All Interfaces

All of unit's interfaces can be monitored by clicking on the **INTERFACES** button, rather than dragging down to expose the drop-down menu.

The resulting screen will show all the interfaces.



Section 5: NetClock Logs

The unit generates log files for:

- System
- Events
- Alarms
- Timing
- GPS Qualification
- Oscillator (Discipline)
- Journal
- Update
- Authentication

The logs are all stored internally by default. With the exception of the NTP log, all logs can also be configured to be stored externally, if desired.

The log entries for the logs can also be configured to be automatically sent to a Syslog Server for external log storage. In order for these logs to be sent to a Syslog server, each desired log needs to be configured for Syslog operation. With the exception of the Authentication and NTP logs, all log setup options can be configured from the **Logs Configuration** page.

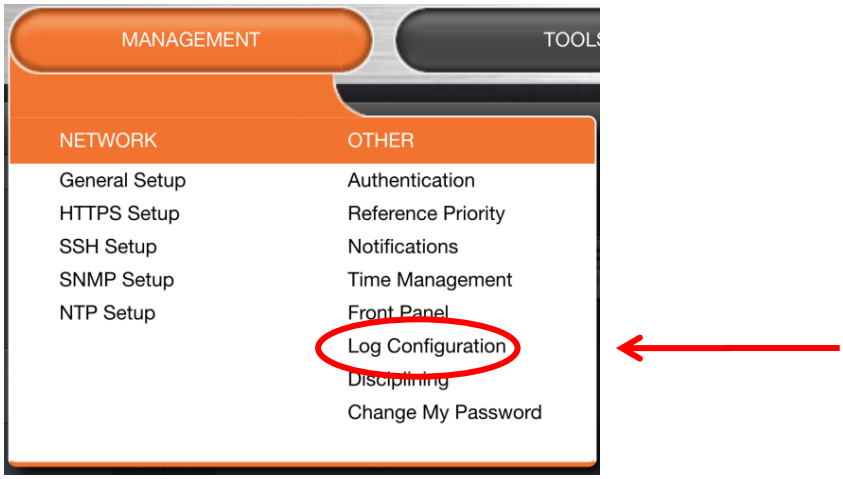
NOTE: The NTP log has no available configuration options.

In each log, entries appear with the most recent events first (i.e., in reverse chronological order, starting from the top).

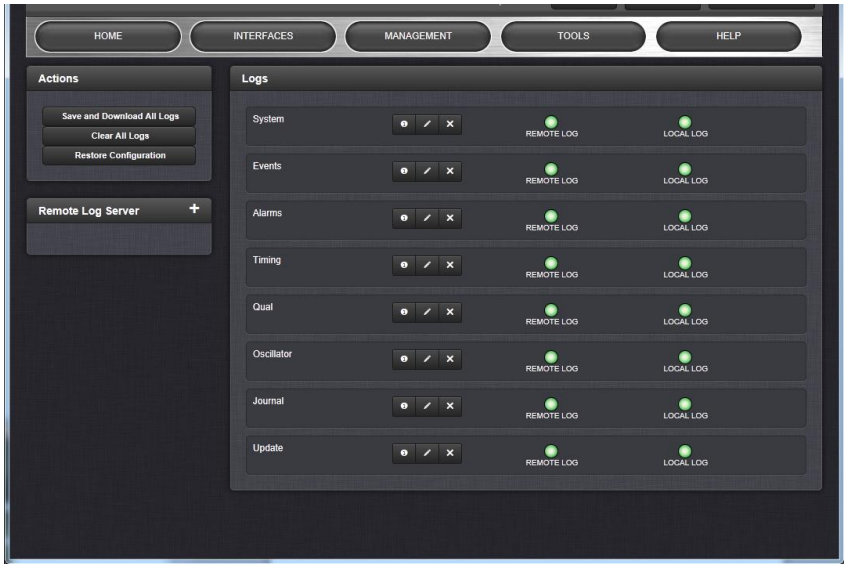
5.1 Accessing all the Logs

To access all the logs:

1. Navigate to the Logs page **through MANAGEMENT/OTHER/Log Configuration**:



2. The **Logs** screen will appear.

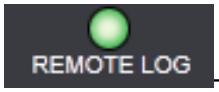


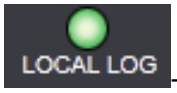
Each of the available logs will appear in the Logs table.

For each entry the following is available:

-  —Click this button to read the log.
-  —Click this button to configure the log.
  - The window that displays will offer the configuration options for that log.
-  —Click this button to clear the log.

NOTE: The “Clear File” feature does not delete any of the logs that have been sent to and stored in a Syslog server.

- 

—If this is green, the log is stored remotely.
- 

—If this is green, the log is stored on the unit.

5.1.1 The Log Screen

The log screen is broken into 3 panels:

The **Logs** panel

The **Logs** panel allows you access to the logs stored locally on the unit.

The **Actions** panel

The **Actions** panel allows you to perform batch actions on your logs:

- **Save and Download All Logs—**Save and download all the logs on the unit.
- **Clear All Logs—**Clear all the logs on the unit.
- **Restore Configuration—**Restore all log configurations to their factory settings.

The **Remote Log Server** panel

The **Remote Log Server** panel is where you set up and manage logs on one or more remote locations.

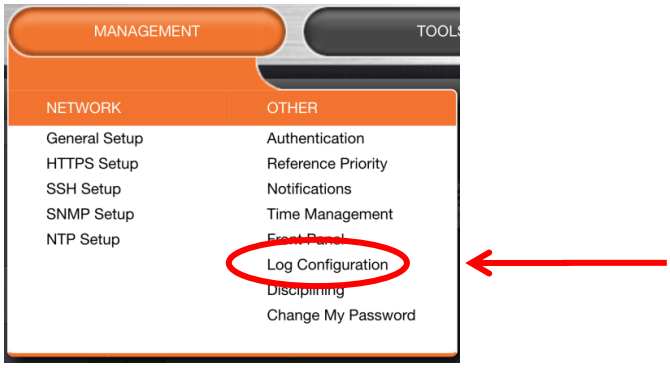
5.2 Accessing Individual Logs

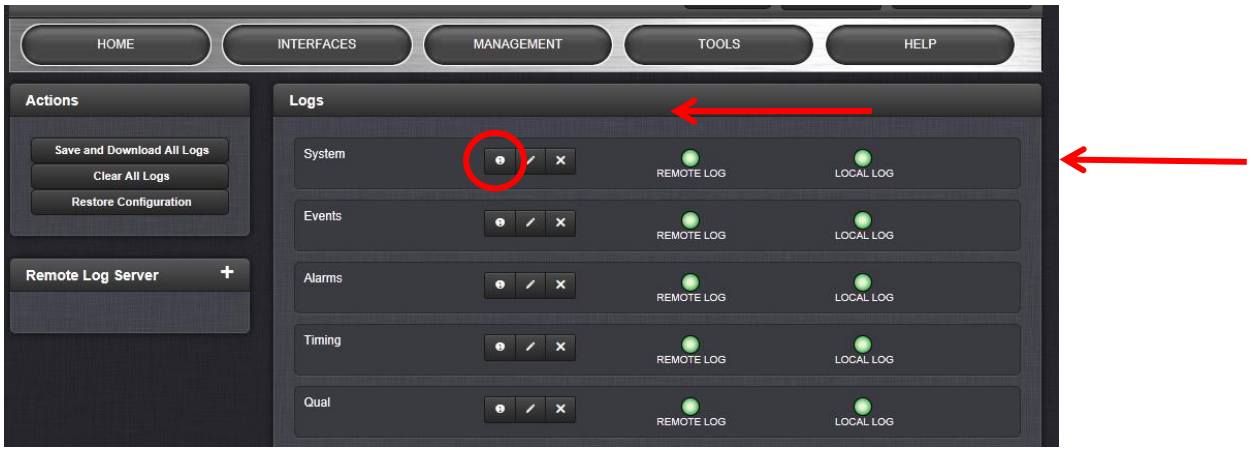
To access individual logs:

1. Select the log from the **LOGS** column in the **TOOLS** drop-down menu.

OR

1. Access the **Logs** screen through the MANAGEMENT/OTHER/Log Configuration drop-down menu.



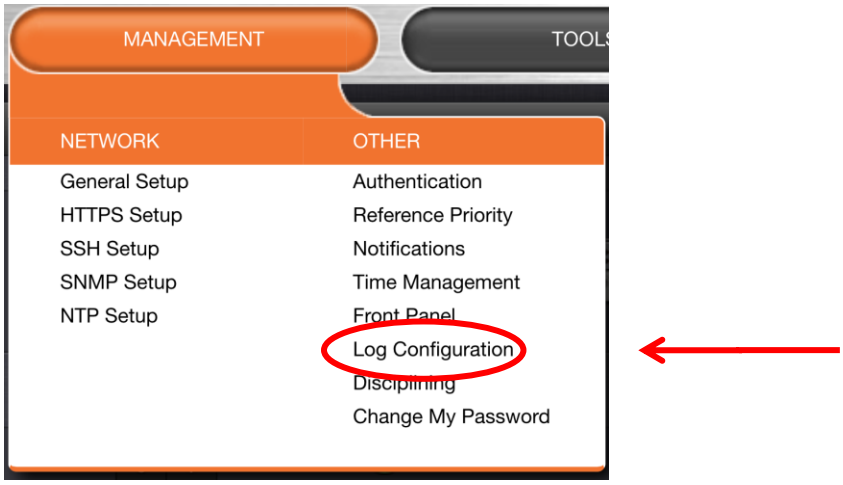


2. Click on the  button in the table entry on the **Logs** panel.

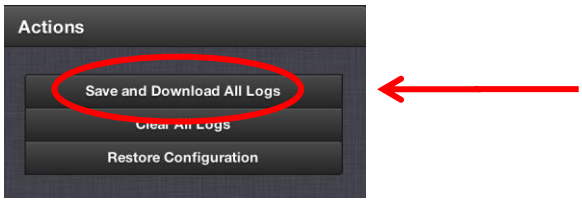
5.3 Saving and Downloading All Logs

To save and down all logs:

3. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



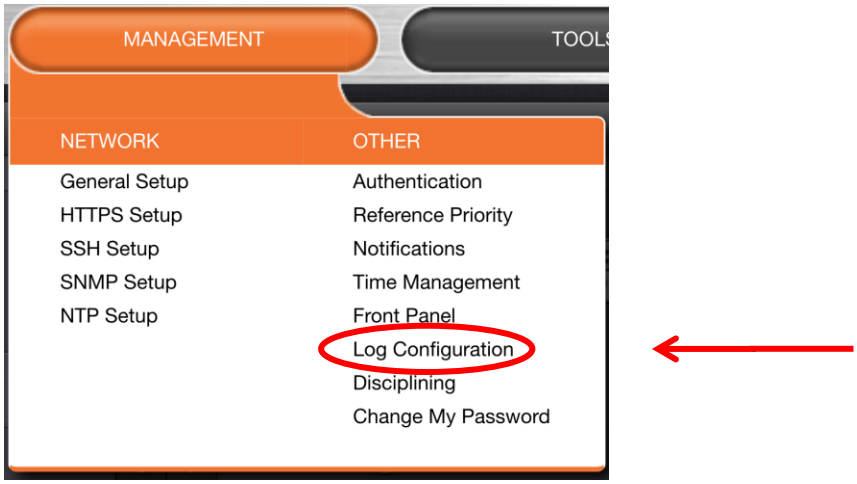
4. In the **Actions** panel, click on the **Save and Download All Logs** button.



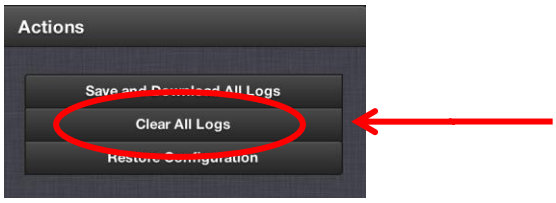
5.4 Clearing All Logs

To clear all the logs:

4. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



5. In the **Actions** panel, click on the **Clear All Logs** button.

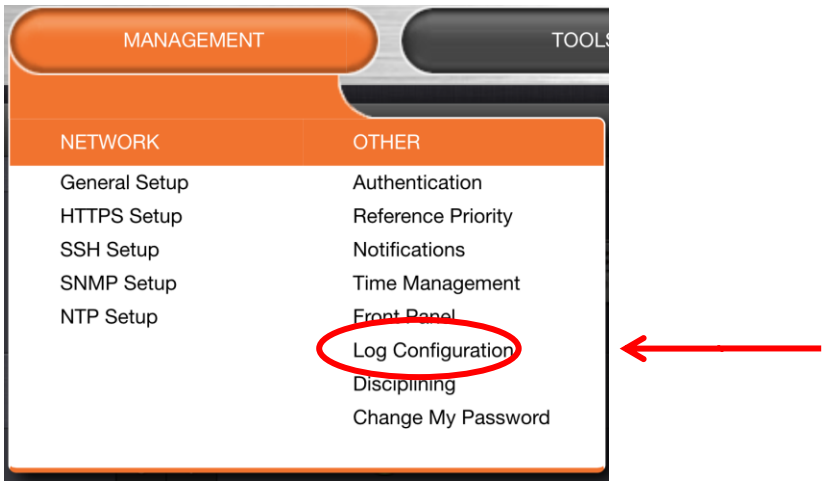


6. In the message window that displays, click **OK**.

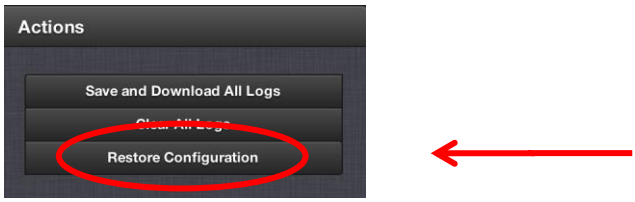
5.5 Restoring Log Configurations

To restore log configurations:

5. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



6. In the **Actions** panel, click on the **Restore Configurations** button.

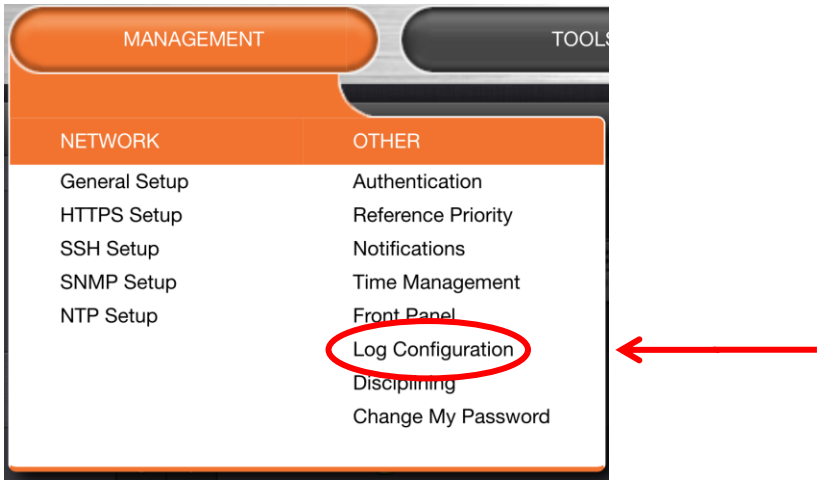


7. Click the **Browse** button.
8. Navigate to the directory where the configurations are stored and click **Upload**.

5.6 Adding Remote a Log Server

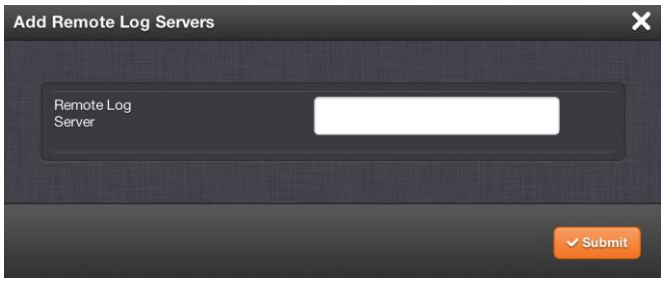
To add remote log servers:

1. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



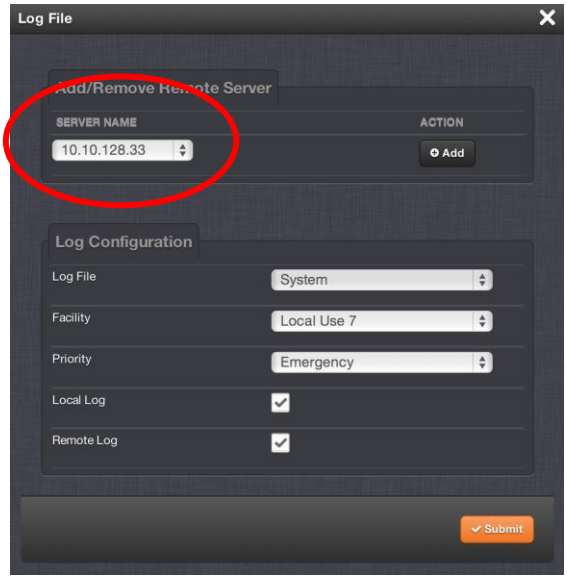
2. In the **Remote Log Server** panel, click on the **"+"** button in the top-right corner of the panel.

3. The **Add Remote Log Servers** window displays.



4. Enter the IP address or host server name (e.g. "MyDomain.com") you wish to use as a remote log server
5. Click the **Submit** button.
6. Your remote log server will appear in the **Remote Log Server** panel.

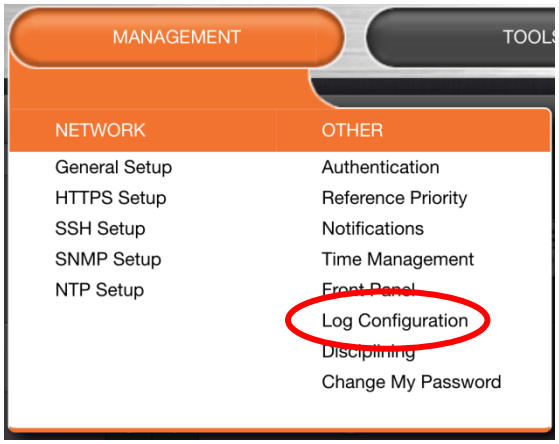
7. The remote server now appears as an option in the **SERVER NAME** drop-down list in the **Add/Remove Remote Server** panel in any log file configuration screen.



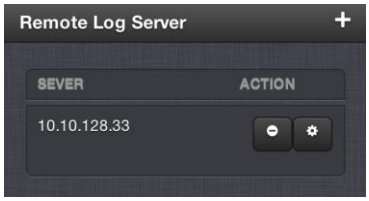
5.7 Changing or Deleting a Remote Log Server

To change or delete a remote log server:

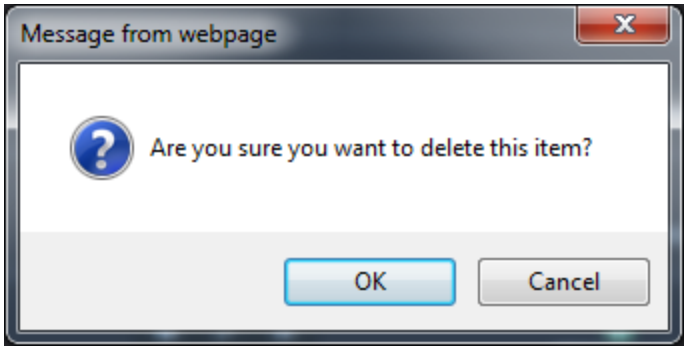
1. Navigate to the Logs page through **MANAGEMENT/OTHER/Log Configuration**:



2. In the **Remote Log Server** panel locate the remote server you wish to change or delete.

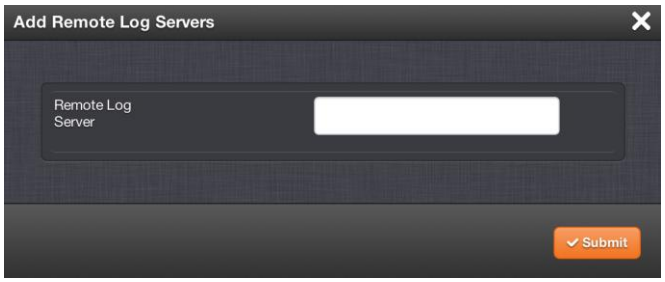


3. Choose
   - the  button to delete the remote log server and in the message window that displays click **OK**.



OR

   - the  button to change the remote log server in the **Add Remote Log Servers** window and type in a new IP address or host domain server (e.g. MyDomain.com).



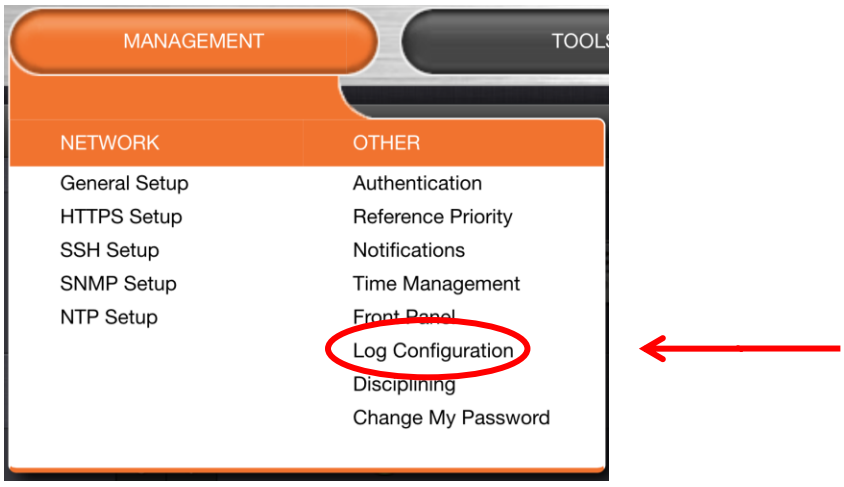
NOTE: Clicking the Delete button in the Log File configuration window does NOT remove the remote log server from the network. In this instance it merely deselects the server as that particular log's remote log server.

5.8 Configuring Logs

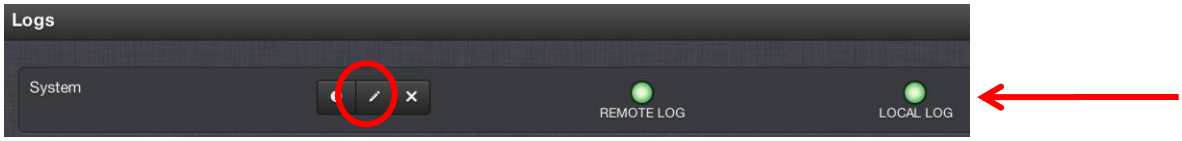
NOTE: The NTP log has no available configuration options.

To configure a log:

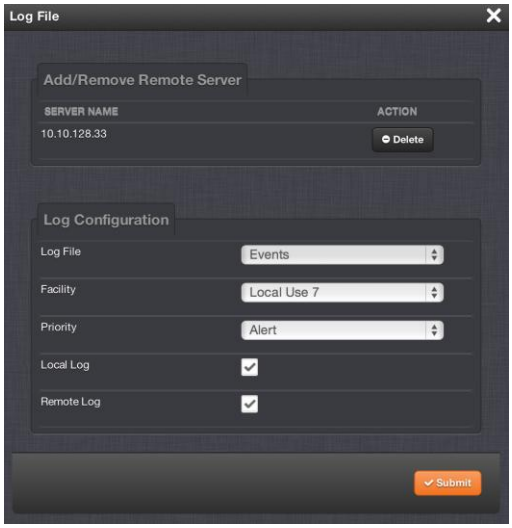
1. Navigate to the **Logs** page through **MANAGEMENT/OTHER/Log Configuration**.



2. In the **Logs** panel select the log you wish to configure and click on the  button.



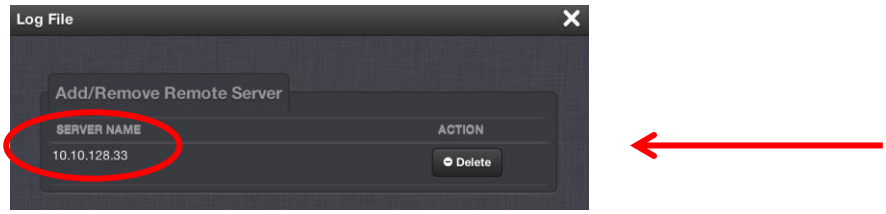
3. In the Log File window, fill in the available fields



The following log configuration options are available:

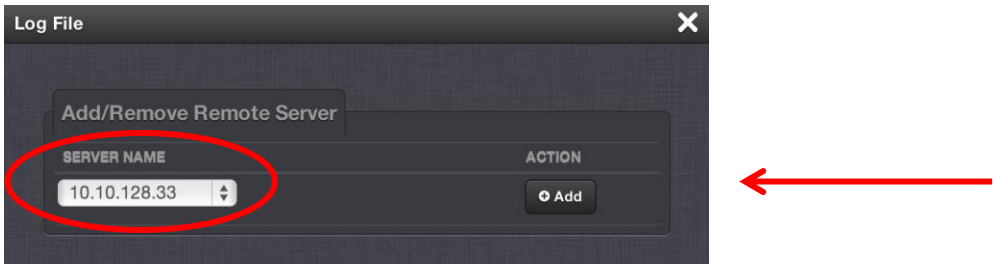
- **Add/Remove Remote Server**—The Syslog server(s) to which remote logs are sent. This panel is only available if **Remote Log** is checked in the **Log Configuration** panel.

  If the log has a remote log server to which it writes, the name of the server will appear here. Click **Delete** to remove the remote server.



NOTE: Clicking the **Delete** button in the **Log File** configuration window does NOT remove the remote log server from the network. In this instance it merely deselects the server as that particular log's remote log server.

If the log does not have a remote log server assigned, there will be a drop-down list of server choices. Click **Add** to add a remote server from the drop-down list.



If this list is empty, you will need to set up a remote log server in through the **Remote Log Server** panel. See **5.6 Adding Remote a Log Server**.

- **Log File**—Displays the name of the log file being configured.
- **Facility**—Value (defined by the Syslog server) to determine where the log is stored in the Syslog server. Set this value to match the scheme used by the remote server.
- **Priority**—Value (defined by the Syslog server) to determine where the log is stored in the Syslog server. Set this value to match the scheme used by the remote server.

  Important note about Facility and Priority values: In addition to configuring the log entries to be sent to a specific location in the Syslog server, the combination of these two values also determines which local log the entries are sent to inside the unit. Changing either or both of these values from the factory default values will alter which log the entries are sent to inside the unit. The table *Factory Default Facility and Priority Codes*, below, displays which Log Tab the log entries will be sent to (by default), based on the configuration of these two values.

If remote logging is not being used, the Facility and Priority values should not be changed from the default values. Altering these values can cause log entries that have similar values to be sent to the same log file (combining different types of log entries into one log). The factory default settings for the Facility and Priority configurations of all logs that can be sent to a Syslog server are as follows:

Log Tab Name	Facility	Priority
Event	Local Use 7	Alert
Alarms	Local Use 7	Critical
Oscillator	Local Use 7	Debug
GPS Qualification	Local Use 7	Warning
Journal	Local Use 7	Notice
Update	Local Use 7	Information
Timing	Local Use 7	Error
System	Local Use 7	Emergency

Factory Default Facility and Priority Codes

- **Local Log**—Enable or disable this particular log being stored inside the unit. When this box is checked, the log will be stored inside the unit.
- **Remote Log**—Configure the desired Syslog servers. When this box is checked, the particular log will be sent to a Syslog server.

In order for the logs to be formatted correctly for Syslog storage, all log entries are displayed using Syslog formatting. Each log entry contains the date and time of the event, the source of the log entry, and the log entry itself.

NOTE: The "time" of all log entries will be in UTC, Local, TAI or GPS time, as configured in the "Timescale" field that is located in the System Time Setup page.

5.8.1 System Log

Displays log entries related to the Timing system events and daemon events (such as the Alarms, Monitor, Notification, or SNMP daemons starting or stopping, etc.).

"Updating UTC-GPS Offset value from 0 to 16": UTC is being offset by this value to account for the time differences between the UTC and GPS timescales.

5.8.2 Events Log

Displays log entries related to GNSS reception status changes, Sync/Holdover state changes, SNMP traps being sent, etc. Details for example event log entries include the following:

"Reference Change": The unit has switched from one input reference to another (for example, IRIG was the selected input being used, but now GNSS is the selected reference).

"GPS Antenna Problem": The GPS Antenna Problem alarm indicates the GNSS receiver has detected an over-current or undercurrent condition (an open or short exists in the GNSS antenna cable, or the GNSS antenna is not connected to the unit). The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status. The current draw measurements that will indicate an antenna problem are:

- Under-current indication < 8 mA
- Over-current indication > 80 mA

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

"GPS Antenna OK": The antenna coax cable was just connected or an open or short in the antenna cable was being detected but is no longer being detected.

"Frequency Error": The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.

"Frequency Error cleared": The Frequency Error alarm was asserted but was then cleared.

"In Holdover": Input references were available, but all input references have since been lost. If the references are not restored before the Holdover period expires, time sync will be lost.

"No longer in Holdover": Input references were lost at one point (or declared not valid), but have since been restored OR the Input references were not restored before the Holdover period expired (Time Sync alarm is asserted).

"In Sync": The unit is synchronized to its Time and 1PPS inputs.

"Not In Sync": The unit is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.

"Sending trap for event 1 (SNMPSAD)": An SNMP trap was sent by the SNMP agent to the SNMP Manager. The event number in this entry indicates which SNMP trap was sent.

"The Unit has Rebooted": The unit was either rebooted or power cycled.

5.8.3 Alarms Log

Displays log entries for the Timing engine. Details for example entries include the following:

"The Unit has Rebooted": The unit was either rebooted or power cycled.

"In Holdover": Input references were available, but all input references have since been lost. If the references are not restored before the Holdover period expires, time sync will be lost.

"No longer in Holdover": Input references were lost at one point (or declared not valid), but have since been restored OR the Input references were not restored before the Holdover period expired (Time Sync alarm is asserted).

"In Sync": The unit is synchronized to its selected Time and 1PPS reference inputs.

"Not In Sync": The unit is not synchronized to its Time and 1PPS inputs and is not currently in Holdover. NTP will indicate to the network that it is Stratum 15 and so the time server likely be ignored as a time reference.

"Frequency Error": The oscillator's frequency was measured and the frequency error was too large. Or, the frequency couldn't be measured because a valid input reference was not available.

"Reference change": The unit has selected a different Time and 1PPS input reference for synchronization. Either the previously selected input reference was declared not valid (or was lost), so a lower priority reference (as defined by the Reference Priority Setup table) is now selected for synchronization OR a valid reference with higher priority than the previous reference is now selected for synchronization.

EXAMPLE: GNSS is the highest priority reference with IRIG input being a lower priority. The unit is synced to GNSS and so GNSS is the selected reference. The GNSS antenna is disconnected and IRIG becomes the selected reference. The Reference change entry is added to this log.

5.8.4 Timing Log

Displays log entries related to Input reference state changes (for example, IRIG input is not considered valid), antenna cable status.

"GR antenna fault": The GNSS Antenna Problem alarm indicates the GNSS receiver has detected an over-current or undercurrent condition (an open or short exists in the GNSS antenna cable, or the GNSS antenna is not connected to the unit). The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.

"GR antenna ok": The antenna coax cable was connected at this time or an open or short in the antenna cabling was occurring but is no longer being detected.

5.8.5 GPS Qualification Log

If the unit is connected to a GNSS antenna and is tracking satellites, this log contains a running hourly count of the number of GNSS satellites tracked each hour. This history data can be used

to determine if a GNSS reception problem exists and whether this is a continuous or intermittent reception issue.

GNSS reception may be displayed as cyclic in nature. A cyclic 12 hour pattern of decreased GNSS reception typically indicates that the GNSS antenna has an obstructed view of the horizon. The GNSS satellites are in a 12-hour orbit, so if part of the sky is blocked by large obstructions, at the same time every day (at approximately 12 hour intervals), the GNSS reception may be reduced or may vanish altogether. If this occurs, the antenna should be relocated to afford it an unobstructed view of the sky.

Every hour (displayed in the log as UTC time), the unit counts the total number of satellites that were tracked during that hour. The GNSS qualification log shows the number of satellites that were tracked followed by the number of seconds that the particular number of satellites were tracked during the hour (3600 seconds indicates a full hour). The number to the left of the "=" sign indicates the number of satellites tracked and the number to the right of the "=" sign indicates the number of seconds (out of a total of 3600 seconds in an hour) that the unit was tracking that number of satellites. For example, **"0=3600"** indicates the unit was tracking 0 satellites for the entire hour, while **"0=2700 1=900"** indicates the unit was tracking one satellite for 900 seconds, but for the remaining portion of the hour it was tracking zero satellites.

Every hourly entry in the log also contains a quality value, represented by "Q= xxxx" (where x can be any number from 0000 through 3600). The Qualification log records how many satellites were tracked over a given hour. If for every second of the hour a tracked satellite was in view, the Quality value will equal 3600. For every second the unit tracked less than the minimum number of satellites, the value will be less than 3600. The minimum requirement is one satellite at all times after the unit has completed the GNSS survey and indicates "Stationary". A minimum of four satellites are required in order for the GNSS survey to be initially completed.

If all entries in the qualification log are displayed as "0=3600", a constant GNSS reception problem exists, so the cause of the reception issue is continuous. If the unit occasionally shows 0=3600 but at other times shows that 1 through 12 have numbers of other than "0000", the reception is intermittent, so the cause of the reception issue is intermittent. If the Quality value normally equals 3600 but drops to lower than 3600 about every 12 hours, the issue is likely caused by the GNSS antenna having an obstructed view of the sky.

Example GPS Qualification Log Entry:

```
6 = 151 7 = 1894 8 = 480 9 = 534 10 = 433 12 = 108 Q = 3600
```

In this example, the unit tracked no less that 6 satellites for the entire hour. Out of the entire hour, it was tracking 6 satellites for a cumulative total of 151 seconds (not necessarily in a row). For the duration of the hour, it was tracking, 7, 8, 9, 10 and 12 satellites for a period of time. Because it was tracking at least at least one satellite for the entire hour, this Quality value is Q=3600.

NOTE: If the unit is not connected to a GNSS antenna, this log will remain empty.

5.8.6 Oscillator Log

Displays log entries related to oscillator disciplining. Provides the calculated frequency error periodically while synchronizing to a reference.

5.8.7 Journal Log

Displays log entries created for all configuration changes that have occurred (such as creating a new user account, for example).

5.8.8 Update Log

Displays log entries related to software updates that have been performed.

5.8.9 Authentication Log

Displays log entries for authentication events (e.g., unsuccessful login attempts, an incorrectly entered password, etc.) that are made to unit's command line interfaces (such as the front panel setup port, telnet, SSH, FTP, etc.).

5.8.10 NTP Log (Not configurable)

The NTP log displays operational information about the NTP daemon. Entries in this log include indications for when NTP was synchronized to its configured references (e.g., it became a Stratum 1 time server), stratum level of the NTP references, etc.

"Synchronized to (IP address), stratum=1": NTP is synchronizing to another Stratum 1 NTP server.

"ntp exiting on signal 15": This log entry indicates NTP is now indicating to the network that it is a Stratum 15 time server because it is not synchronized to its selected reference.

"Time reset xxxxx s": These entries indicate time corrections (in seconds) applied to NTP.

"No servers reachable": NTP can't locate any of its configured NTP servers.

"Synchronized to PPS(0), stratum=0": NTP is synchronized using the PPS reference clock driver (which provides more stable NTP synchronization).

Section 6: Software Upgrades & License Installation

6.1 Software Upgrades

Spectracom periodically releases new versions of software for NetClock as well as other products. Software updates are offered for free and made available for download from the Spectracom website.

To download software updates for your unit as they become available, please visit www.spectracomcorp.com, and from the website navigation menu select **Support/Software**. You can also register your email address to receive automatic notification of software updates. Refer to *2.12* **Product Registration** for information on registering.

Once an available software update has been downloaded from the Spectracom website, the update files can be transferred to the unit by:

- using a web browser via HTTPS on the **TOOLS/Upgrade/Backup** page.
- transferring the files via FTP or SCP/SFTP.
- from interactive logins like:
  - the serial port
  - telnet
  - SSH
  - an SNMP set

When using the web interface to transfer the files from a PC to the unit, the software update begins after the files have been transferred. If the files are manually transferred using FTP or SFTP, the update can be delayed until the next time the unit is either rebooted or power cycled. The update process occurs automatically with no user interaction required. The files are place in the **`/home/spectracom`** directory. Multiple files can be uploaded to the unit at one time.

To transfer the files using the web interface:

1. Go to www.spectracomcorp.com and from the website navigation menu select **Support/Software,** click on the appropriate NetClock link and follow the on-screen instructions for downloading the software.
2. Navigate to the **TOOLS/Upgrade/Backup** page.
3. Click on the **Update System Software** button in the **Actions** panel on the left side of the screen.
4. Click the **Choose File** button and navigate to the software update file you have downloaded.
5. Click **Upload**.

After the update file has been uploaded to the unit:

6. Click on the **Update System Software** button in the **Actions** panel on the left side of the screen.
7. Click the **Choose File** button and select to the software update file you have downloaded.
8. Click **Update**.

At this point, the system will be analyzed against the files in the update. Any system element with a newer version of software in the update file will be updated.

To “roll back” system elements to an earlier version, select the older Update file in the **Choose File** pull-down, select both **Update System** and **Force Update**, and click **Update**. All system elements will be “forced” to the version in the update file.

To delete a previously uploaded update file, select the file in the **Choose File** pull-down, select **Delete Update File**, and click **Submit**. Note that **Delete Update File** and **Update System** cannot be selected at the same time.

The unit will save system configurations across upgrades but will not save other information. In particular, update files may not be retained after a successful update.

All system elements will be forced to the versions in the update file, and all configuration information will be erased as part of the update.

The versions of software currently installed in unit can be found on the **TOOLS/Upgrade/Backup** page. This page displays the software versions for the main unit as well as the versions of software for any installed option modules.

6.2 License Installation

Any software options available for the unit have to be enabled by a license installation on the product. The license installation is made in the same way as a software upgrade. A file has to be uploaded into the product and then installed.

License files are archive files with a **`tar.gz`** extension. They may contain multiple licenses for multiple products.

1. Receiver the file from Spectracom.
2. Click on the **Apply License File** button in the **Actions** panel on the left side of the screen.
3. Click the **Choose File** button and navigate to the software update file you have downloaded.
4. Click **Upload**.

Section 7: Day-to-Day Operation

Operation of the unit is relatively intuitive and requires little operator intervention during normal network activities.

7.1 Leap Second Occurrence

7.1.1 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 UTC time in sync with the earth's rotation.

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

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

NOTE: Leap seconds only apply to the "UTC" and "Local" timescales. Leap seconds do not affect the "GPS" and "TAI" timescales. However, a leap second event will change the GPS to UTC and TAI to UTC offsets. When a leap second occurs, the unit will automatically change these offsets by the proper amount, no matter which timescale is currently being used by the system.

The unit can be alerted of impending leap seconds by any of the following methods:

- GNSS Receiver (if available as an input reference)—The GNSS satellite system transmits information regarding a Leap second adjustment at a specific Time and Date an arbitrary number of months in advance.
- Input references other than GNSS—Some of the other available input references also contain pending Leap Second notification in the data streams that can be read by the unit.
- Manual user input—the unit can be manually configured by a user with the date/time of the next pending leap second. On this date/time, the System Time will automatically correct for the leap second (unless the System Time's timescale is configured as either GPS or TAI).

7.1.2 Leap Second Alert Notification

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

1. Data Formats 2 and 7 available from the ASCII Data option modules 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 unit 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.

7.1.3 Sequence of a Leap Second Correction Being Applied

The following is the time output sequence that the unit 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 …

Section 8: NetClock 9483 Option Modules

Spectracom offers several configurations for the NetClock 9483. This section contains technical details and specifications for option module cards that may have been selected at the time of purchase, and information regarding configuration and usage that can be used after installation.

Option Name	Module / PN	Description	Refer to Section
NENA	**1209-1F**	NENA-Compliant Option Module	*8.1*
Option 16	**1209-06**	Gigabit Ethernet (3X, 10/100/1000BaseT)	*8.2*
Option 13	**1209-0A**	T1 / E1 – (100 /120 Ω)	*8.3*
Option 12	**1209-12**	Precision Time Protocol (PTP) Input / Output	*8.4*

NOTE: Contact sales@spectracomcorp.com for general inquiries regarding option module card functionality or availability. If you do not have a NetClock 9483 product that already shipped preconfigured with specific option module cards, or if you have purchased new option cards for your NetClock 9483, review the "*NetClock 9483 Option Card Installation Guide*" document for detailed option card installation steps.

8.1 NENA-Compliant Option Module

The NetClock 9483's NENA-Compliant option module provides IRIG support (including support for all NENA formats), ASCII RS-232 timecode support, as well as ASCII RS-485 timecode and relay / alarms.

8.1.1 NENA Option Module Specifications

Outputs:	**(1) IRIG B/E, IEEE 1344/C37.118-2005 (AM/TTL) output**	**(1) ASCII RS-232 output**	**(1) ASCII RS-485**	**(2) Relay/Alarm outputs**
Connector:	BNC (J1)	DB9F (J2)	3.81mm Terminal block (J3)	
Accuracy:	+/- 20 microseconds to +/- 200 microseconds of UTC, format dependant	+/- 100-1000 microseconds (format dependant)	+/- 100-1000 microseconds (format dependant)	Switch time 4 msec, max.

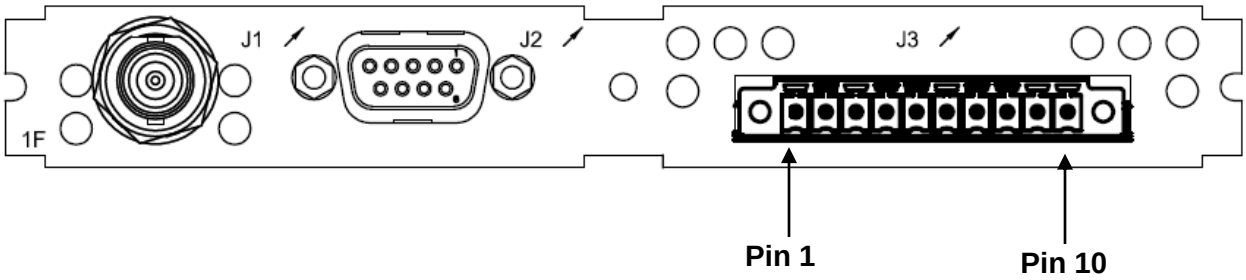


Figure 8-1: Model 1204-1F: NENA-Compliant Option Card Rear Plate

IRIG Output Specifications

AM IRIG Output:

- Output impedance: 50 Ω nominal
- Amplitude (adjustable): 500mV p-p min, 6V p-p max into 50 Ω
  1V p-p min, 12V p-p max into > 600 Ω
- AM Carrier:
  - IRIG A – 10KHz
  - IRIG B – 1KHz
  - IRIG E – 100Hz, 1KHz
  - IRIG G – 100 KHz
- Modulation Ratio: 3.3:1 nominal

DCLS IRIG Output:

- Signal Level: 0V to 4.3V (TTL compatible) into 50 Ω

- Output impedance of buffer is ~7 to 10 Ω

ASCII RS-232 Specification

Outputs:	+/- 5VDC minimum, +/- 5.4 VDC typical
Signal Type and Connector:	RS-232 DB9F

RS-232 TX Port:

- RS-232 Input
  - -25VDC to +25VDC
  - +0.6V $V_{IL\ min}$, +1.2V $V_{IL\ TYP}$
  - +1.5V $V_{IH\ TYP}$, +2.4V $V_{IH\ MAX}$
  - Input Impedance >3k Ω
- RS-232 Output
  - +/- 5VDC minimum
  - +/- 5.4 VDC typical
  - Output Impedance 300 Ω, minimum
  - -13.2VDC to +13.2VDC
- 1PPS Output
  - Signal Level: 0V to 4.3V (TTL compatible) into 50 Ω
    - Output impedance of buffer is ~7 to 10 Ω
  - Rise/fall times of ~20nsec.

Pin Assignments

NOTE: In the following tables, pin number assignments are defined starting with Pin 1 to Pin 10, arranged from left to right, respectively.

Pin Number	Signal Name	Function
Top row of 5 pins		
1	PPS_OUT	1PPS output
2	SERIAL_OUT_TX	RS-232 Transmit data
3	SERIAL_OUT_RX	RS-232 Receive data
4	NC	No connection
5	GND	Ground
Bottom row of 4 pins		
6	NC	No connection
7	NC	No connection
8	NC	No connection
9	NC	No connection

Table 8-1: ASCII RS-232 Output Connector Pin Assignment

ASCII RS-485 Specifications

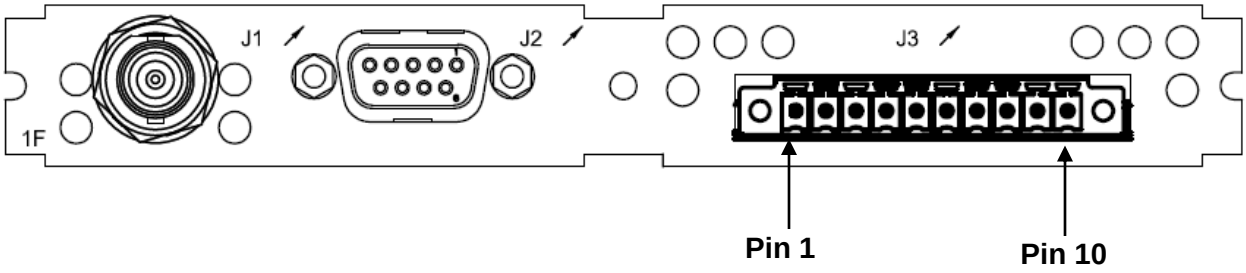
Inputs / Outputs:	(2) Two contact relay connections (NC, common, NO)
Signal Type and Connector:	Terminal block Contacts Switch under max. load of 30VDC, 2A Contacts rated to switch 220VDC Breakdown voltage of 1000VDC between contacts Switch time 4 msec, max.

RS-485 TX Output:

- RS-485 Differential Output
    - +1.65V Typical Common Mode Output Voltage
    - 2V min Differential Output Voltage Swing with 100 Ω load, 3.3V Differential Output Voltage Swing, No Load, with ESD protection

Pin Assignments

NOTE: In the following table, pin numbers are defined starting with Pin 1 to Pin 10, arranged from left to right, respectively.



Connector Pin	Signal	Direction	Characteristics
1	RS-485 TX+	Out	0V to 3VDC differential, 120 Ω load
2	RS-485 TX-	Out	0V to 3VDC differential, 120 Ω load
3	GROUND	N/A	GROUND
4	Relay 1 NO	Out	Normally Open 30VDC, 2A max. Switching Power
5	Relay 1 NC	Out	Normally Closed 30VDC, 2A max. Switching Power
6	Relay 1 COMMON	Out	Common Contact 30VDC, 2A max. Switching Power
7	Relay 2 NO	Out	Normally Open 30VDC, 2A max. Switching Power
8	Relay 2 NC	Out	Normally Closed 30VDC, 2A max. Switching Power
9	Relay 2 COMMON	Out	Common Contact 30VDC, 2A max. Switching Power
10	GROUND	N/A	GROUND

Figure 8-2: Relay / RS-485 Outputs Pin Assignment

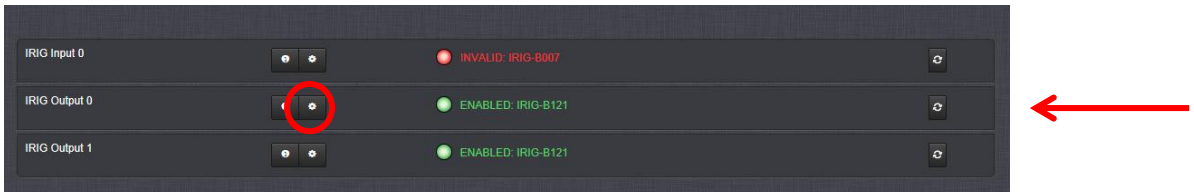
NOTE: The last device on each of the RS-485 remote output should be terminated into 120 Ω. Auxiliary Spectracom equipment (such as wall display clocks) include a 120 Ω resistor for termination.

8.1.2 IRIG and ASCII RS-232 Timecode Output Setup

To configure the IRIG output and ASCII RS-232 Timecode options, navigate to the **Setup / Outputs** page and select the Slot labeled "**SLOT 1** (**IRIG ASCII**)". Options can be set from both the **IRIG** and **ASCII RS-232** tabs, detailed in this section.

Configuring IRIG output

1. Navigate to the **IRIG OUT BNC** entry through the **INTERFACES/OPTION CARDS** drop-down menu.
2. The **IRIG OUT BNC** window will appear.



3. Click on the  button in the **IRIG Output** row for the IRIG output you wish to configure.

NOTE: If you have only one input or output of any type, the unit will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

4. The **IRIG Output** screen will display.

5. Populate the fields as desired. The available fields are:

Signature Control: Used to control when the IRIG modulation will be present. This function allows the modulation to stop in certain situations.

> **Output Always Enabled:** IRIG time code modulation is present, even when NetClock is not synchronized to its references.
>
> **Output Enabled in Holdover:** IRIG time code modulation is present unless the NetClock is not synchronized to its references (Modulation is present while in the Holdover mode).

Output Disabled in Holdover: IRIG time code modulation is present unless the NetClock references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No IRIG output modulation is present, even if any NetClock input references are present and considered qualified.

Format: Defines the desired IRIG output formatting. Available options include: IRIG A, B, G, NASA-36, IRIG E (100 Hz or 1 kHz)

Modulation: Changes the type of output signal modulation:

- **IRIG AM** is an amplitude modulated output. The amplitude of the output is determined by the value entered in the "Amplitude" field.
- **IRIG DCLS** is a TTL modulated output.

Coded Expression: Defines the data structure of the IRIG signal, where:

BCD = Binary Coded Decimal
TOY = Time of Year
CF = Control Field
SBS = Straight Binary Seconds

Control Field: IRIG signals have an optional section in the data stream that can be used to include additional information (such as the present year, for example). This field allows the Control Field section of the IRIG output to be defined. The available configurations are as follows:

RCC-2004: IRIG spec 200-04 specified a location for year value, if included in this field.
IEE 1344 (C37.118-2005): IRIG B format with extensions. Control Field contains year, Leap Second and DST information.
Spectracom Format: Year is included in Control Field but not in the same location as RCC-2004 output (year is offset by one position).
Spectracom FAA Format: A unique IRIG output Control Field that contains satellite lock status and time error flags.
NASA: A variant of IRIG B.

Time Scale: Used to select the time base for the output IRIG data stream. The available choices are **UTC**, **TAI** (Temps Atomique International), **GPS** and **Local**. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GPS satellites (as of September, 2013, this is currently 16 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set up on the **Setup / Time Management** page. (Refer to the *"Configuring the System Time Timescale"* section for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: System Time may be configured as UTC time, but it might be desired to output the IRIG time as local time instead. With the Timescale field set to "Local", select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the IRIG output data stream. Refer to Section *3.13.3* for more information on Local Clocks.

Amplitude: The peak-to-peak output voltage level into a 600 Ω load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. The value of 128 will cause the Mark amplitude to be about 5vp-p into high impedance. A value of 200 results in an output amplitude of about 9vp-p into high impedance.

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

Offset: Provides the ability to account for IRIG cable delays or other latencies in the IRIG input. The Offset value is entered and displayed in nanoseconds (ns). The available Offset range is -500 to +500 ms.

Each IRIG code specifies a carrier frequency that is modulated to encode date and time, as well as control bits to time-stamp events. Initially, IRIG applications were primarily military and government associated. Today, IRIG is commonly used to synchronize voice loggers, recall recorders, and sequential event loggers found in emergency dispatch centers and power utilities.

Format	Encoding	Modulation	Carrier	Coded Expressions	Bit rate	Time Frame Interval
IRIG-A	A000	DCLS	N/A	BCD_{TOY}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A001	DCLS	N/A	BCD_{TOY}, CF	1000 pps	0.1 sec
IRIG-A	A002	DCLS	N/A	BCD_{TOY}	1000 pps	0.1 sec
IRIG-A	A003	DCLS	N/A	BCD_{TOY}, SBS	1000 pps	0.1 sec
IRIG-A	A004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	1000 pps	0.1 sec
IRIG-A	A006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec
IRIG-A	A007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	1000 pps	0.1 sec
IRIG-A	A130	AM	10 kHz	BCD_{TOY}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A131	AM	10 kHz	BCD_{TOY}, CF	1000 pps	0.1 sec
IRIG-A	A132	AM	10 kHz	BCD_{TOY}	1000 pps	0.1 sec
IRIG-A	A133	AM	10 kHz	BCD_{TOY}, SBS	1000 pps	0.1 sec
IRIG-A	A134	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	1000 pps	0.1 sec
IRIG-A	A135	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	1000 pps	0.1 sec
IRIG-A	A136	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}	1000 pps	0.1 sec
IRIG-A	A137	AM	10 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	1000 pps	0.1 sec
IRIG-B	B000	DCLS	N/A	BCD_{TOY}, CF and SBS	100 pps	1 sec
IRIG-B	B001	DCLS	N/A	BCD_{TOY}, CF	100 pps	1 sec
IRIG-B	B002	DCLS	N/A	BCD_{TOY}	100 pps	1 sec
IRIG-B	B003	DCLS	N/A	BCD_{TOY}, SBS	100 pps	1 sec
IRIG-B	B004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and	100 pps	1 sec

				SBS		
IRIG-B	B005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	100 pps	1 sec
IRIG-B	B006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	100 pps	1 sec
IRIG-B	B007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	100 pps	1 sec
IRIG-B	B120	AM	1 kHz	BCD_{TOY}, CF and SBS	100 pps	1 sec
IRIG-B	B121	AM	1 kHz	BCD_{TOY}, CF	100 pps	1 sec
IRIG-B	B122	AM	1 kHz	BCD_{TOY}	100 pps	1 sec
IRIG-B	B123	AM	1 kHz	BCD_{TOY}, SBS	100 pps	1 sec
IRIG-B	B124	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	100 pps	1 sec
IRIG-B	B125	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	100 pps	1 sec
IRIG-B	B126	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}	100 pps	1 sec
IRIG-B	B127	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	100 pps	1 sec
IRIG-E	E000	DCLS	N/A	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E001	DCLS	N/A	BCD_{TOY}, CF	10 pps	1 sec
IRIG-E	E002	DCLS	N/A	BCD_{TOY}	10 pps	1 sec
IRIG-E	E003	DCLS	N/A	BCD_{TOY}, SBS	10 pps	1 sec
IRIG-E	E004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	1 sec
IRIG-E	E005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	1 sec
IRIG-E	E006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	10 pps	1 sec
IRIG-E	E007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	1 sec
IRIG-E	E110	AM	100 Hz	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E111	AM	100 Hz	BCD_{TOY}, CF	10 pps	1 sec
IRIG-E	E112	AM	100 Hz	BCD_{TOY}	10 pps	1 sec
IRIG-E	E113	AM	100 Hz	BCD_{TOY}, SBS	10 pps	1 sec
IRIG-E	E114	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	1 sec
IRIG-E	E115	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	1 sec
IRIG-E	E116	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}	10 pps	1 sec
IRIG-E	E117	AM	100 Hz	BCD_{TOY}, BCD_{YEAR}, and SBS	10 pps	1 sec
IRIG-E	E120	AM	100 Hz	BCD_{TOY}, CF and SBS	10 pps	1 sec
IRIG-E	E121	AM	1 kHz	BCD_{TOY}, CF	10 pps	10 sec
IRIG-E	E122	AM	1 kHz	BCD_{TOY}	10 pps	10 sec
IRIG-E	E123	AM	1 kHz	BCD_{TOY}, SBS	10 pps	10 sec
IRIG-E	E124	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10 pps	10 sec
IRIG-E	E125	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10 pps	10 sec
IRIG-E	E126	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}	10 pps	10 sec
IRIG-E	E127	AM	1 kHz	BCD_{TOY}, BCD_{YEAR}, and	10 pps	10 sec

				SBS		
IRIG-G	G000	DCLS	N/A	BCD_{TOY}, CF and SBS	10000 pps	10 msec
IRIG-G	G001	DCLS	N/A	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G002	DCLS	N/A	BCD_{TOY}	10000 pps	10 msec
IRIG-G	G003	DCLS	N/A	BCD_{TOY}, SBS	10000 pps	10 msec
IRIG-G	G004	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10000 pps	10 msec
IRIG-G	G005	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and CF	10000 pps	10 msec
IRIG-G	G006	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}	10000 pps	10 msec
IRIG-G	G007	DCLS	N/A	BCD_{TOY}, BCD_{YEAR}, and SBS	10000 pps	10 msec
IRIG-G	G140	AM	100 kHz	BCD_{TOY}, CF and SBS	10000 pps	10 msec
IRIG-G	G141	AM	100 kHz	BCD_{TOY}, CF	10000 pps	10 msec
IRIG-G	G142	AM	100 kHz	BCD_{TOY}	10000 pps	10 msec
IRIG-G	G143	AM	100 kHz	BCD_{TOY}, SBS	10000 pps	10 msec
IRIG-G	G144	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, CF and SBS	10000 pps	10 msec
IRIG-G	G145	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, and CF	10000 pps	10 msec
IRIG-G	G146	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}	10000 pps	10 msec
IRIG-G	G147	AM	100 kHz	BCD_{TOY}, BCD_{YEAR}, and SBS	10000 pps	10 msec
NASA-36	NA	AM	1msec	UNKNOWN	100 pps	1 sec
NASA-36	NA	DCLS	10msec	UNKNOWN	100 pps	1 sec

Table 8-2: Available IRIG Output Signals

NOTE: The Spectracom IRIG formats use the control functions for BCD year information and a Time Sync Status bit and in format E the control functions are used for straight binary seconds (SBS). Refer to individual IRIG Time Code description figures and text. IRIG Standard 200-98 format B had 27 control bits and format E had 45 bits for control functions. These control bits could be used for any use and there was no defined function. Spectracom used the control function element at index count 55 as the TIME SYNC STATUS and the sub-frame after position identifiers P6 and P7 as the year info and for format E the sub-frame after P8 and P9 for the straight binary seconds (SBS). The position of the BCD year information does not conform to the newer IRIG Standard 200-04. IRIG Standard 200-04 incorporated the year information after P5 and reduced the allocated control bits to 18 for format B and 36 for format E.

NOTE: DCLS is DC Level Shifted output, pulse width modulated with a position identifier having a positive pulse width equal to 0.8 of the reciprocal of the bit rate, a binary one (1) having a positive pulse width equal to 0.5 of the reciprocal of the bit rate and a binary zero (0) having a positive pulse width equal to 0.2 of the reciprocal of the bite rate.

The NetClock can provide IRIG A, IRIG B, IRIG E and IRIG G code in amplitude modulated (AM) or pulse width coded (TTL) formats. A signature control feature may be enabled for any IRIG output. Signature control removes the modulation code when a Time Sync Alarm is asserted.

For reference, detailed information about the IRIG B and IRIG E formats follows.

IRIG B Output

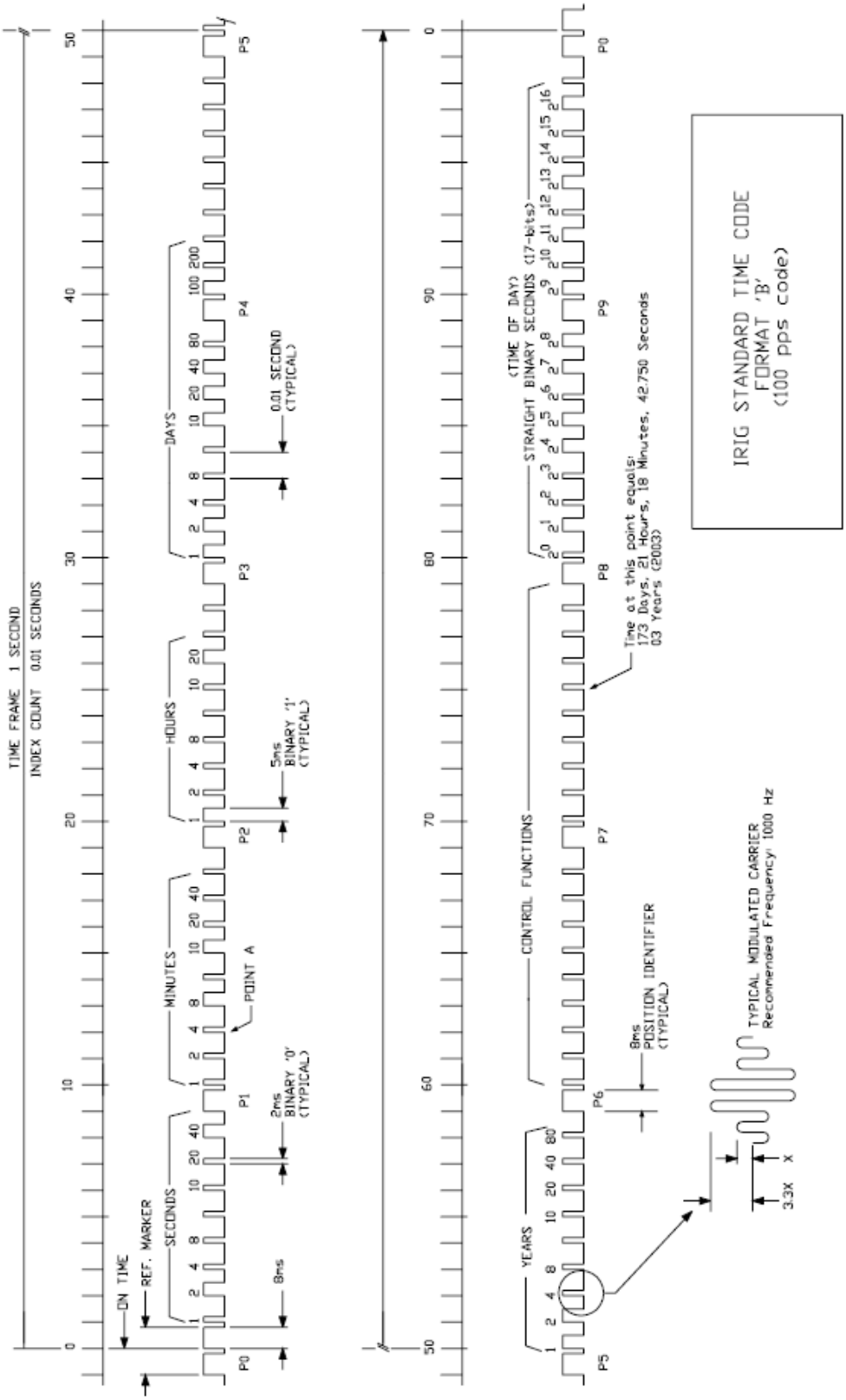


Figure 8-3: IRIG B Time Code Description

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

Time frame: 1.0 seconds.

Code digit weighting:

Binary Coded Decimal time-of-year.
Code word - 30 binary digits.
Seconds, minutes hours, and days.
Recycles yearly.

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

Code word structure:

BCD: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P0 and P5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

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

Table 8-3 lists the Control Function Field and each element's function.

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

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

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

Pulse rates:

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

Element identification: The "on time" reference point for all elements is the pulse leading edge.

Index marker (Binary 0 or uncoded element): 2 millisecond duration.
Code digit (Binary 1): 5 millisecond duration.
Position identifier: 8 millisecond duration.

Reference marker, 1 per second. The reference marker appears as two consecutive position identifiers. The second position identifier marks the on-time point for the succeeding code word.

Resolution:

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

Carrier frequency: 1 kHz when modulated.

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

Table 8-3: IRIG B Control Function Field

IRIG E Output

The IRIG E code contains the Binary Coded Decimal (BCD) time of year and Control Functions. Figure 8-11 illustrates the IRIG E data structure. The BCD time of year provides the day of year, 1-366, and time of day to tens of seconds. The hour of the day is expressed in 24 hour format. The Control Function field includes a time synchronization status bit, year information and SBS time of day.

Time frame: 10 seconds.

Code Digit Weighting:

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

Code Word Structure: BCD word tens of seconds digits begin at index count 6. Binary coded elements occur between position identifier elements P0 and P5 (3 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

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

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

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

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

Pulse rates:

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

Element identification: The "on time" reference point for all elements is the pulse leading edge.

Index marker (Binary 0 or uncoded element): 20 millisecond duration.
Code digit (Binary 1): 50 millisecond duration.
Position identifier: 80 millisecond duration.

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

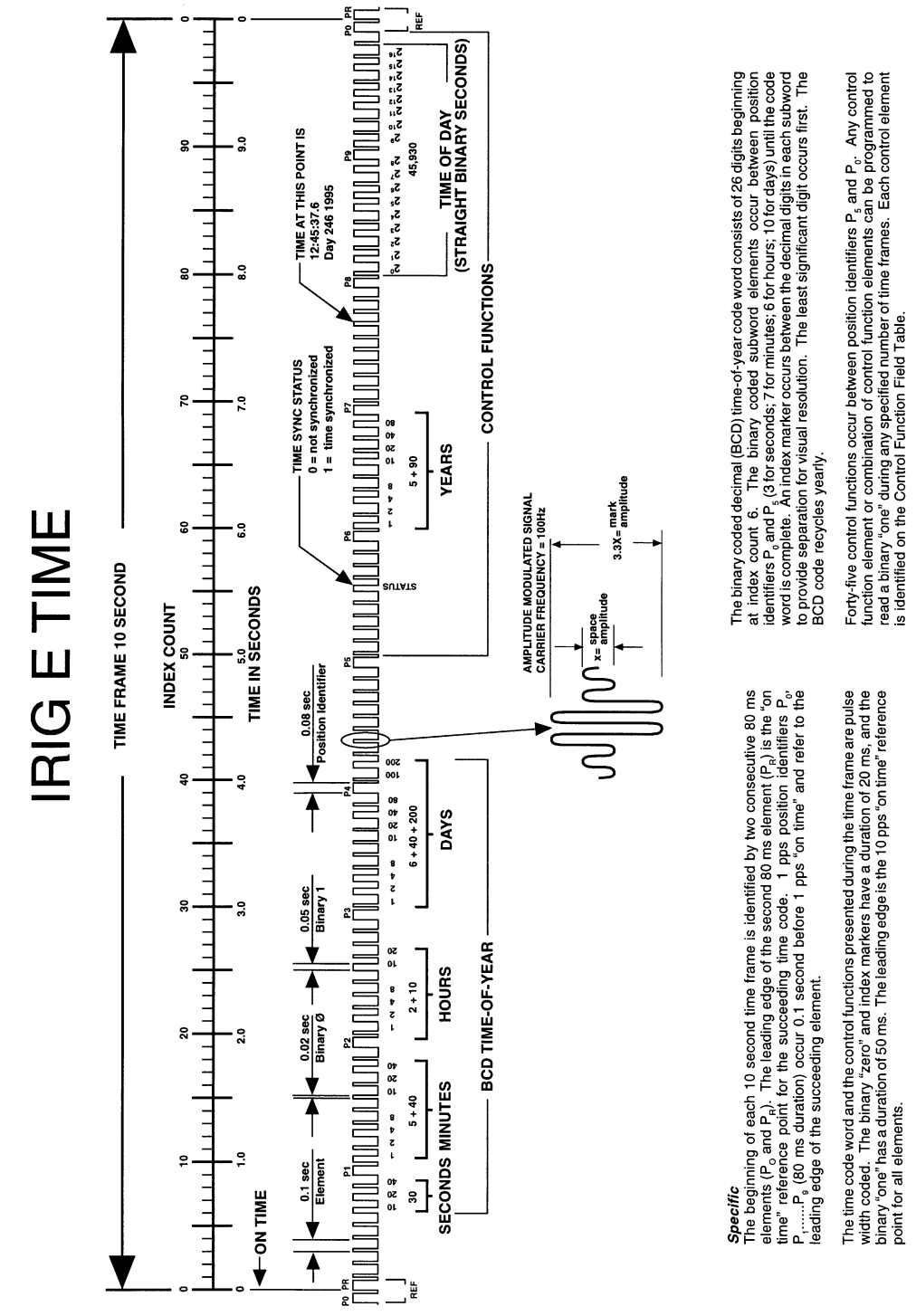


Figure 8-4: IRIG E Time Code Description

BIT #	*CF ELEMENT #*	*FUNCTION*		
50	1	SPACE		
51	2	SPACE		
52	3	SPACE		
53	4	SPACE		
54	5	SPACE		
55	6	TIME	SYNC	STATUS
56	7	SPACE		
57	8	SPACE		
58	9	SPACE		
59	PID P6	POSITION		IDENTIFIER
60	10	YEAR	UNITS	Y1
61	11	YEAR	UNITS	Y2
62	12	YEAR	UNITS	Y4
63	13	YEAR	UNITS	Y8
64	14	SPACE		
65	15	YEAR	TENS	Y10
66	16	YEAR	TENS	Y20
67	17	YEAR	TENS	Y40
68	18	YEAR	TENS	Y80
69	PID P7	POSITION		IDENTIFIER
70	19	SPACE		
71	20	SPACE		
72	21	SPACE		
73	22	SPACE		
74	23	SPACE		
75	24	SPACE		
76	25	SPACE		
77	26	SPACE		
78	27	SPACE		
79	PID P8	POSITION		IDENTIFIER
80	28	SBS		2^0
81	29	SBS		2^1
82	30	SBS		2^2
83	31	SBS		2^3
84	32	SBS		2^4
85	33	SBS		2^5
86	34	SBS		2^6
87	35	SBS		2^7
88	36	SBS		2^8
89	PID P9	POSITION		IDENTIFIER
90	37	SBS		2^9
91	38	SBS		2^{10}
92	39	SBS		2^{11}
93	40	SBS		2^{12}
94	41	SBS		2^{13}
95	42	SBS		2^{14}
96	43	SBS		2^{15}
97	44	SBS		2^{16}
98	45	SPACE		
99	PID P0	POSITION IDENTIFIER		

Table 8-4: IRIG E Control Function Field

Configuring the ASCII Time Code Output (RS-232 or RS-485)

NOTE: The process of configuring the ASCII Time Code output is independent of the communications protocol.

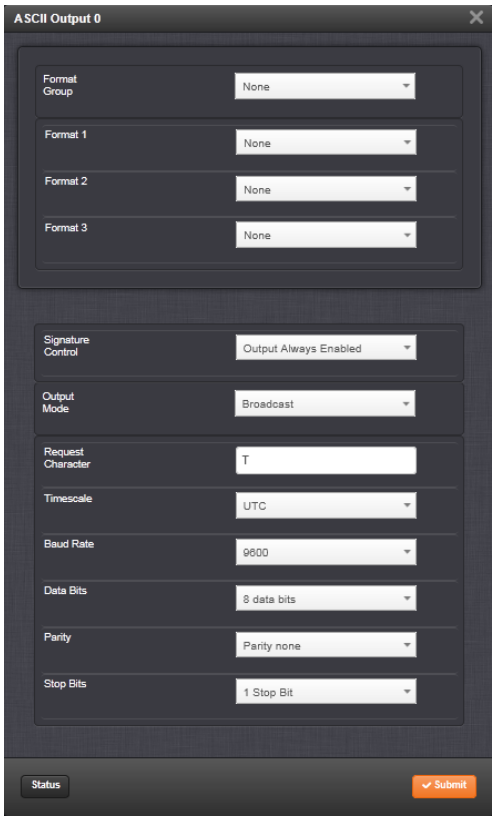
To configure any ASCII data output port:

1. Navigate to the **ASCII TIMECODE** entry through the **INTERFACES/OPTION CARDS** drop-down menu.
2. The **ASCII TIMECODE** window will appear.

3. Click on the  button in the **ASCII Input 0** row.

NOTE: If you have only one input or output of any type, the unit will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

4. The **ASCII Output 0** edit window will display.



- **Format Group:** Configures the message format type. Choices are:
  - Auto
  - Spectracom
  - NMEA
  - ICD-153
  - EndRun

  The choice of format group determines the format choices available in the **Format 1, Format 2** and **Format 3** fields.

Format 1: Selects either the first of up to three or the only format message to be outputted. Refer to Section 13: for a description of available formats.

Format 2: Selects the second consecutive format message to be outputted. Select “None” if only one output format is desired. Refer to Section 13: for a description of available formats.

Format 3: Selects the third consecutive format message to be outputted. Select “None” if only one output format is desired. Refer to Section 13: for a description of available formats.

Signature Control: Used to control when the ASCII modulation will be present. This function allows the modulation to stop in certain situations.

No Signature Control: The ASCII data input is present, even when NetClock is not synchronized to its references.

Output Always Enabled: ASCII time code modulation is present, even when NetClock is not synchronized to its references.

Output Enabled in Holdover: ASCII time code modulation is present unless the NetClock is not synchronized to its references (Modulation is present while in the Holdover mode).

Output Disabled in Holdover: ASCII time code modulation is present unless the NetClock references are considered not qualified and invalid. (Modulation is not present while in the Holdover mode).

Output Always Disabled: No ASCII output modulation is present, even if any NetClock input references are present and considered qualified.

Mode: This field determines when the output data will be provided. The available Mode selections are as follows:

Broadcast: The format messages are automatically sent out on authorized condition (Signature control), every second a message is generated in sync with the 1PPS.

Request (On-time): A format message is generated in sync with 1PPS after the configured request character has been received.

Request (Immediate): A format message is generated as soon as the request character is received. As this selection does not correlate the output data to the on-time point for the message, in Data Formats that do not provide sub-second information (such as Formats 0 and 1 whereas Format 2 provides sub-second information), it should be noted that the output data can be provided immediately, but a time error could occur when using the on-time point of the message in addition to the data for timing applications.

Time Scale: Used to select the time base for the incoming IRIG data. The entered Timescale is used by the system to convert the time in the incoming data stream to UTC time for use by the System Time.

The available choices are **UTC**, **TAI** (Temps Atomique International), **GPS** and **Local**. UTC is also referred to as ZULU time. GPS is the raw GPS time as transmitted by the GPS satellites (as of 2011, this is currently 15 seconds ahead of UTC time). If GPS or TAI time is used, then the proper timescale offsets must be set on the **Setup / Time Management** page. (Please refer to Section *3.13.1* for more information). Local timescale allows a Local Clock to apply a time offset for Time Zone and DST correction.

Local Clock: The incoming IRIG input time information may be provided as local time, but System Time may be configured as UTC time, so internal computations need to be performed. With the Timescale field set to “Local”, select the name of a previously created Local Clock. The Time Zone and DST rules, as configured in the Local Clock will be applied to the front panel time display. Refer to Section *3.13.3* for more information on Local Clocks.

Request character: This field defines the character that NetClock needs to receive in order for a one-time output data stream to be provided.

Baud Rate: Determines the speed that the output port will operate at.

Data Bits: Defines the number of Data Bits for the output port.

Parity: Configures the parity checking of the output port.

Stop Bits: Defines the number of Stop Bits for the output.

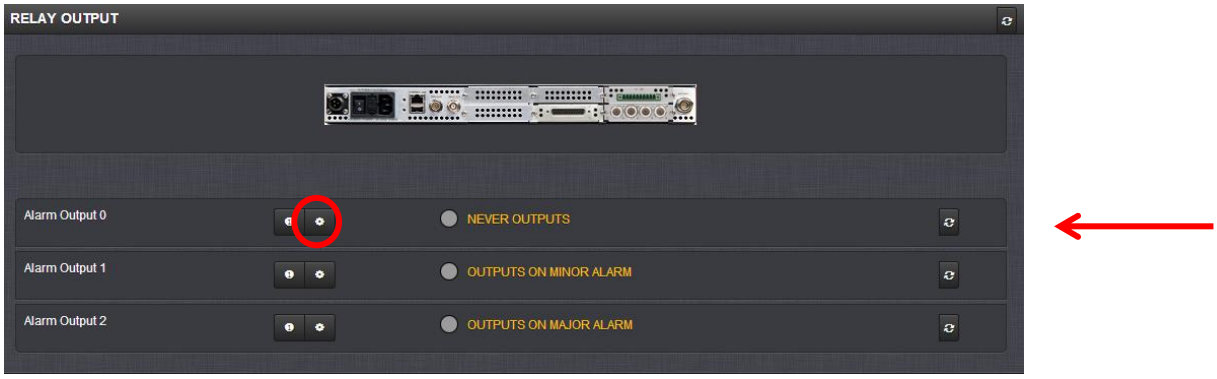
Configuring the Relay Output

To manage the alarm relays:

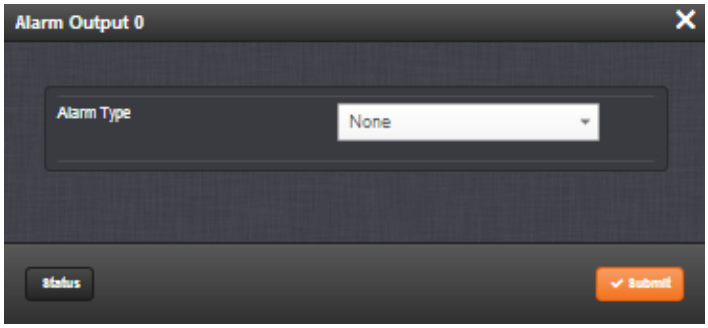
1. Navigate to the **Relay Output** entry for the card you wish to configure through the **INTERFACES HAVEQUICK OUT /OPTION CARDS** drop-down menu.

NOTE: The relay output can also be accessed as **Alarm Output** under **INTERFACES/OUTPUTS**.

2. The **Relay Output** window will appear.



3. Click on the  button in the **Alarm Output** row for the output you wish to configure.
4. The **Alarm Output** window will display.



5. Choose one of the following options from the drop-down list:
   - **None**—Will not output for an alarm.
   - **Minor**—Will output on a minor alarm.
   - **Major**—Will output on a major alarm.

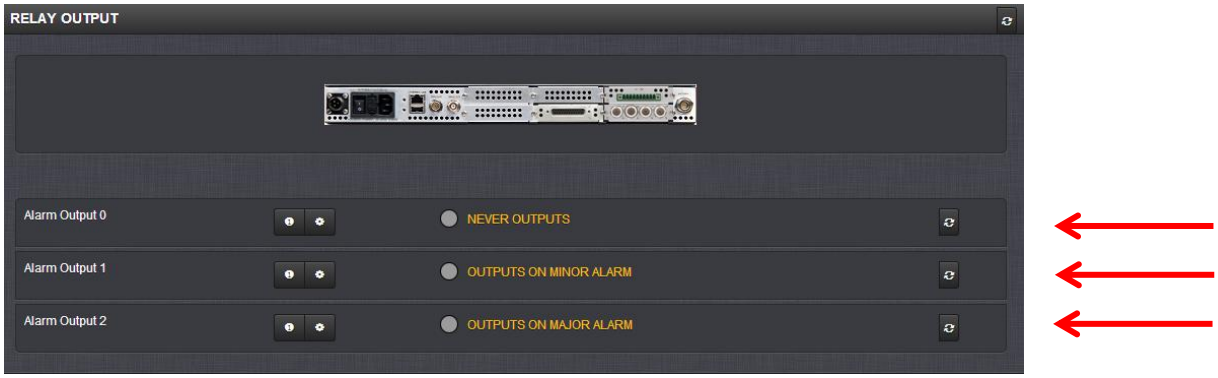
8.1.3 Viewing the Relay Output

To view the status of the alarm outputs:

1. Navigate to the **Relay Output** entry for the card you wish to configure through the **INTERFACES HAVEQUICK OUT /OPTION CARDS** drop-down menu.

NOTE: The relay output can also be accessed as **Alarm Output** under **INTERFACES/OUTPUTS**.

2. The **Relay Output** window will appear.



1. Each alarm will show one of 3 options:
   - **NEVER OUTPUTS**
   - **OUTPUTS ON MINOR ALARM**
   - **OUTPUTS ON MAJOR ALARM**

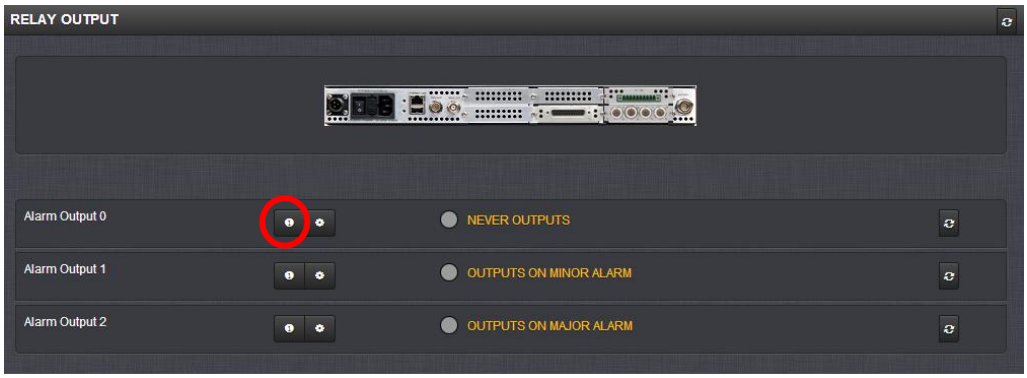
8.1.4 Viewing the Relay Output Settings

To view the settings of each output:

1. Navigate to the **Relay Output** entry for the card you wish to configure through the **INTERFACES HAVEQUICK OUT /OPTION CARDS** drop-down menu.

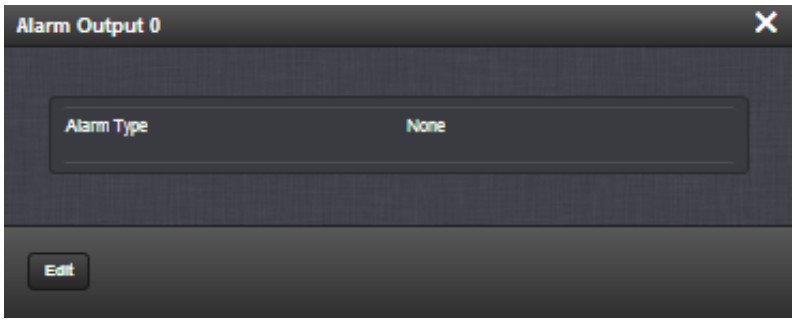
NOTE: The relay output can also be accessed as **Alarm Output** under **INTERFACES/OUTPUTS**.

2. The **Relay Output** window will appear.



3. Click on the  button in the **Alarm Output** row for the output for which you wish to see the settings.

4. The **Alarm Output** window will display.



5. Each alarm will show one of 3 options:
   - **OUTPUTS ON MAJOR ALARM**
   - **OUTPUTS ON MINOR ALARM**
   - **NEVER OUTPUTS**

8.2 Model 1209-06: Multi-Port Gigabit Ethernet (3X) Module

Inputs / Outputs:	(3) Gigabit Ethernet (10/100/1000 Base-T)
Signal Type and Connector:	RJ-45
Management:	Enabled or Disabled (NTP server only)
Maximum Number of Cards:	1
Ordering Information:	1209-06: Gigabit Ethernet (3X) Module (configured through the **Network / Interfaces** page of NetClock web interface)

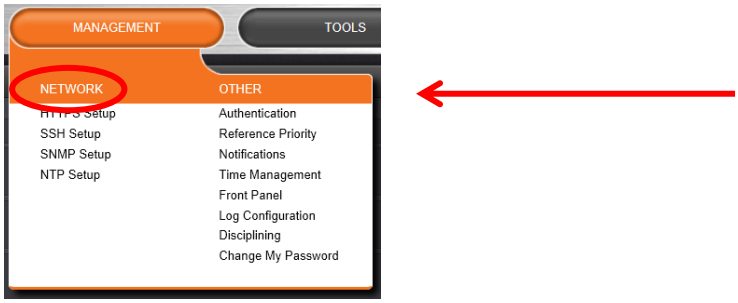
1204-06 Option Module Card Rear Plate

This option module card adds three (3) 10/100/1000-base-T network interfaces in addition to the standard 10/100-base-T network interface.

8.2.1 Accessing the Network Management Screen

In order to monitor and manage any of the Ethernet ports:

1. Navigate to the **Network Management** screen through **MANAGEMENT/NETWORK**.



2. The **Network Management** screen will display. The **Ports** panel will show the Ethernet ports you have available and their connection status.

The **eth0** port is the built-in Ethernet port. The **eth1**, **eth2** and **eth3** ports are those provided by the 1204-06 card.

See the earlier section on managing Ethernet ports.

8.2.2 Routing Tables

There are five (5) routing tables in the system: one for each network interface, and a main routing table.

Main Routing Table: This routing table is used when network traffic is generated from the server. It will generally have the same default gateway as the routing table for `eth0`, unless configured otherwise.

Interface Routing Tables: These routing tables are specific to each interface. They are named **`t0`** (for **`eth0`** interface) though **`t3`** (for **`eth3`** interface). The system is configured by default with rules to use the individual routing table for each interface for all network traffic being received or transmitted from or to the corresponding interface. For example, when an NTP request is received on interface **`eth2`**, it is tagged as such and the response will use routing table **`t2`** when sending the NTP response packet. Each routing table has a default gateway that is used when there is no explicit routing table entry that matches the destination address for a given network packet.

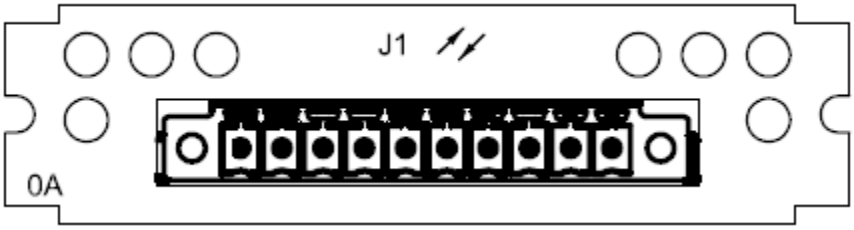
See the earlier section for information on configuring routing tables

8.2.3 Domains and Domain Name Servers (DNS)

Each network interface may exist on a separate domain and therefore have a different domain name and domain name servers from the other interfaces. The system supports a single domain name and up to 2 DNS addresses per network interface. These may be assigned via DHCP or configured manually via the Web interface configuration screen for each network interface.

8.3 Model 1209-0A: T1 / E1 - 120 Ω Module

Inputs / Outputs:	(1) 1.544/2.048 MHz RS-485 Output (2) T1 / E1 120 Ω
Signal Type and Connector:	Terminal block 1.544/2.048 MHz RS-485 T1 according to GR-499-CORE (3V into 100 Ω) E1 according to ITU-T G703 (3V into 120 Ω)



Model 1204-0A Option Module Card Rear Plate

The T1 / E1 option module card provides 1.544 MHz or 2.048 MHz and E1 or T1 data outputs for the NetClock platform.

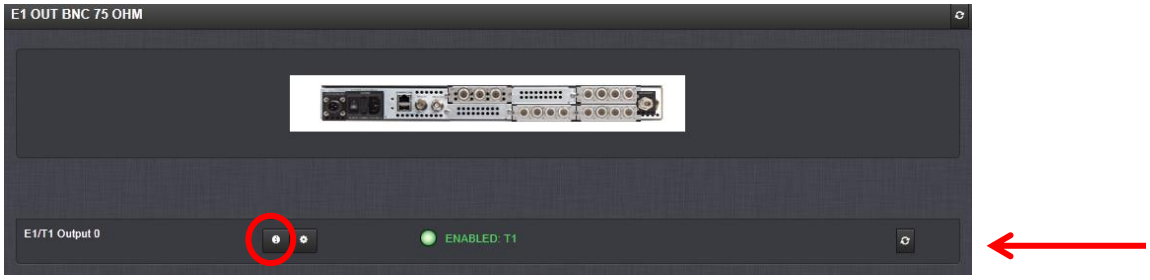
Pin Assignments

Pin No.	Signal Name	Function	Description
1	GND	Ground	Ground
2	1.544MHz/2.048MHz	RS-485 A Terminal	Square wave
3	1.544MHz/2.048MHz	RS-485 B Terminal	Square wave
4	GND	Ground	Ground
5	T1/E1 output A1	GR-499/G.703	Tip
6	T1/E1 output B1	GR-499/G.703	Ring
7	GND	Ground	Ground
8	T1/E1 output A2	GR-499/G.703	Tip
9	T1/E1 output B2	GR-499/G.703	Ring
10	GND	Ground	Ground

Table 8-5: T1 / E1 Option Card Pin Assignments

8.3.1 Setup / Configuration of the E1/T1 Outputs

1. Navigate to the **E1/T1 OUT** entry for the card you wish to configure through the **INTERFACES/OPTION CARDS** drop-down menu.
2. The **E1/T1 OUT** window will appear.



3. Click on the  button in the **E1/T1 Output 0** row.

NOTE: If you have only one input or output of any type, NetClock will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

4. The **E1/T1 Output 0** editing screen will appear.

5. Fill in the required information. Fields on this page are:

- **Signature Control**—Controls when the output will be present. Options include:
  - **Output Always Enabled**—The output is present, even when the unit is not synchronized to its references.
  - **Output Enabled in Holdover**—The output uses the current framing mode unless the unit is not synchronized to its references (the output is present while in the Holdover mode). While not synchronized, the output will change SSM states if SSM is enabled, or transition to AIS.
  - **Output Disabled in Holdover**—The output uses the current framing mode unless the unit's references are considered not qualified and invalid (the output is

not present while in the Holdover mode). While references are invalid, the output will change SSM states if SSM is enabled, or transition to AIS.

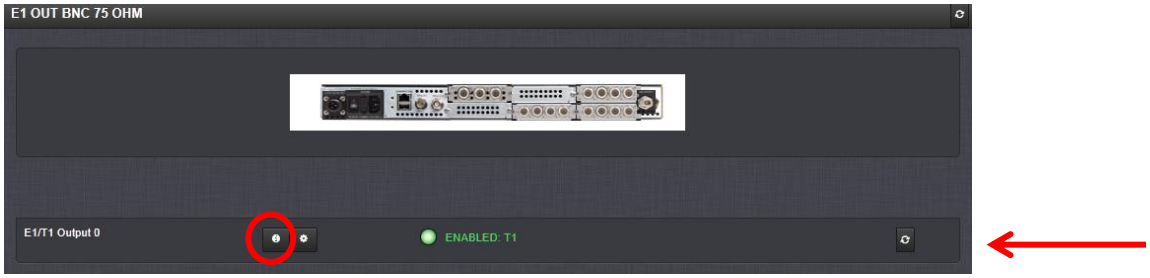
- **Output Always Disabled**—The output is not present, even if any references are present and considered qualified.

- **Mode**—This option selects T1, E1, or disabled mode. For T1 mode, the clock output will be 1.544 MHz, and for E1 the clock output will be 2.048 MHz.
- **SSM Enabled**—Enables or disables Sync Status Messaging (SSM). T1 SSM is not valid with **D4/Superframe** or **AIS** framing. E1 SSM is not valid with **AIS** framing.
- **E1 Encode**—HDB3 only.
- **E1 Framing**—This option selects the framing standard (**CRC-4**, **No CRC-4**, or **AIS**).
- **T1 Framing**—This option selects the framing standard **(D4/Superframe, Extended Superframe [CRC-6/no CR C-6**], or **AIS**).
- **T1 Encoding**—This option selects the encoding method **(B8ZS or AMI)**.
- **T1SSM Value**—This option selects the SSM quality level transmitted when SSM is enabled.
- **E1 SSM Value**—This option selects the SSM quality level transmitted when SSM is enabled.

8.3.2 Viewing E1/T1 Module Settings

To view settings information for this option module card:

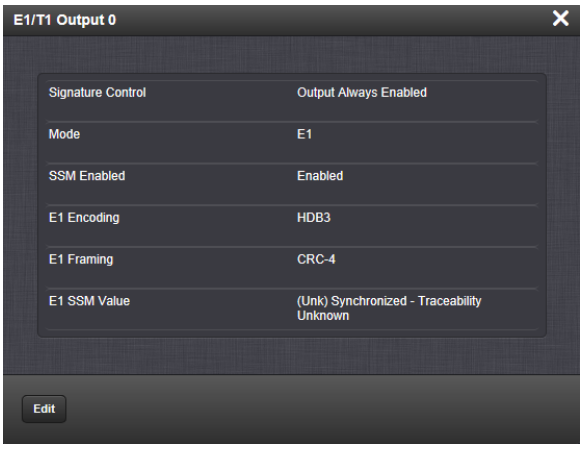
1. Navigate to the **E1 OUT BNC** entry for the card for which you wish to see the settings through the **INTERFACES/OPTION CARDS** drop-down menu.
2. The **E1 OUT BNC** window will appear.

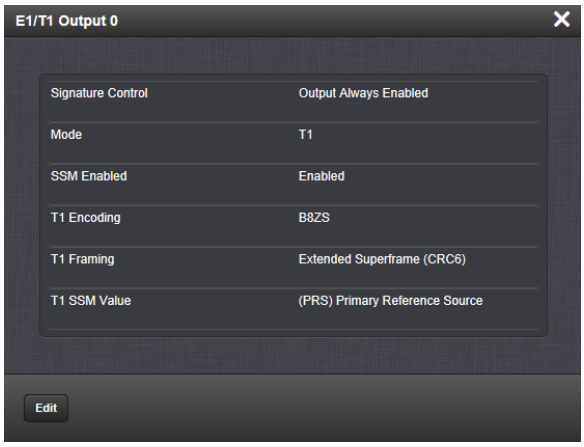


3. . Click on the  button in the **Freq Input 0** row.

NOTE: If you have only one input or output of any type, NetClock will number that input or output 0. Additional inputs or outputs will be numbered 1 or above.

4. The **E1/T1 Output 0** status screen will display. The information available will vary according to whether the output signal mode is E1 or T1.





The information in each field is as follows:

- **Signature Control**—Controls when the output will be present. Options include:
  - **Output Always Enabled**—The output is present, even when the unit is not synchronized to its references.
  - **Output Enabled in Holdover**—The output uses the current framing mode unless the unit is not synchronized to its references (the output is present while in the Holdover mode). While not synchronized, the output will change SSM states if SSM is enabled, or transition to AIS.
  - **Output Disabled in Holdover**—The output uses the current framing mode unless the unit's references are considered not qualified and invalid (the output is not present while in the Holdover mode). While references are invalid, the output will change SSM states if SSM is enabled, or transition to AIS.
  - **Output Always Disabled**—The output is not present, even if any references are present and considered qualified.
- **Mode**—This option selects T1, E1, or disabled mode. For T1 mode, the clock output will be 1.544 MHz, and for E1 the clock output will be 2.048 MHz.
- **SSM Enabled**—Enables or disables Sync Status Messaging (SSM). T1 SSM is not valid with **D4/Superframe** or **AIS** framing. E1 SSM is not valid with **AIS** framing.
- **E1 Encode**—HDB3 only.
- **E1 Framing**—This option selects the framing standard (**CRC-4**, **No CRC-4**, or **AIS**).
- **T1 Framing**—This option selects the framing standard **(D4/Superframe, Extended Superframe [CRC-6/no CR C-6**], or **AIS**).
- **T1 Encoding**—This option selects the encoding method **(B8ZS or AMI)**
- **T1SSM Value**—This option selects the SSM quality level transmitted when SSM is enabled.
- **E1 SSM Value**—This option selects the SSM quality level transmitted when SSM is enabled.

8.4 Model 1209-12: Precision Time Protocol (PTP) Module

The Precision Time Protocol (PTP) option module provides PTP support for the NetClock 9483. PTP is a protocol that can be used to synchronize computers on a local area network. The Precision Time Protocol (PTP) Module supports PTP Version 2, as specified in the IEEE 1588-2008 standard. (PTP Version 1 is not supported), via one (1) Ethernet port.

Inputs / Outputs:	(1) Configurable as Input or Output
Signal Type and Connector:	RJ-45
Management:	Web interface
Resolution:	8 nS (+/- 4 nS) packet timestamping resolution
Accuracy:	30 nS accuracy (3σ) Master to Slave via crossover cable

The PTP option module implements a PTP Ordinary Clock that can be configured to run as:

- A **Master Clock**, in which case it transmits PTP packets via the Ethernet port, with information about the current time and synchronization reference selected by the NetClock device.
- A **Slave Clock**, in which case it provides to the NetClock device a time and synchronization reference retrieved from information carried by the PTP packets received via the Ethernet port.
- A **Master/Slave Clock**, in which case the PTP option module can change mode according to priority and quality criteria compared with the other PTP Clocks on the network.

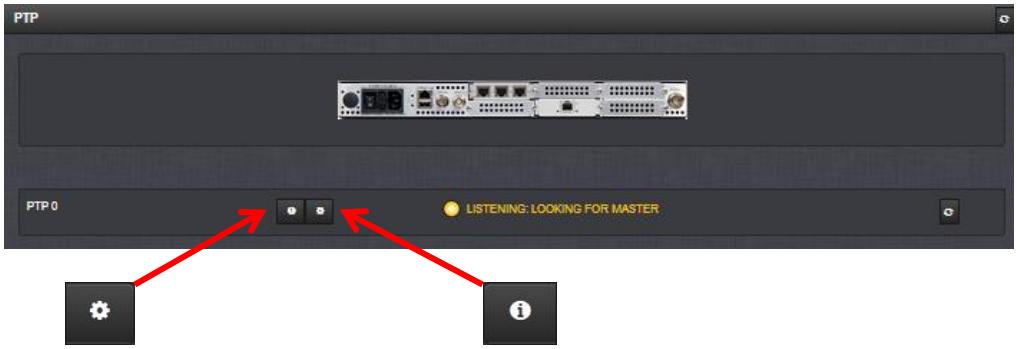
8.4.1 Configuration as a Slave Clock

8.4.2 Accessing the PTP Card Status and Settings

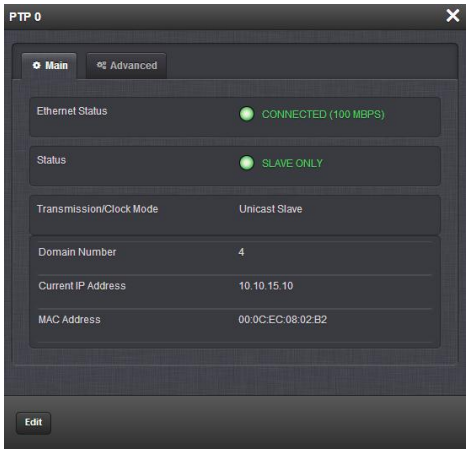
To view the status of the input and output of the PTP card, and to alter PTP settings:

1. Navigate to the PTP screen through **MANAGEMENT/OPTION CARDS**.

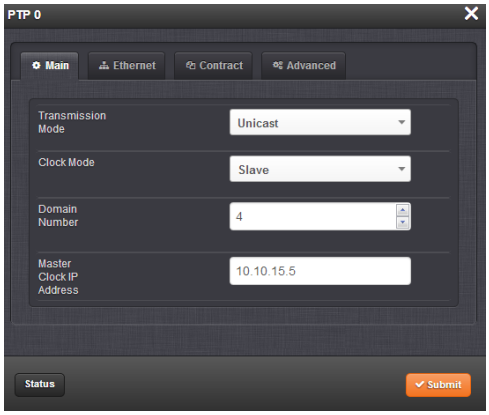
2. The PTP screen will display.



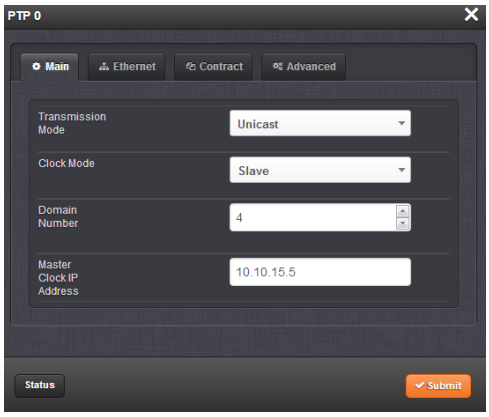
3. To view the PTP settings, click on the  button.
4. The **PTP** status screen will display



5. To configure the PTP settings, click on the  button.
6. The **PTP** edit screen will display.



Configuring PTP—Main Tab

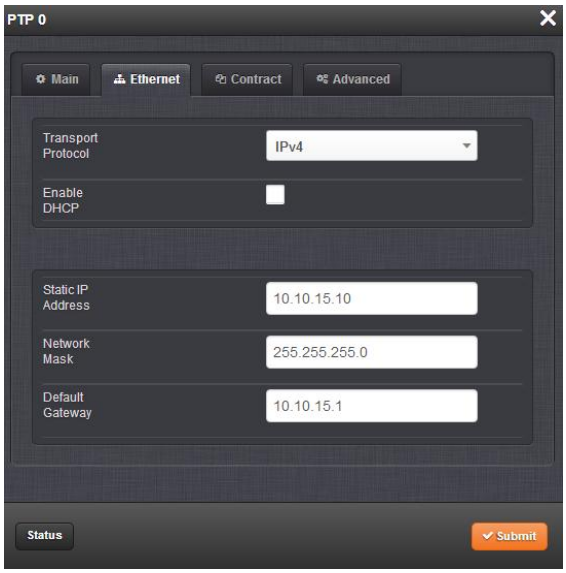


In the Main tab, you configure:

- **Transmission Mode**—Will be one of:
  - Unicast
  - Multicast'
  - Minicast
- **Clock Mode—** The Master/Slave Mode of the PTP Module**.** Will be one of:
  - Slave
  - Master
  - Disabled

  The default value is Slave.
- **Domain Number—**Sets the current PTP Domain Number, as defined in IEEE Std 1588-2008 Section 7.1. Range: [0,255]. Default setting: 0
- **Master Clock IP Address—**Static IP address of the unicast Master Clock. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

Configuring PTP—Ethernet Tab

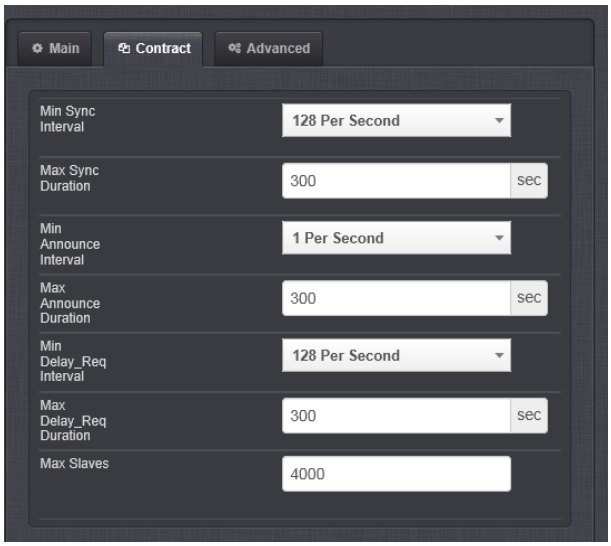


Under the Ethernet tab you configure:

- **Transport Protocol**— Selects the transport protocol used for PTP Packets. Possible values are:
  - IPv4 (The default)—Internet Protocol version 4 (Layer 3 protocol).
  - 802.3/Ethernet—IEEE802.3/Ethernet Protocol (Layer 2 protocol).

  Operating limitations: The IEEE802.3/Ethernet Protocol is not supported in Unicast transmission mode.
- **Enable DHCP**—This is a checkbox to enable or disable the delivery of IP addresses from a DHCP Server. The default setting is enabled (the box is checked).
- **Static IP Address**—When a DHCP server is not requested or is requested but not available, the PTP Module will use this IP address. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Network Mask**—When a DHCP server is not requested or is requested but not available, the PTP Module will use this Network Mask. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].
- **Default Gateway**—When a DHCP server is not requested or is requested but not available, the PTP Module will use this Default Gateway. In the format "#.#.#.#" with no leading zeroes or spaces, where each '#' is a decimal integer from the range [0,255].

Configuring PTP—Contract Tab



NOTE: The settings under this tab only apply to unicast mode.

Under the **Contract** tab, you configure:

- **Min Sync Interval—**The minimum value of Sync interval granted by the Master Clock. In packets per second.
- **Max Sync Duration—**The maximum value of Sync interval granted by the Master Clock. In seconds.
- **Min Announce Interval—**The minimum value of the Announce interval granted by the Master Clock. In packets per second.
- **Max Announce Duration—**The maximum value of the Announce interval granted by the Master Clock. In seconds.
- **Min Delay_Req Interval—**In packets per second.
- **Max Delay_Req Duration—**In seconds.
- **Max Slaves—**The maximum number of slaves the card will serve.

8.4.3 Configuration as a Slave Clock

By default, the PTP Module is configured to function as a multicast PTP Slave, which allows a unit to be able to synchronize to a multicast PTP Master (such as another unit with a PTP module option card configured as a Master) when configured with the following parameters:

- Announce Interval = once every 4 seconds or faster (This is set in the **PTP Edit** window, under the **Contract** tab).
- Delay Mechanism = End-to-End (This is set in the **PTP Edit** window, under the **Advanced** tab).
- Transmission Mode = Multicast (This is set in the **PTP Edit** window, under the **Main** tab).
- Synchronization Mode = Two-Step Mode faster (This is set in the **PTP Edit** window, under the **Advanced** tab).

When first connected to a network that contains an active Master Clock, it may take up to a minute for the Port State to change to the "slave" state. After that, it will take up to two minutes for the PTP connection to be accepted as a valid reference by the unit.

If the unit is not entering the "Slave" Port state (as reported by the **Main** tab on the **PTP Status** page), check the following:

- From the **PTP** Status window under the **Main** tab, check that **Ethernet Status** indicates "Connected."
- From the **PTP** Status window under the **Advanced** tab, check that **Port Activity** indicates "Enabled."
- From the **PTP** Status window under the **Main** tab, check that the **Ethernet Status** indicates a speed of 100 Mb/s.
- From the **PTP** Status window under the **Main** tab, check that the clock is set to be a SLAVE ONLY.
- From the **PTP** Status window under the **Main** tab, check that the **Transmission/Clock Mode** is a Slave mode and that multicast/unicast/minicast state is correct.
- Check that the Ethernet Transport Protocol set for the Slave Clock is the same as the Transport Protocol of the Master Clock to which the Slave Clock must be synchronized with. (Check the **Transport Protocol** on the **PTP** edit window, under the **Ethernet** tab.)
- Check that the **Domain Number** set for the Slave Clock is the same as the Domain Number of the Master Clock to which the Slave Clock must be synchronized with. (Check the **Domain Number** on the **PTP** status window, under the **Main** tab.)
- From the **PTP** status window, under the **Advanced** tab, check that the **Current IP Address** is valid.
- From the **PTP** edit window under the **Advanced** tab, check that the Time To Live (TTL) for PTP packets is compatible with the network.
- If in Multicast mode, check that the switches/routers are transparent to multicast frames
- From the PTP status window under the Advanced tab, check that the Clock Class is "Master, In Sync."

NOTE: If DHCP is enabled and PTP was not successful in obtaining an IP address, DHCP will need to be restarted to retry. To restart DHCP:

1. In the **PTP** edit window under the Ethernet tab, select the **Enable DHCP** checkbox.
2. Click the **Submit** button at the bottom of the window.

8.4.4 Configuration as a Master Clock

To configure the IEEE-1588 (PTP) Module as a Master Clock, perform these steps:

General actions

- Ensure the PTP port is Connected to the network (check the Link Status in the **PTP Status/Network** page).
- Ensure the PTP port speed is 100 Mb/s (check the **Port Speed** in the **PTP Status** page under the **Advanced** tab).
- Be sure that valid time and 1PPS references are currently selected (go to **MANAGEMENT/OTHER/Time Management**).

In order to operate properly as a Master Clock, the unit must be synchronized to a non-PTP reference. Confirm that the chosen reference transmits the following information (as reported by the Time Properties on the **PTP Status** page, under the **Advanced** tab):

- The proper TAI or UTC time (including the current year)
- The current TAI to UTC offset (required even if the reference's time is in TAI)
- Pending leap second information at least a day in advance.

If the reference does not transmit this information, it must be provided by the user in order for the Master Clock to function properly.

The built-in GNSS reference provides all information needed with no user intervention.

Specific PTP Module Actions

Confirm that:

- From the **PTP** status window under the Advanced tab, check that **PTP Port Activity** is enabled (if not, enable it from the **PTP** edit window, under the **Ethernet** tab).
- From the **PTP** edit window under the **Main** tab, check that the clock is set to be a Master.
- From the PTP status window under the Main tab, check that a valid IP address is currently being used.

When the PTP Module is set to be a Master Clock, the module will immediately attempt to become the active Master Clock on the network (**Port State** = **Master**). If it does, it will start to transmit PTP packets (even if the unit is not yet synchronized).

There are several reasons why the PTP Module may not become the active Master Clock, or may not be broadcasting the correct time, even if it is set to be a Master Clock:

1. If using any reference other than self for 1PPS, the unit will not become an active Master Clock until the **Time Figure of Merit (TFOM)** value of the system is less than 15. After first going into sync after power-up, it may take a minute or two for the Time Figure of Merit (TFOM) value to fall to an acceptable level. The current Time Figure of Merit (TFOM) value is available in the **Time Properties** panel under the **Advanced** tab on the **PTP** status window page.

2. PTP uses the TAI timescale to transfer time. Many timing references communicate time in the UTC timescale. UTC is offset from TAI by a small amount which changes every time a leap second occurs. The TAI to UTC Offset is part of the PTP Specification and must be provided to a Master Clock. If no active reference can provide that information, the offset must be provided by the Host. The TAI to UTC Offset can be set from the **MANAGEMENT/OTHER/Time Management** page (while setting the GPS to UTC Offset).

3. The PTP Protocol also provides for the transfer of Leap Second information. If the active time reference does not provide Leap Second information, it must be added by the user through the **MANAGEMENT/OTHER/Time Management** page. If this is not done, the PTP network will have the incorrect UTC time after a leap second event.

4. If there are multiple multicast Master Clocks on the network, the PTP Module uses the Best Master Clock (BMC) algorithm specified in the PTP Specification to decide whether or not to become the active Master Clock. The BMC algorithm selects the Best Master Clock on the network from the following criteria:

    a. The BMC algorithm first selects the clock having the higher Priority1 parameter (a lowest value means a higher priority)
    b. If the BMC cannot be determined from the previous parameter, the BMC algorithm selects the clock having the higher Clock Quality (Clock Class, Clock Accuracy, Clock Variance)
    c. If the BMC cannot be determined from the previous parameters, the BMC algorithm selects the clock having the higher Priority2 parameter

The Master Clock selected by the BMC algorithm as the Best Master Clock will transition into the Master state to become the active Master Clock on the network. It will then start to transmit Sync packets to the Slave Clocks. The other Master Clocks will transition into the Passive state.

Configuration in Master/Slave Mode

The IEEE-1588 (PTP) Module also supports a combined Master/Slave mode. The Master/Slave mode works best in a unit which is not synchronized to any other reference. When the module is plugged into the PTP network, it will become a slave to the Best Master Clock on the network.

If all Master Clocks are removed from the network, the unit containing the Master/Slave module will go into Holdover mode. However, the module will use that Holdover time to become the Best Master Clock on the network, and it will provide time to the network until the unit's **Holdover Timeout** expires. If another Master Clock comes online and becomes the Best Master Clock, the Master/Slave module will become a Passive Master Clock until the unit's Holdover Timeout expires.

For more information on Holdover Mode, refer to **3.15.1** Holdover Mode.

NOTE: The Master/Slave mode is not supported in unicast transmission mode.

Transmission Modes

- Multicast Mode--This is the default mode. PTP packets are transmitted to all PTP Clocks by means of multicast IP addresses dedicated to the PTP protocol (224.0.1.129, 224.0.0.107). PTP packets received by the PTP Clocks are then filtered from the Domain Number, the Port Identity (Clock Identity + Port Number) of the transmitter, the packet identifier (Sequenced).

  When the Master Clock is set in multicast mode, this module will deny the requests from the Slaves Clocks to run in unicast mode.

  When the Master Clock is set in Unicast mode, it doesn't transmit any PTP messages until a Slave has been granted to run in unicast mode.

- Unicast Mode—This is a Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

NOTE: The Unicast mode is only implemented for the following PTP packets:

- Announce
- Sync and Follow-Up
- Delay_Req and Delay_Resp

The unicast mode is activated at the initiative of the Slaves. Each Slave, which wants to run in unicast mode, shall first negotiate unicast contracts with the Master.

- Minicast/Hybrid Mode—The Minicast/Hybrid mode is a method to minimize the PTP packets payload on the network, where:
  The transmissions initiated by the Master (Announce, Sync/Follow-Up) run in multicast mode.
  The transmissions initiated by the Slaves (Delay_Req/Delay_Resp) run in unicast mode.

Configuring Minicast Mode

On the Master side:

- In the **PTP** edit window under the Main tab, select Multicast for the **Transmission Mode**. Enable the Minicast.

On the Slave side:

1. In the **PTP** edit window under the Main tab, select Multicast for the **Transmission Mode**. Enable the Minicast mode.

Unicast Mode

Point-to-Point transmission mode between two PTP Clocks by means of the unique IP address assigned to each PTP Clock.

The unicast mode is activated at the initiative of the Slaves. Each Slave, which wants to run in unicast mode, shall first negotiate unicast contracts with the Master.

To enter the unicast mode, perform the following steps:

On the Master side:

1. In the **PTP** edit window under the Main tab, select Multicast for the **Transmission Mode**. Enable the Unicast mode.

On the Slave side:

1. In the **PTP** edit window under the Main tab, select Multicast for the **Transmission Mode**. Enable the Unicast mode.

When the Master Clock is set in multicast mode, this one will deny the requests from the Slaves Clocks to run in unicast mode.

When the Master Clock is set in Unicast mode, it doesn't transmit any PTP messages until a Slave has been granted to run in unicast mode.

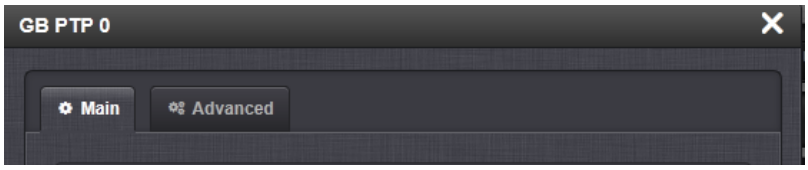
NOTE: The Unicast mode is only implemented for the following PTP packets:

- Announce
- Sync and Follow-Up
- Delay_Req and Delay_Resp

8.4.5 Viewing PTP Settings

The **PTP status** page is available either through the **INTERFACES** drop-down menu.

The GB PTP Status page contains 2 tabs:



- **Main**
- **Advanced**

The **Main** tab provides the following information:

- **Ethernet Status**—Whether the module is connected to a network through Ethernet.
  - **Green**=Connected. The speed of the connection is indicated.
  - **Orange**=Not connected.
- **Port State**— Reports the current state of the PTP State Machine:
  - Disabled: PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.
  - Initializing: Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn't leave this state while it can't get the current time and synchronization references from the unit to synchronize with it.
  - Listening: PTP module is looking for a Master Clock.
  - Master: PTP Master has become the active Master Clock on the network.
  - Passive: PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.
  - Uncalibrated: PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.
- **Number of Unicast Slaves**—Number of PTP Slaves that have been granted by the PTP Master to run in unicast mode.
- **Profile**—Whether the profile is the default or Telecom.
- **Domain Number**—The current PTP Domain Number.
- **Current IP Address**—The IP address currently being used by the PTP interface.
- **MAC Address**—The MAC address currently being used by the PTP interface.

The **Advanced** tab provides the following information:

Time Properties:

- **UTC Offset**—The Master's current offset between UTC time and TAI time. Units: seconds.
- **UTC Offset Valid**— Indicates whether or not the Master's UTC Offset is valid.
- **Leap Second**—The Leap second correction as set on the **Time Management** page.
- **Time Traceable**— Indicates whether the Master's time is traceable (Enabled) to a primary reference or not (Disabled).
- **Frequency Traceable**—Indicates whether the Master's Frequency is traceable (Enabled) to a primary reference or not (Disabled).
- **PTP Time Scale**—Indicates the timescale that the Master is using to broadcast its time. TAI is the default PTP timescale.
- **Time source**—The Time Source that the Master is using. Refer to IEEE Standard 1588-2008, Section 7.6.2.6.

Clock Quality

- **Clock Accuracy**—A number describing the accuracy of the oscillator in the Master relative to its UTC reference. (See IEEE Standard 1588-2008, Section 7.6.2.5).
- **Offset Scaled Log Variance**—(Defined in IEEE Standard 1588-2008, Section 1.6.3)
- **Clock Class—**A number describing the state of the time and 1pps references of the PTP Clock.

Refer to the following table for Clock Class information (see IEEE standard 1588-2008, Table 5, Section 7.6.2.4).

PTP Timescale	Arbitrary Timescale	Clock Class Definition
6	13	Time and 1pps references are synchronized with the host references and PTP clock shall not be a slave to another clock in the domain.
7	14	Time and 1pps references are in holdover state, within specifications and PTP clock shall not be a slave to another clock in the domain.
52	58	Time and 1pps references are in holdover state, not within specifications, and PTP clock shall not be a slave to another clock in the domain. Then, applied to Master Clocks who have just powered on and have not yet achieved a suitable TFOM value.
187	193	Time and 1pps references are in holdover state, not within specifications, and PTP clock may be a slave to another clock in the domain.
255	255	Class assigned to "Slave-Only" clocks.
248	248	"Unknown" class.

Ethernet Status

- **Current IP Address**— The IP address currently being used by the PTP interface.

NOTE: If the PTP Module is set up for DHCP but fails to obtain an IP address, it will use the Static IP instead. To reacquire a DHCP address, reset the module via the Main tab in the PTP settings window.

- **Current Network Mask**— The Network Mask currently being used by the PTP interface.
- **Current Gateway**—The Gateway address currently being used by the PTP interface.

Port Status

- **Port Number—**The PTP Port Number, as defined in the IEEE 1588-2008 Specification, Section 7.5.2.3. Always set to 1 for our Ordinary Clock.
- **Port Activity—**Reports whether or not the network interface is active for PTP (Enabled) or not (Disabled).
- **Port State**— Reports the current state of the PTP State Machine:
    - **Disabled**—PTP Ethernet port is Disabled. See PTP Setup/Network page, PTP Network Settings options.
    - **Initializing**—Ethernet link is unplugged/PTP Module is in power-up state. A Master Clock doesn't leave this state while it can't get the current time and synchronization references from the unit to synchronize with it.
    - **Listening**—PTP module is looking for a Master Clock.
    - **Master**—PTP Master has become the active Master Clock on the network.
    - **Passive**—PTP Module has become a Passive Master Clock. (There is another Master Clock on the network with better quality or higher priority). This Master will wait until the Best Master Clock Algorithm determines it should become the best Master Clock, and then it will transition to the Master Clock state.
    - **Uncalibrated**—PTP Slave has selected a Master Clock on the network attempts to synchronize with it using sync packets.
- **Link Status**—Indicates whether or not the Ethernet link for PTP is active (Connected) or not (Disconnected).
- **Slave Sync Mode**—Determines the number of steps in the PTP protocol. Will be one of the following:
    - Two-Step Mode
    - One-Step

NOTE: One-Step mode is not supported with the Peer-to-Peer Delay Mechanism.

The current implementation of one-step mode involves a software-oriented timestamping. Two-step mode implements a hardware oriented timestamping, insensitive to software execution time variations. **Two-step mode is recommended**, as it increases the PTP Clock's accuracy.

NOTE: Peer-to-Peer Delay Mechanism is only applicable on networks equipped with Transparent Clocks (switches/routers IEEE 1588 compatible). Peer-to-Peer Delay Mechanism is not supported in Unicast transmission mode.

Grandmaster Properties

Reports information from the current Grandmaster Clock. If the PTP Module is currently a Master, this will report information on the current module.

- **Clock Identity—**Displays the clock identity of the current Grandmaster Clock on the network**.**
- **Clock Class**—A number describing the state of the clock (see Table 5 of Section 7.6.2.4 of IEEE Standard 1588-2008).
- **Clock Accuracy—**A number describing the accuracy of the oscillator in the Grandmaster Clock (see IEEE Standard 1588-2008, Section 7.6.2.5).
- **Offset Scaled Log Variance**—See IEEE Standard 1588-2008 Section 7.6.3.
- **Priority1—**See IEEE Standard 1588-2008, Section 7.6.3.
- **Priority2—**See IEEE Standard 1588-2008, Section 7.6.3.

Slave Properties

- **Negotiation Enabled**—Reports whether the Unicast Negotiation option is Enabled or Disabled.
- **Contract State:** Reports the unicast contract state.
    - **NEGO_OFF—**Unicast negotiation option is Disabled.
    - **NEGO_ON—**Unicast negotiation option is Enabled.
    - **REQUESTED—**Unicast contract has been requested to the PTP Master.
    - **GRANTED—**Unicast contract has been granted by the PTP Master.
    - **RENEWED**—Renewal of the unicast contract has been requested to the PTP Master.
    - **CANCELED—**Cancellation of the unicast contract has been requested to the PTP Master.
- **Contract Duration:** Duration of the unicast contract. Units: Seconds.
- **Contract Delay:** Delay before the end of the unicast contract. Units: Seconds.
- **Message Interval:** Announce Interval negotiated for the unicast mode. Units: log2 seconds.
- **Contract State:** Reports the unicast contract state (see above 'Announce Contract State').
- **Contract Duration:** Duration of the unicast contract. Units: Seconds.
- **Contract Delay:** Delay before the end of the unicast contract. Units: Seconds.
- **Message Interval:** Sync Interval negotiated for the unicast mode. Units: log2 seconds.
- **Contract State:** Reports the unicast contract state (see above 'Announce Contract State').
- **Contract Duration**: Duration of the unicast contract. Units: Seconds.
- **Contract Delay:** Delay before the end of the unicast contract. Units: Seconds.
- **Log Message Interval:** Delay_Resp Interval negotiated for the unicast mode. Units: log2 seconds

Master Properties

- **Unicast Negotiation:** Reports whether the Unicast Negotiation option is Enabled or Disabled.
- **Number of Slave Clocks Connected:** Number of PTP Slaves that have been granted by the PTP Master to run in unicast mode.

Module Info.

- **PTP Version**—Current version of PTP being used.
- **Software Version**—Current software revision level
- **Hardware Version**—Current hardware revision level.
- **Software Compilation Date**—Date the software was compiled.
- **Software Compilation Time**—Time the software was compiled

Section 9: NetClock 9489 Outputs

9.1 1PPS Output

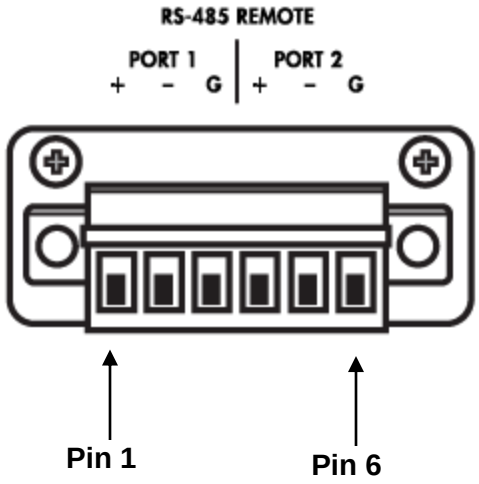
The NetClock 9489 1PPS output is identical to the NetClock 9483. For additional information, refer to Section *1.9*:"*1PPS Output*" for 1PPS output specifications.

9.2 ASCII RS-485 Outputs

The NetClock 9489 provides two (2) ASCII RS-485 outputs. The two RS-485 outputs appear on tabs next to the **1PPS output** tab.

Pin Assignments

NOTE: In the following table, pin assignments are defined left to right, starting with Pin 1.



PIN	SIGNAL
1	RS-485 TX+
2	RS-485 TX-
3	GND
4	RS-485 TX+
5	RS-485 TX-
6	GND

Figure 9-1: ASCII RS-485 Output Pin Assignment

Section 10: General NetClock Troubleshooting

The front panel LEDs and the web interface provide NetClock status information that can be used to help troubleshoot failure symptoms that may occur.

10.1 Troubleshooting Front Panel LED Status Indications:

The front panel LEDs can provide "local" status information about the NetClock. Observe the front panel LEDs and use the table below to find the recommended troubleshooting steps or procedure for the observed condition.

LED	Current Status	Indication	Troubleshooting
Power	LED is blank (not lit).	NetClock has no AC and/or DC input power applied.	1) Verify AC power is connected to an AC source and AC power switch is ON. 2) Verify DC power (within the correct voltage range, as stated on the DC connector) is applied to the DC power connector. 3) Refer to Section 2.2
Sync	LED is off	No valid Reference inputs available since power-up.	1) Make sure the Input Reference Priority table has the desired inputs enabled, based on desired priority. 2) Make sure the desired input references are connected to the correct port of NetClock. 3) Refer to Section *3.16*.
Sync	LED is orange	Holdover mode: All available inputs have been lost.	1) Make sure the Input Reference Priority table still has the desired inputs enabled, based on desired priority. Refer to Section *3.16*. 2) Make sure desired input references are still connected to the correct port of NetClock. 4) Verify GPS antenna installation (if applicable). Refer to Section 9.4
Sync	LED is red	Time Sync alarm: NetClock was just powered-up and has not yet synced to its references. Or, all available reference inputs have been lost and the Holdover mode has since expired.	***Note:*** *If NetClock was just recently powered-up or rebooted and input references are applied, no troubleshooting may be necessary. Allow a few minutes for the input reference to be declared valid (allow 35 – 40 minutes for a new install with GPS input).* 1) Make sure the Input Reference Priority table still has the desired inputs enabled, based on desired priority. Refer to Section *3.16*. 2) Make sure desired input references are still connected to the correct port of NetClock. 3) Verify GPS antenna installation (if applicable). Make sure the antenna has a clear view of the sky.
Fault	LED is blinking	GPS Antenna problem	1) Verify GPS antenna is connected to NetClock

	orange	alarm is asserted	GPS input connector 2) Check antenna cable for presence of an open or a short. Refer to Section 9.4 for additional information.
Fault	LED is solid red	Major alarm is asserted	Refer to Section *10.1.1*
Fault	LED is solid orange	Minor alarm is asserted	Refer to Section *10.1.2*

Table 10-1: Troubleshooting front panel LED indications

10.1.1 Fault Light - Major Alarm

There are several conditions that can cause the front panel Fault lamp to indicate a Major alarm has been asserted. These conditions include:

- **Frequency error:** Indicates a jump in the oscillator's output frequency has been detected. Contact Tech Support for additional information.
- **1PPS is not in specification:** The 1PPS input reference is either not present or is not qualified.
- **Too few GPS sat 2nd threshold:** The GPS receiver is continuing to track less than the minimum number of satellites. Refer to Section *10.4* for information on troubleshooting GPS reception issues.
- **GPS Receiver Fault:** There was a problem with communications between NetClock and its GPS receiver.

10.1.2 Fault light - Minor Alarm

There are several conditions that can cause the front panel Fault lamp to indicate a Minor alarm has been asserted. These conditions include:

- **Too few GPS sat 1st threshold:** The GPS receiver has been tracking less than the minimum number of satellites for too long of a duration. Refer to Section *10.4* for information on troubleshooting GPS reception issues.
- **The unit has rebooted:** NetClock was either rebooted or intentionally/inadvertently power cycled.

10.2 Unable to Open NetClock Web User Interface:

With NetClock connected to either a stand-alone or networked PC and with the network configuration correct, it should be possible to connect to the product web interface.

Verify	Current Status	Indication	Troubleshooting
LEDs on network connector	Green “Good link” is not solid green	NetClock ICMP test is failing. NetClock is not connected to PC via Ethernet connection	1) Verify one end of standard network cable is connected to NetClock’s Ethernet port and other end is connected to a hub/switch. Or a network cross-over cable is connected to NetClock and a stand-alone PC. 2) Verify network settings of NetClock are valid for the network/PC it is connected with (IP address is on the same subnet as the other PC).
	Green “Good Link” is solid green on both NetClock and other end of network cable.	NetClock ICMP test is passing. NetClock is connected to PC via Ethernet connection	1) Disconnect NetClocks network cable and ping its assigned address to ensure no response (no duplicate IP addresses on the network). 2) Try accessing NetClock from another PC on the same network. 3) Network Routing/firewall issue. Try connecting directly with a PC and network cross-over cable.

Table 10-2: Troubleshooting Network Connection Issues

10.3 Troubleshooting Web Interface Status Page Indications

NetClock's web user interface can provide "remote" status information about NetClock. The Status pages contain information on the current status. Locate the provided status fault indication in the following table for troubleshooting guidance.

Web UI Page location	Current Status	Indication	Troubleshooting
HOME page**, System Status** panel, **Status** row	**SYNC** indicator is not "lit" (not **Green**). **HOLD** indicator is "lit" (Orange). —OR— **FAULT** indicator is "lit" (Red). Below the **System Status** panel there is an **Out of Sync** alarm statement	The unit is in Holdover mode —OR— The unit is now out of Time Sync	All available Input References have been lost. The **Reference Status** table on the **HOME** page will show the current status of all inputs (Green is valid and Red is invalid or not present). 1) Make sure the Input Reference Priority table still has the desired reference inputs Enabled, based on the desired priority. 2) Make sure the desired input references are still connected to the correct input port of the unit. 3) Verify GNSS antenna installation (if applicable). Refer to **10.4 Troubleshooting GPS Reception Issues (Holdover and/or Time Sync Alarms Occurring)**.
HOME page**, System Status** panel, **Power** row	**AC** and/or **DC** indicator is red instead of green **NOTE**: The **AC** indicator will only display on the **HOME** screen if the unit is equipped with an AC power input. The **DC** indicator will only display on the HOME screen if the unit is equipped with a DC power input.	Specified AC and/or DC input power is not present.	If **AC** indicator is red: 1) Verify AC power cord is connected to an AC outlet. 2) Verify AC power input switch is ON. 3) Check the two fuses in the AC power module. If **DC** indicator is red: 1) Verify DC power source is within range specified at the DC power connector. 2) Verify DC power is present at the input connector. 3) Verify DC input polarity.

MANAGEMENT/ NTP Setup page **NTP Status Summary** panel **Stratum** row	Stratum 15	NTP is not synchronized to its available input references (the unit may have been in Holdover mode, but Holdover has since expired without the return of valid inputs)	***Note**: If the unit was just recently powered-up or rebooted and input references are applied, no troubleshooting may be necessary. Allow at least 10-20 minutes for the input references to be declared valid and NTP to align to the System Time (allow an additional 35-40 minutes for a new install with GNSS input).* **1)** Verify in the **Configure Reference Priorities** table that all available references enabled. 2) Verify that the **Reference Status** on the **HOME** page shows "OK" (Green) for all available references. 3) Verify NTP is enabled and configured correctly. Refer to **3.16.1 Configuring NTP**.
MANAGEMENT/ NETWORK page **Actions** panel **Access Control Network Access Rules** table	Cannot login or access the web interface.	The following error message is displayed: "`Forbidden You don't have permission to access/ on this server`"	This message is displayed when any value has been added to the **Network Access Rules** table and your PC is not listed in the table as an **Allow From** IP address. To restore access to the web interface, either 1) Login from a PC that is listed as an **Allow From** in this table; or 2) If it is unknown what PCs have been listed in the Access table, perform an **`unrestrict`** command to remove all entries from the **Network Access Rules** table. This will allow all PCs to be able to access the web interface.

Table 10-3: Troubleshooting Web Interface Indications

10.4 Troubleshooting GPS Reception Issues (Holdover and/or Time Sync Alarms Occurring):

When a GPS receiver is installed in NetClock, a GPS antenna can be connected to the rear panel antenna connector via a coax cable to allow it to track many satellites in order for GPS to be an available input reference. Many factors can prevent the ability for the GPS receiver to be able to track the minimum number of satellites.

With the GPS antenna installed outdoors, with a good view of the sky (the view of the sky is not being blocked by obstructions), NetClock will typically track between 5-10 satellites (the maximum possible is 12 satellites). If the antenna's view of the sky is hindered, or if there is a problem with the GPS antenna installation, the GPS receiver may only be able to a few satellites or may not be able to track any satellites at all.

When GPS is a configured time or 1PPS input reference, if the GPS receiver is unable to continuously track at least four satellites (until the initial GPS survey has been completed) or at least one satellite thereafter, the GPS signal will not be considered valid. If no other inputs are enabled and available, NetClock may not initially be able to go into time sync. Or, if GPS reception is subsequently lost after initially achieving time sync, NetClock will go into the Holdover mode. If GPS reception is not restored before the Holdover period expires (and no other input references become available) NetClock will go out of sync. The GPS reception issue needs to be troubleshot in order to regain time sync.

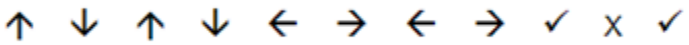
For additional information on troubleshooting GPS reception issues with NetClock, please refer to the *NetClock GPS Reception Troubleshooting* document, available from the Spectracom website (visit www.spectracomcorp.com and from the site navigation menu, select **Support → Library → Installation and Troubleshooting Guides**).

10.5 Front Panel Keypad is Inoperative:

The front keypad can be locked in order to prevent inadvertent operation. It can be locked and unlocked using either the keypad or the web interface. When locked, the keypad operation is disabled until it is unlocked using either of the two following processes:

A) To unlock the front panel keypad using the keypad (locally):

1) Perform the following key sequence:



B) To unlock the front panel keypad using the web browser (remotely):

1) Open the NetClock web interface and navigate to the **Setup / Front Panel** page.
2) Change the "Lock" from "**Enabled**" to "**Disabled**".
3) Click "Submit".

10.6 No 1PPS and / or 10 MHZ Output Present:

If the 1PPS and / or the 10 MHz output are not present, input power may not be applied. Or NetClock is not synchronized to its input references and Signature Control is enabled.

Web UI Page	Current Status	Indication	Troubleshooting
HOME page	**Reference Status** Table	One or more input references indicate "Not Valid" (red)	All available Input References have been lost. The **Reference Status** table on this same page will show the current status of all inputs (Green is valid and red is not valid, or not present). If Signature Control is enabled in this state, the output may be disabled see **3.4.11.3 Configuring 1PPS Output**,

			3.4.11.4 Configuring 10 MHz Frequency: 1) Make sure the Input Reference Priority table still has the desired inputs enabled, based on desired priority. 2) Make sure desired input references are still connected to the correct input port. 3) Verify GNSS antenna installation (if applicable).
Navigate to **INTERFACES/OUTPUTS/ PPS Output** page	Select the PPS Output screen. See **3.4.11.3 Configuring 1PPS Output.**	Signature Control will show **Output Always Enabled, Output Enabled in Holdover, Output Disabled in Holdover** or **Output Always Disabled**	1) With **Output Always Enabled** selected, the selected output will be present no matter the current synchronization state. 2) Any other configured value will cause the applicable output to be halted if the unit is not fully synchronized with its input references.

Table 10-4: Troubleshooting 1PPS and/or 10 MHz Outputs not Being Present

10.7 The Front Panel LCD Window is Blank:

As long as input power is applied (as indicated by the power light being green and the LED time display incrementing) the LCD can display data. The LCD can be configured to display different information while the keypad is not in use. One available configuration is to have the LCD display a blank page when not in use. The LCD window operation can be verified and can also be configured via the web interface or the front panel keypad.

A) **Using the front panel keypad to verify the LCD is configured to display a blank page:**
To verify the front panel LCD is configured to display a blank page, just press any keypad button. As long as the keypad is unlocked, the “Home” screen will be displayed (after one minute of not pushing any keys, the screen will go back to blank).

Note: The LCD display that is selected is the page that is normally displayed in the LCD window, beginning one minute after the keypad is no longer being used.

B) **Using the front panel keypad to change the information normally displayed in the LCD when the keypad is not in use:**

To use the front panel keypad to reconfigure the LCD to display something other than a blank page (such as GPS information, network configuration, etc), refer to Section 2.9.

C) **Using the web browser to change the information normally displayed in the LCD when the keypad is not in use:**

To use the web UI to reconfigure the LCD to display something other than a blank page (such as GPS information, network configuration, etc), refer to Section 3.13.9 Front Panel LED/LCD Display and Keypad Configuration (9483 only)

10.8 Front Panel Serial Port is Not Responding:

The front panel serial port can be used for NetClock configuration or to obtain select data. The serial port is a standard DB9Female port. Communication with this port is via a standard DB9 F to DB9M serial cable (minimum pinout is pin 2 to 2, pin 3 to 3 and pin 5 to 5) connected to a PC running a terminal emulator program such as Microsoft HyperTerminal. The port settings of the terminal emulator should be configured as 9600, N, 8, 1 (flow control setting does not matter).

If the terminal emulator program does not display any data when the keyboard <Enter> key is pressed, either NetClock is not powered up or there is a problem with the connection between NetClock and the PC.

1. Using a multimeter, ring out the pins from one end of the serial cable to the other. Verify the cable is pinned as a straight-thru serial cable (pin 2 to 2, pin 3 to 3 and pin 5 to 5) and not as a null-modem or other pin-out configuration.

2. Disconnect the serial cable from NetClock. Then, jumper (using a wire, paperclip or car key, etc) pins 2 and 3 of the serial cable together while pressing any character on the PC's keyboard. The character typed should be displayed on the monitor. If the typed character is not displayed, there is a problem with either the serial cable or with the serial COM port of the PC.

3. Refer to Section 11: "*Using HyperTerminal to Connect to NetClock*" for more information on using HyperTerminal (or similar terminal emulator software) to communicate with the the unit via serial port.

10.9 Front Panel Cooling Fan is Not Running:

The cooling fan (located on the front panel, to the right of the LED time display) is a temperature controlled cooling fan. An internal temperature sensor determines when the cooling fan needs to turn on and off. It is normal operation for the cooling fan to not operate the entire time NetClock is running. It may be turned off for long periods at a time, depending on the ambient and internal temperatures.

To verify the cooling fan is still operational, power cycle the NetClock unit (if AC and DC power are both applied, momentarily turn off the AC power switch and disconnect the DC power connector).

NOTE: If the internal temperature in the unit is below 30 degrees Celsius, the fan may not turn on as part of the power-up sequence. In this case, it is recommended to let the unit "warm up" for approximately 30 minutes, in order to allow the unit to get to the appropriate temperature.

10.10 Network PCs are Not Able to Synchronize to NetClock:

In order for clients on the network to be able to sync to NetClock, a few factors have to be met.

1. The PC(s) must be routable to NetClock. Make sure you can access the NetClock product web interface from a PC that is not syncing. If the PC can't access the web interface, a network issue likely exists. Verify the network configuration.

2. The network clients have to be configured to synchronize to NetClock's address. For additional information on syncing Windows PC's, visit the Spectracom website (www.spectracomcorp.com), and from the main site navigation menu select **Support > Library > Installation and Troubleshooting Guides**, and download / view the document titled *Synchronizing Windows Computers*. The last section of this document also contains troubleshooting assistance for Windows synchronization. For UNIX/Linux computer synchronization, please visit http://www.ntp.org/.

3. If at least one PC can sync to NetClock, the issue is likely not with the NetClock itself. The only NetClock configurations that can prevent certain PCs from syncing to the time server are the NTP Access table and MD5 authentication. Refer to Sections *0* and **Error! Reference source not found.**, respectively. A network or PC issue likely exists. firewall may be blocking Port 123 (NTP traffic), for example.

4. NTP in NetClock must be "in sync" and at a higher Stratum level than Stratum 16 (such as Stratum 1 or 2, for example). This requires NetClock to be either synced to its input references or in Holdover mode. Check the current NTP stratum level and the sync status.

Section 11: Using HyperTerminal to Connect to NetClock

In Microsoft Windows versions up to and including Windows XP, the HyperTerminal program is typically located under Accessories → Communications in the Windows PC Start Menu.

NOTE: Starting with the release of Windows Vista, Microsoft discontinued including the HyperTerminal program along with the operating system. For this reason, if you are using a Windows operating system that was released after Windows XP (e.g., any version of Windows Vista or Windows 7, etc), you may need to use an alternative terminal emulator program in order to establish serial port connections with the NetClock. Many terminal emulation programs are freely available and downloadable from the web that can be used for this purpose. Once you've obtained a suitable program, the same general instructions listed in this section can be followed.

Establish a new connection using the serial port to which you have connected the NetClock (typically COM1).

Figure 11-1: Establishing a New Terminal Connection with HyperTerminal

Figure 11-2: Connecting to the Computer's Serial Port

Configure the COM1 properties using the following options (see Figure 11-3). Refer to Section 12: for a list of all available serial commands.

- **Bits per second:** 9600
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** None

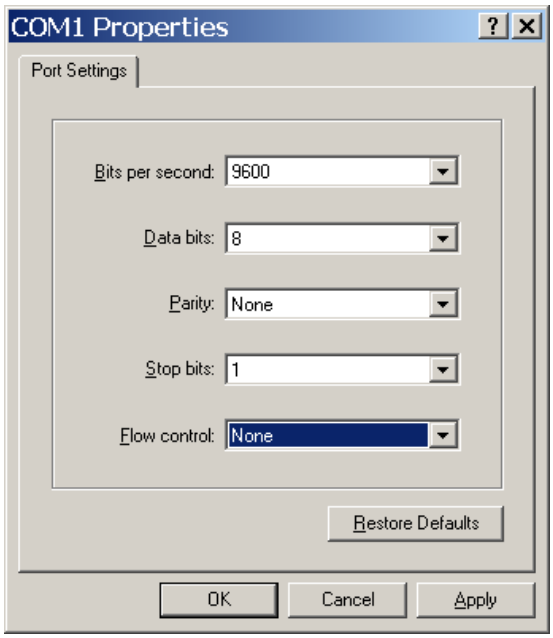


Figure 11-3: Configuring the Serial Port Connection Properties

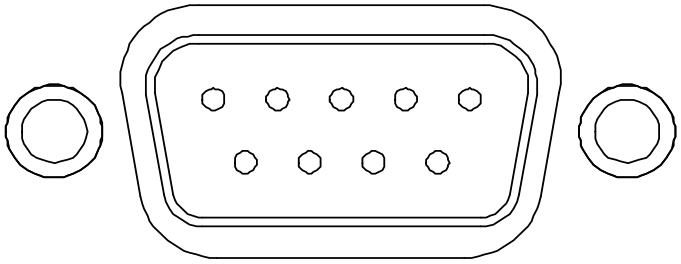


Figure 11-4: Serial Port Pin Configuration

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

Table 11-1: Setup Port Cable Pin-Outs

Section 12: NetClock 9400 Series Commands

The NetClock 9400 Series products feature a suite of command line interface (CLI) commands that can be used to set certain options or get status information, via serial cable connections or a remote connection such as **`telnet`** or **`ssh`** (if enabled). This section includes information and details regarding the usage of these commands.

Notes:

1. Typing "**`helpcli`**" will provide a list of all available commands and their syntax (note: typing "**`help`**" will output bash shell help only and will not provide useful information).

2. You can scroll up or scroll down through the output by using the Page Up / Page down keys, or the arrow keys.

3. Type "**`q`**" (lower-case) to quit.

4. Pressing the up / down keys scrolls through previously typed commands.

5. Commands need to be typed in all lower-case letters.

6. Where **`eth0`** is the base network port and **`eth1`** (and higher) are used with the optional Gigabit Ethernet module for multiple network interfaces.

7. User accounts with "user" group permissions can perform "**`get`**" commands but cannot perform any "**`set`**" commands or change / reset passwords. Only user accounts with "admin" group permissions can perform "**`set`**" commands or change / reset password. Refer to Section *3.14*: "*User Accounts*" for user account setup information.

`list:` Outputs a list of available serial port commands.

Command	Description
`clean`	Restores NetClock configuration to factory defaults and reboots.
`cleanhalt`	Restores NetClock configuration to factory defaults and halts.
`dateget`	Displays current date (i.e. 13 APR 2012).
`dateset`	Used to set the current date.
`defcert`	Used to create a new Spectracom self-signed SSL certificate for HTTPS in case of expiration of the original certificate.
`dhcp4get`	Displays whether the IP4 Ethernet port is enabled.
`dhcp4set`	Used to enable or disable the IP4 Ethernet port.
`dns4get`	Displays the configured DNS servers.
`dns4set`	Used to configure the DNS servers.

dhcp6get	Displays whether DHCPv6 is enabled.
dhcp6set	Used to enable or disable DHCPv6
doyget	Used to obtain the current Day of Year.
doyset	Used to set the current Day of Year.
gpsdop	Displays GPS receiver positional accuracy estimates.
gpsinfo	Not currently supported.
gpsloc	Displays GPS latitude, Longitude and antenna height.
gpsmdl	Displays the GPS Manufacturer and Model.
gpssat	Displays GPS satellites tracked and maximum signal strength being received.
gw4get	Displays IPv4 gateway addresses.
gw4set	Used to configure the IPv4 gateway addresses.
gw6get	Displays IPv6 gateway address.
gw6set	Used to configure the IPv6 gateway address.
halt	Used to Halt the system for shutdown.
helpcli	Provides list of available commands and syntax.
hostget	Displays the DNS hostname.
hostset	Sets the DNS hostname.
ip4get	Displays IPv4 Ethernet port information (IP address, net mask and gateway).
ip4set	Used to setIPv4 Ethernet port information (IP address, net mask and gateway).
ip6add	Used to add IPv6 Ethernet port information (IP address, net mask and gateway).
ip6del	Used to delete IPv6 IP address.
ip6get	Used to obtain the IPv6 IP address.
licenses	Displays configured licenses installed (if any).
list	Displays a simple list of commands.
loadconf	Restore a saved configuration and reboot.
localget	Used to obtain the configured local clock.
locallist	Used to display local clocks.
localset	Used to configure local clocks.
model	Displays the units Serial Number.
net	Displays network settings.
netnum	Displays the number of general-purpose network interfaces.

net4	Displays IPv4 network settings.
net6	Displays IPv6 network settings.
options	Displays configured options installed (if any).
oscget	Displays the installed system oscillator.
portget	Display whether network port is enabled.
portset	Used to enable or disable a network port.
portstate	Display the current state for a network port.
ppsctrl	Enable / disable individual 1PPS output signals.
priorset	Sets the priority of an entry in the reference priority table.
reboot	Used to warm-boot the unit without having to disconnect or reconnect power.
reftable	Displays reference priority table.
release4	Used with DHCP to release the IPv4 address.
reftable	Displays reference priority table.
release4	Used with DHCP to release the IPv4 address.
release6	Used with DHCPv6 to release the IPv6 address.
renew4	Used with DHCP to keep the assigned IPv4 address.
resetpw	Resets the administrator account (spadmin) password back to the default value "admin123".
routes4	Displays the current IPv4 routing table(s).
rt4add	Adds an IPv4 static route.
rt4del	Deletes an IPv4 static route.
rt4get	Displays the configured IPv4 static routes.
saveconf	Generate archive of current configuration.
savelog	Generate archive of all log files.
scaleget	Displays configured system timescale.
scaleset	Used to configure the system timescale.
services	Displays the state of services (enabled / disabled).
servget	Displays the status of individual services.
servset	Enable or disable specific services.
slaacget	Displays whether SLAAC is enabled.
slaacset	Used to enable or disable SLAAC.

stateset	Enable or disable an entry in the reference priority table. index = 0..15 state = 0 (disable), 1 (enable)
status	Displays information about the oscillator disciplining.
syncstate	Display timing system synchronization state.
sysupgrade	Performs system upgrade using the update bundle provided.
testevent	Generates SNMP events in the enterprise MIB.
tfomget	Displays current estimated system time error (TFOM - Time Figure of Merit).
timeget	Displays current system time (time is displayed in the configured timescale – See **scaleget** command to retrieve the configured timescale).
timeset	Used to manually set the current time (hours, minutes in seconds); time is entered based on the configured timescale – See **scaleget** command to retrieve the configured timescale.
unrestrict	Used for clearing access control restrictions to the NetClock.
version	Displays the installed main NetClock and timing system software versions.
yearget	Displays the current year.
yearset	Used to set the current year.

Section 13: ASCII Data Formats for use with the ASCII RS-485 and RS-232 Input/Outputs

This section describes each of the Data Format selections available for use with the ASCII Input/Output timecode option modules (these are the ASCII data streams accepted as inputs to the modules and available as outputs from the modules).

Three NMEA (National Marine Electronics Association) Formats and ten different Spectracom Data Formats are available for selection. The three available NMEA Formats are GGA, RMC and ZDA. The available Spectracom Data Formats are Formats 0, 1, 1S, 2, 3, 4, 7, 8, 9, BBC EndRun formats, and GSSIP formats used for SINCGARS compatibility.

13.1 NMEA GGA Message

Format GGA provides essential fix data which includes 3D location and accuracy data.

Example message:

$GPGGA,123519.00,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47

Where:

GGA	=	Global Positioning System Fix Data
123519.00	=	Fix taken at 12:35:19 UTC
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
1	=	Fix quality: 0 = Invalid 1 = GPS fix (SPS) 2 = DGPS fix 3 = PPS fix 4 = Real Time Kinematic 6 = estimated (dead reckoning) (2.3 feature) 7 = Manual input mode 8 = Simulation mode
08	=	Number of satellites being tracked
0.9	=	Horizontal dilution of position
545.4,M	=	Altitude, Meters, above mean sea level
46.9,M	=	Height of geoid (mean sea level) above WGS84 ellipsoid
(empty field)	=	Time in seconds since last DGPS update
(empty field)	=	DGPS station ID number
***47**	=	The checksum data, always begins with *

13.2 NMEA RMC Message

NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information.

Example message:

$GPRMC,123519.00,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A

Where:

RMC	=	Recommended Minimum sentence C
123519.00	=	Fix taken at 12:35:19 UTC
A	=	Status A=active or V=Void.
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
022.4	=	Speed over the ground in knots
084.4	=	Track angle in degrees True
230394	=	Date - 23rd of March 1994
003.1,W	=	Magnetic Variation
***6A**	=	The checksum data, always begins with *

13.3 NMEA ZDA Message

The Format ZDA Data message provides Date and Time information.

Example message:

$GPZDA,HHMMSS.00,DD,MM,YYYY,XX,YY*CC

Where:

HHMMSS.00	=	HrMinSec(UTC)
DD,MM,YYYY	=	Day,Month,Year
XX	=	Local zone hours -13..13
YY	=	Local zone minutes 0..59
***CC**	=	Checksum

13.4 Spectracom 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:

Example message:

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 manually 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

13.5 Spectracom Format 1

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.

Available Formats 1 and 1S are very similar to each other. 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 (i.e., 01, 02 etc.), select Format 1.
- If your device requires the single digit day of the month for days 1 through 9 (i.e., ^1, ^2, etc.), select Format 1S instead. Refer to Section *13.6* for information on Format 1S.

Format 1 data structure:

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

Where:

CR	=	Carriage Return
LF	=	Line Feed
I	=	Time Sync Status (space, ?, *)
^	=	Space separator
WWW	=	Day of Week (SUN, MON, TUE, WED, THU, FRI, SAT)
DD	=	Numerical Day of Month (01-31)
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

13.6 Spectracom Format 1S

Format 1S (Space) is very similar to Format 1, with the exception of a space being the first character of Days 1 through 9 of each month (instead of the leading "0" which is present in Format 1).

Available Formats 1 and 1S are very similar to each other. 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 single digit day of the month for days 1 through 9 (i.e., 1, 2, etc.), select Format 1S.

- If your device requires the two digit day of the month for days 1 through 9 (i.e., 01, 02, etc.), select Format 1 instead. Refer to Section *13.5* for information on Format 1.

Example message:

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

Where:

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

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

The time 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

13.7 Spectracom 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.

Example 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)
:	=	Colon separator
SS	=	(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. The "*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)	OCXO Error (milliseconds)	Rubidium Error (microseconds)
Space	Lock	<0.01	<0.3
A	<10	<0.72	<1.8
B	<100	<7.2	<18
C	<500	<36	<90
D	>500	>36	>90

Table 13-1: 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.

13.8 Spectracom 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:

Example message:

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 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 time difference from UTC, ±HHMM, is selected when the Serial Com 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 for the end of the month.
L = When a leap second correction is scheduled for the end of the month.

Example: **0003 20010415 124536-0500D #**

The example data stream provides the following information:

Data Format: 3
Sync Status: Day 271 of year 2001.
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.

13.9 Spectracom 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
^	=	Space separator
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 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.

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.

13.10 Spectracom 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.

Example 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.

13.11 Spectracom 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:

(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.

13.12 Spectracom Format 9

Format 9 provides Day of Year and time information.

Example message:

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

Where:

SOH	=	Start of header (ASCII Character 1)
DDD	=	Day of Year (001-366)
:	=	Colon Separator
HH	=	Hours (00-23)
MM	=	Minutes (00-59)
SS	=	Seconds (00-59), (00-60 for leap second)
Q	=	Time Sync Status (space = SYNC, '.' = NOT IN SYNC, '*'=NOT IN SYNC, '#' = NOT IN SYNC, "?" = NOT IN SYNC)
CR	=	Carriage Return (ASCII Character 13)
LF	=	Line Feed (ASCII Character 10)

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

13.13 BBC Message Formats

13.13.1 Format BBC-01

This format provides year, month, day, day of week, day of month, hours, minutes, and seconds.

Example message:

T:ye:mo:da:dw:ho:mi:sc

Where:

T	=	Indicates the synchronous moment for the time setting.
ye	=	Year (00 - 99)
mo	=	Month (01 - 12)
da	=	Day of month (01 - 31)
dw	=	Day of week (01=Monday to 7=Sunday)
ho	=	Hours (00 - 23)
mi	=	Minutes (00 - 59)
sc	=	Seconds (00 - 59)

13.13.2 Format BBC-02

This is a hexadecimal frame / message sent twice per second. The message should be sent such that the final "99" occurs at 0 msec and 500 msec.

Format:

START		Year		Month	Day	Hour	Min.	Sec.
AA	**AA**	**07**	**DA**	**06**	**16**	**13**	**59**	**01**

Millisecond		Time Zone		Daylight	Leap-second Sign	Leap-second Month	Leap-Second Zone	GPS Week	
02	**BA**	**80**	**00**	**00**	**00**	**00**	**00**	**1A**	**2A**

GPS Second			GPS to UTC Offset	Check-sum	END	
09	**3A**	**7E**	**12**	**FE**	**99**	**99**

Where:

Leap Second Sign:
01=Positive
FF=Negative,

00=No leap second

Leap Second Month:
00=None scheduled
03=March
06=June
09=September
0C=December

Leap Second Zone:
0=Out of zone
1=Within zone
Zone is 15 minutes before to 15 minutes after a leap second.

GPS Week: Up to FFFF
GPS Second: Second of week 000000 up to 093A7F (604799 decimal)
GPS to UTC offset: 2's complement binary signed integer, seconds
Checksum: Sum of all bytes up to and including the checksum (sum includes the **AAAA** start identifier but excludes the 9999 end identifier)

13.13.3 Format BBC-03 PSTN

The third format is a string ASCII characters and is sent on a received character.

The message should be advanced by an appropriate number such that the stop bit of each **<CR>** occurs at the start of the next second. For example, at 300 baud, 8 data bits, 1 stop bit, and no parity, each bytes takes 10/300s=33ms, so the **<CR>** byte should be advanced by 33ms in order for the **<CR>**'s stop bit to line up with the start of the next second.

Time information is available in UTC format or UK TOD format.

't' command

Input format: **t<CR>**

Output format:

Current Second	Second + 1	Second + 2	Second + 3
<CR>	**HHMMSS<CR>**	**HHMMSS<CR>**	**HHMMSS<CR>**

Number of characters: 7 (including CR)

Each **HHMMSS** filed refers to the time at the start of the next second. The data transmitted by the NetClock is timed so that the stop bit of each **<CR>** ends at the start of the next second.

'd' command

The NetClock transmits the date on request.

Input format: **d<CR>**

Output format: **YYMMDD<CR>**

Number of output characters: 7 (including CR)

's' command

The NetClock transmits the status information on request.

Input format: **s<CR>**
Output Format: **status**

Number of output characters: 1

Where returned value for **status** are:

G = System Good
D = Failure of NetClock internal diagnostics
T = NetClock does not have correct time

'l' command

The loopback command will cause the NetClock to echo the next character received back to the caller. This may be used by a caller's equipment to calculate the round trip delay across the PSTN connection in order to apply a correction to the received time data.

Input format: **l<CR>**
Output format: (Next character received)

'hu' command

The hang up command will cause the NetClock to drop the line immediately and terminate the call.

Input format: **hu<CR>**

Format BBC-04

The first format is a string of ASCII characters and is sent once per second.

Example message: **T:ho:mi:sc:dw:da:mo:ye:lp:cs<CR><LF>**

Where:

T	=	Indicates the synchronous moment for the time setting.
ho	=	Hours (00 - 23)
mi	=	Minutes (00 - 59)
sc	=	Seconds (00 - 59)
dw	=	Day of week (01=Monday to 7=Sunday)
da	=	Day of month (01 - 31)
mo	=	Month (01 - 12)
ye	=	Year (00 - 99)

lp	=	0 (for 60s, no leap) or 1 (for 61s, leap)
cs	=	Checksum. This is calculated from the start of the message, including start identifier and excluding CRLF. It is created by adding all the 1s. If he sum is even, 0 is returned. If the sum is odd, 1 is returned. This is mathematically the same as sequentially running an XOR on each bit of each byte..

Standard Serial configuration is:

- RS-232 format
- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

13.13.4 Format BBC-05 (NMEA RMC Message)

NMEA Message Format RMC, (Recommended Minimum) provides fix information, speed over ground and Magnetic Variance information. Note that this RMC Message is not exactly the same as the official NMEA RMC MESSAGE (that correspond to the 3.01 NMEA 0183 standard and is also available in the setup menu list).

The specific BBC RMC message (BBC-05) corresponds to version 2 of the NMEA 0183 standard, following the description below:

Example message:

```
$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
```

Where:

RMC	=	Recommended Minimum sentence C
123519	=	Fix taken at 12:35:19 UTC
A	=	Status A=active or V=Void.
4807.038,N	=	Latitude 48 deg 07.038' N
01131.000,E	=	Longitude 11 deg 31.000' E
22.4	=	Speed over the ground in knots
84.4	=	Track angle in degrees True
230394	=	Date—23rd of March 1994
003.1,W	=	Magnetic Variation
*6A	=	The checksum data, always begins with *

13.14 GSSIP Message Format

The ASCII Outputs support 3 ICD-GPS-153C (GPS STANDARD SERIAL INTERFACE PROTOCOL – GSSIP) messages which are used to support emulation of a SAASM GPS used in a SINCGARS interface. The messages are the Buffer Box (253), Time Transfer (5101), and the Current Status (5040).

The ICD-GPS-153C defines the format of these messages. The Current Status and Time Transfer are sent once per second (1HZ). The Buffer Box is sent once every 6 seconds (1/6 HZ).

The purpose of these three messages is to emulate a SINCGARS interface connection to a SAASM GPS. The NetClock generates these messages emulating the Time and 1PPS transfer behavior of the SINCGARS interface. An external device compatible with the SINCGARS interface can attach to an ASCII Output from the NetClock and receive time and 1PPS as if communicating with and ICD-GPS-153C compatible SAASM GPS. These commands are emulated only and contain only time information. No Position or Velocity information is provided. No SAASM GPS receiver is required because this is emulation and no controlled data is included in the messages. Position and Velocity information is zeroed out.
The ASCII Output supports two configurations for supporting SINCGARS:

Configure Time Transfer as Message Format1 and Current Status as Format2 results in an emulation of the SINCGARS protocol and initialization state machine.

Format1: Time Transfer (5101)
Format2: Current Status (5040)
Format3: Buffer Box (253)

Configure Current Status as Message Format1 and Time Transfer as Format2 results in broadcast of the messages Current Status (1HZ), Time Transfer (1HZ), and Buffer Box (1/6HZ) at their default rates.

Format1: Current Status (5040)
Format2: Time Transfer (5101)
Format3: Buffer Box (253)

13.15 EndRun Formats

The following formats provide compatibility with EndRun technology.

13.15.1 EndRun Time Format

Example message:

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

Where:

T	=	Time Figure of Merit character (TFOM), limited to the range 6 to 9: 9 indicates error > +/ - 10 milliseconds, or unsynchronized condition 8 indicates error < +/ - 10 milliseconds 7 indicates error < +/ - 1 millisecond 6 indicates error < +/ - 100 microseconds
YYYY	=	Year
DDD	=	Day of Year (001-366)
HH	=	Hour of the day (00-23)
:	=	Colon Separator
MM	=	Minutes of the hour
SS	=	Seconds (00-59), (00-60 for leap second)
z	=	The sign of the offset to UTC, + implies time is ahead of UTC
ZZ	=	The magnitude of the offset to UTC in units of half-hours. If **ZZ** = 0, then **z** = +
m	=	Timemode character and is one of: G = GPS L = Local U = UTC T = TAI
CR	=	Carriage Return
LF	=	Line Feed

13.15.2 EndRunX (Extended) Time Format

The EndRunX format is identical to the EndRun format, with the addition of two fields - the current leap second settings and the future leap second settings.

The following example message string is sent once each second:

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

Where:

T	=	Time Figure of Merit character (TFOM), limited to the range 6 to 9: 9 indicates error > +/ - 10 milliseconds, or unsynchronized condition 8 indicates error < +/ - 10 milliseconds 7 indicates error < +/ - 1 millisecond 6 indicates error < +/ - 100 microseconds
YYYY	=	Year
DDD	=	Day of Year (001-366)
HH	=	Hour of the day (00-23)
:	=	Colon Separator
MM	=	Minutes of the hour (00-59)
SS	=	Seconds (00-59), (00-60 for leap second)
z	=	The sign of the offset to UTC, + implies time is ahead of UTC
ZZ	=	The magnitude of the offset to UTC in units of half-hours. If **zz** = 0, then **z** = +
m	=	Timemode character and is one of: G = GPS L = Local U = UTC T = TAI
CC	=	The current leap seconds.
FF	=	The future leap seconds, which will show a leap second pending 24 hours in advance
CR	=	Carriage Return
LF	=	Line Feed

Section 14: License Notices

NTPv4.2.6.p5

This file is automatically generated from html/copyright.html

Copyright Notice

jpg "Clone me," says Dolly sheepishly.

Last update: 1-Jan-2011 08:34 UTC

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) University of Delaware 1992-2011                      *
*                                                                     *
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose with or without fee is hereby     *
* granted, provided that the above copyright notice appears in all    *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name        *
* University of Delaware not be used in advertising or publicity      *
* pertaining to distribution of the software without specific,        *
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
* warranty.                                                           *
*                                                                     *
***********************************************************************
```

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

1. [1]Takao Abe <takao_abe@xurb.jp> Clock driver for JJY receivers
2. [2]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
3. [3]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
4. [4]Viraj Bais <vbais@mailman1.intel.com> and [5]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
5. [6]Michael Barone <michael,barone@lmco.com> GPSVME fixes
6. [7]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. [8]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
8. [9]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. [10]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
10. [11]Nelson B Bolyard <nelson@bolyard.me> update and complete broadcast and crypto features in sntp
11. [12]Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
12. [13]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
13. [14]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
14. [15]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
15. [16]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
16. [17]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
17. [18]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
18. [19]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
19. [20]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
20. [21]Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
21. [22]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
22. [23]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
23. [24]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
24. [25]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
25. [26]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
26. [27]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [28]<H.Lambermont@chello.nl> ntpsweep
27. [29]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
28. [30]Frank Kardel [31]<kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
29. [32]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
30. [33]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
31. [34]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
32. [35]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
33. [36]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
34. [37]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
35. [38]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
36. [39]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
37. [40]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
38. [41]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
39. [42]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
40. [43]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
41. [44]Derek Mulcahy <derek@toybox.demon.co.uk> and [45]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
42. [46]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
43. [47]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
44. [48]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
45. [49]Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
46. [50]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
47. [51]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
48. [52]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
49. [53]Michael Shields <shields@tembel.org> USNO clock driver
50. [54]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
51. [55]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
52. [56]Kenneth Stone <ken@sdd.hp.com> HP-UX port
53. [57]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
54. [58]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
55. [59]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
56. [60]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

---

[53]gif

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

References

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

OpenSSH

This file is part of the OpenSSH software.

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

OpenSSH contains no GPL code.

1)

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

```
 * called by a name other than "ssh" or "Secure Shell".

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

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

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

[The licence continues]

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

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

                                NO WARRANTY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *  notice, this list of conditions and the following disclaimer.
```

```
   * 2. Redistributions in binary form must reproduce the above copyright
   *  notice, this list of conditions and the following disclaimer in the
   *  documentation and/or other materials provided with the distribution.
   *
   * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
   * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
   * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
   * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
   * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
   * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
   * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
   * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
   * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
   * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

OpenSSL

```
LICENSE ISSUES
==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

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

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

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

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

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

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----
Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* Neither the name of the Networks Associates Technology, Inc nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
```

IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----
Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.
Use is subject to license terms below.
This distribution may include materials developed by third parties.
Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered
trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* Neither the name of the Sun Microsystems, Inc. nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

Document Revision History			
Rev	***ECN***	***Description***	***Date***
A	2698	*First-generation of Instruction Manual for the NetClock 9483 / 9400 Product series.*	September 2011
B	2827	*Added updates that coincide with the release of NetClock Model 9489. Additional corrections and document maintenance.*	January 2012
C	2973	*Updates coinciding with latest software release and general document maintenance.*	June 2012
D	3019	*Updates coinciding with latest software release. Updated warranty, feature, and specification information, PTP information sections, adjusted IRIG reference information sections.*	September 2012
E	3103	*General updates, enhancements coinciding with latest software release.*	December 2012
F	3250	*General updates, enhancements coinciding with latest software release.*	September 2013
G	3411	*General updates to reflect new software release 5.1.2*	February 2014

Orolia USA, Inc.
1565 Jefferson Road, Suite 460
Rochester, NY 14623
www.spectracomcorp.com
Phone: US +1.585.321.5800
Fax: US +1.585.321.5219

An Orolia Group Business