SyncServer S6x0 Release 4.1 User Guide

SyncServer S6x0 Release 4.1 User Guide

Intro

This document explains how to install and configure a SyncServer™ S600/S650 v4.1.

Table of Contents

1. Overview

1.1 SyncServer S6x0 Models

1.1.1 SyncServer S600

Modern networks require accurate, secure and reliable time services as provided by the Microchip SyncServer™ S600. The security hardened S600 network time server is purpose built to deliver exact hardware-based NTP time stamps. The unparalleled accuracy and security is rounded out with outstanding ease-of-use features for reliable network time services ready to meet the needs of your network and business operations today and tomorrow.

1.1.2 SyncServer S650

The modular Microchip SyncServer™ S650 combines the best of time and frequency instrumentation with unique flexibility and powerful network/security based features.

The base Timing I/O module with 8 BNC connectors comes standard with the most popular timing I/O signals (IRIG B, 10MHz, 1PPS, etc.). When more flexibility is required, the unique Microchip FlexPort™ Technology option enables 6 of the BNCs to output any supported signal (time codes, sine waves, programmable rates, etc.) all configurable in real time via the secure web interface. This incredibly flexible BNC by BNC configuration makes very efficient and cost effective use of the 1U space available. Similar functionality is applied to the two input BNCs as well. Unlike legacy modules with fixed count BNCs outputting fixed signal types per module, with FlexPort™ Technology you can have up to 12 BNCs output any combination of supported signal types.

This level of timing signal flexibility is unprecedented and can even eliminate the need for additional signal distribution chassis and there is no degradation in the precise quality of the coherent signals.

1.1.3 SyncServer S650i

The Microchip SyncServer™ S650i is a S650 base chassis with no GNSS receiver.

1.2 SyncServer S6x0 Key Features

- <15ns RMS to UTC(USNO) for S650
- 1 x 10-12 Frequency accuracy
- Modular timing architecture with unique and innovative FlexPort™ technology (optional)
- Most popular timing signal inputs/outputs are standard in the base Timing I/O module (IRIG B, 10MHz, 1PPS, etc.) available for the S650.
- Four (4) GbE ports standard, all with NTP hardware time stamping
- Ultra high-bandwidth NTP time server
- Stratum 1 Operation via GNSS satellites
- DoS detection/protection (optional)
- Web-based management with high security cipher suite
- BlueSky Jamming /Spoofing protection
- TACACS+, RADIUS, LDAP, and more (optional)
- -20C to +65C operating temperature (Standard and OCXO)
- IPv6/ IPv4 on all ports
- Rubidium Atomic clock or OCXO oscillator upgrades
- Dual power supply option
- GPS standard and GLONASS/Galileo/QZSS/Beidou/SBAS (optional)
- Dual 10G Ethernet module option
- Low Phase Noise (LPN) module option
- Ultra Low Phase Noise (ULPN) module option

- Telecom Inputs/Outputs module option
- Timing I/O module with HaveQuick/PTTI option
- Timing I/O module with fiber outputs option
- Timing I/O module with fiber input option
- Dual DC power supply option

1.2.1 Software Options

The SyncServer S600/S650 includes built-in hardware features enabled via software license keys.

- Security Protocol License Option: The SyncServer S600/S650 can be seriously hardened from both an NTP perspective and an authentication perspective via this option. This license option includes: - NTP Reflector - high capacity and accuracy - Per port packet monitoring and limiting
- FlexPort Timing License Option: The FlexPort™ Technology option enables the 6 output BNCs (J3-J8) to output any supported signal (time codes, sine waves, programmable rates, and so on.) all configurable in real time through the secure web interface. The 2 input BNCs (J1-J2) can support a wide variety of input signal types.
- GNSS License Option: This option enables the SyncServer S600/S650 to use Galileo, GLONASS, SBAS, QZSS, and BeiDou signals, in addition to the standard GPS signal support..
- PTP Master Output License Option: This option enables PTP default profile, PTP Enterprise profile and PTP Telecom-2008 profile master functionality.
- PTP Client License: This option enables PTP client operations to be configured on an Ethernet port.
- 1PPS TI Measurement License: This license enable 1PPS measurements to be made on the J1 port of a timing card.
- Programmable Pulse Option: This license enables the time-triggered programmable pulse feature on J7 of selected timing cards.
- BlueSky GPS Spoofing Detection Option: This license enables the BlueSky jamming & spoofing detection, protection and analysis features.

See SyncServer S6x0 Part Numbers for all available options. Activation keys are associated with the serial number of the device on which the keys are stored and travel with that device. The user must enter key(s) with web interface via LAN1 port to gain access to the licensed software options web page.

1.2.2 Security Features

Security is an inherent part of the SyncServer S600/S650 architecture. In addition to standard security features related to the hardening of the web interface, NTP and server access, unsecure access protocols are deliberately omitted from the S6x0 while remaining services can be disabled. Advanced authentication services such as TACACS+, RADIUS, and LDAP are optionally available.

The four (4) standard GbE ports, and optional two (2) 10GbE ports, combined easily handle more than 10,000 NTP requests per second using hardware time stamping and compensation (360,000 is max capacity for NTP reflector, 13,000 is max capacity for NTPd). All traffic to the S6x0 CPU is bandwidth limited for protection against DoS (denial of service) attacks.

1.3 Physical Description

The SyncServer S6x0 consists of a 19-inch (48 cm) rack-mountable chassis, plug-in modules (S650 only), and hardware.

All connections for the SyncServer S6x0 are on the rear panel. is a front view of the SyncServer S600 version showing LEDs, display screen, navigation buttons and entry buttons. and show the rear panel connections for the Single AC versions of the SyncServer S600. and show the rear panel connections for the Dual AC versions of the SyncServer S600. and shows the rear panel connections for the Dual DC versions of the SyncServer S600. is a front view of the SyncServer S650 version showing LEDs, display screen, navigation buttons and entry buttons. and show the rear panel connections for the Single AC versions of the SyncServer S650. and show the rear panel connections for the Dual AC versions of the SyncServer S650. and show the rear panel connections for the Dual DC versions of the SyncServer S650.

is a front view of the SyncServer S650 version showing LEDs, display screen, navigation buttons and entry buttons. shows the rear panel connections for the Single AC version of the SyncServer S650i. shows the rear panel connections for the Dual AC version of the SyncServer S650i.

Figure 1-1. SyncServer S600 Front Panel

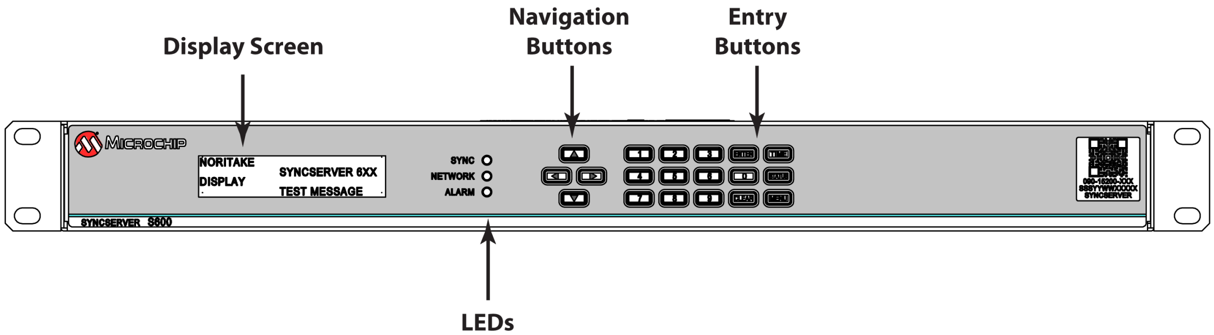


Figure 1-2. SyncServer S600 Rear Panel - Single AC Version

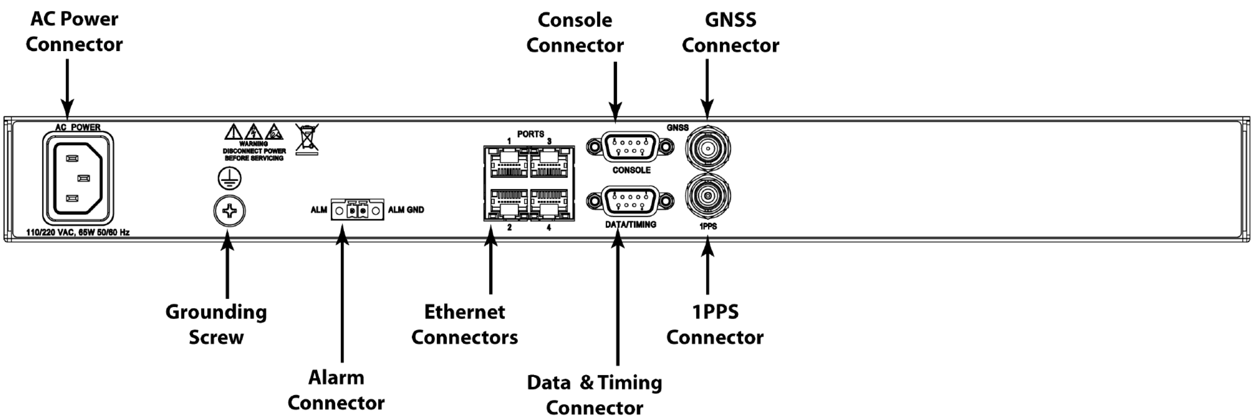


Figure 1-3. SyncServer S600 Rear Panel - Single AC Version with 10 GbE

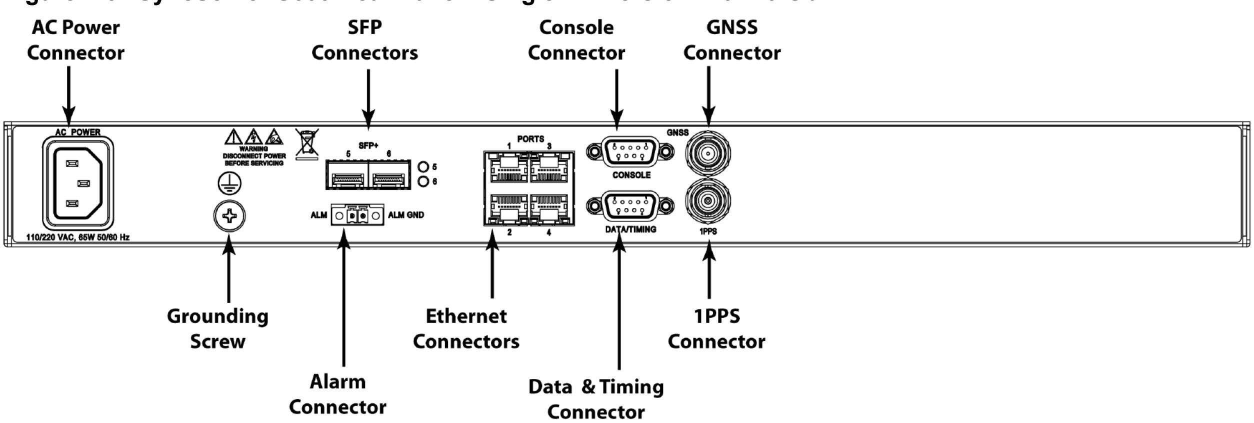


Figure 1-4. SyncServer S600 Rear Panel - Dual AC Version

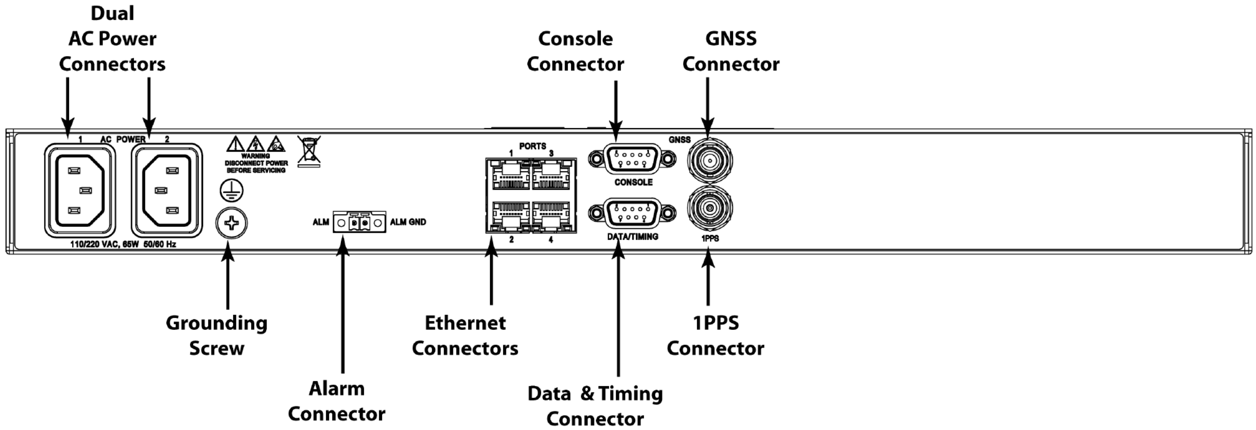


Figure 1-5. SyncServer S600 Rear Panel - Dual AC Version with 10 GbE

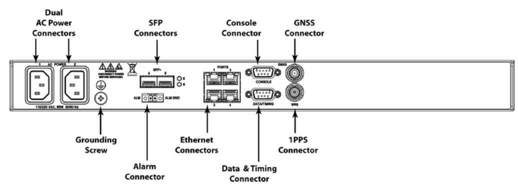


Figure 1-6. SyncServer S600 Rear Panel - Dual DC Version

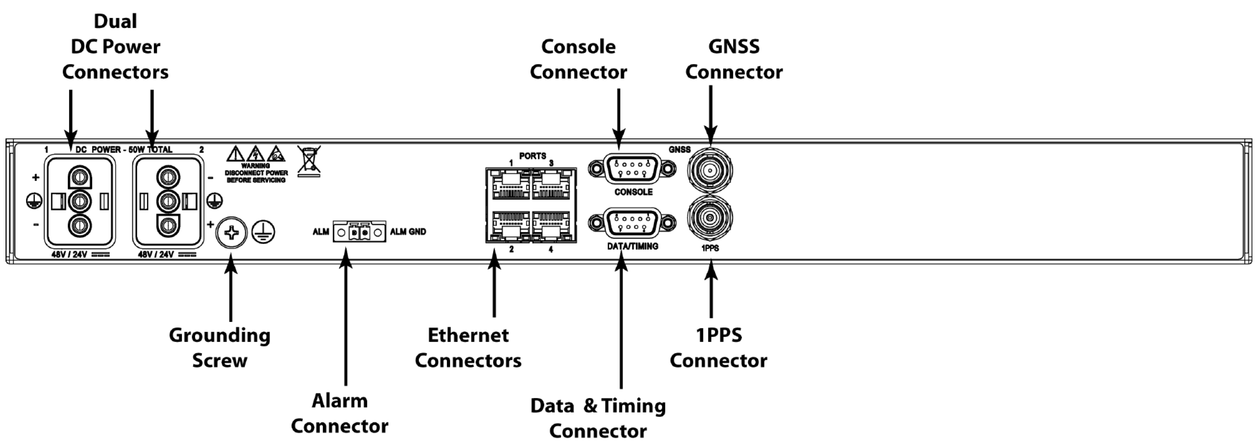


Figure 1-7. SyncServer S600 Rear Panel - Dual DC Version with 10GbE

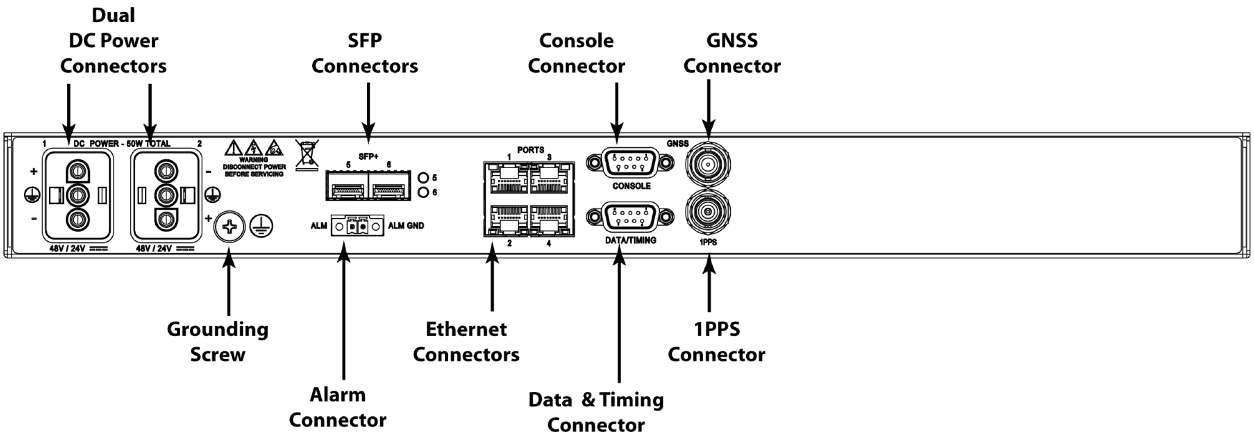


Figure 1-8. SyncServer S650 Front Panel

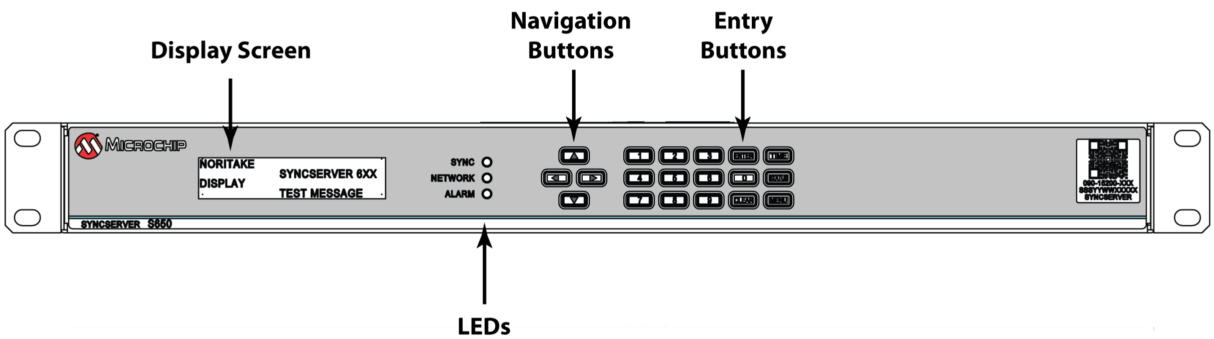


Figure 1-9. SyncServer S650 Rear Panel - Single AC Version

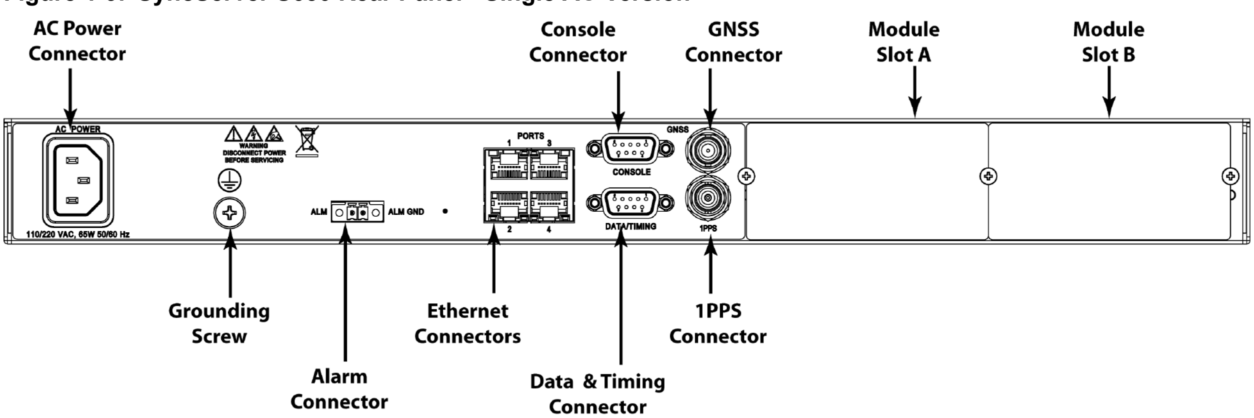


Figure 1-10. SyncServer S650 Rear Panel - Single AC Version with 10 GbE and a Timing I/O Module

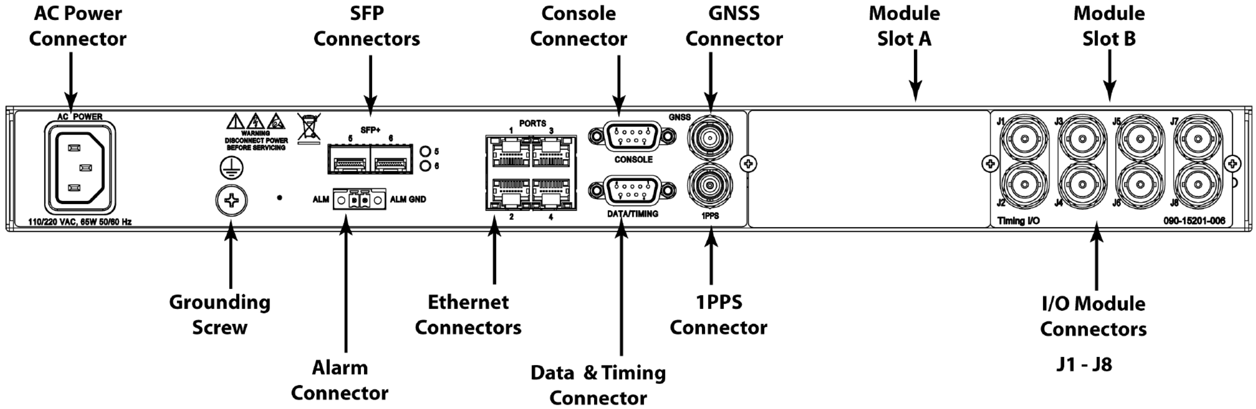


Figure 1-11. SyncServer S650 Rear Panel - Dual AC Version

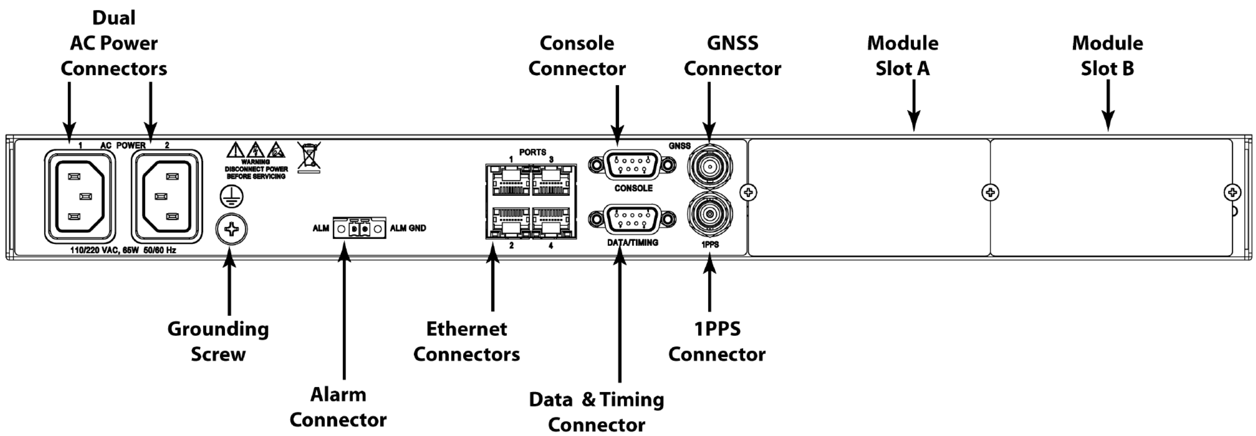


Figure 1-12. SyncServer S650 Rear Panel - Dual AC Version with 10 GbE and a Timing I/O Module

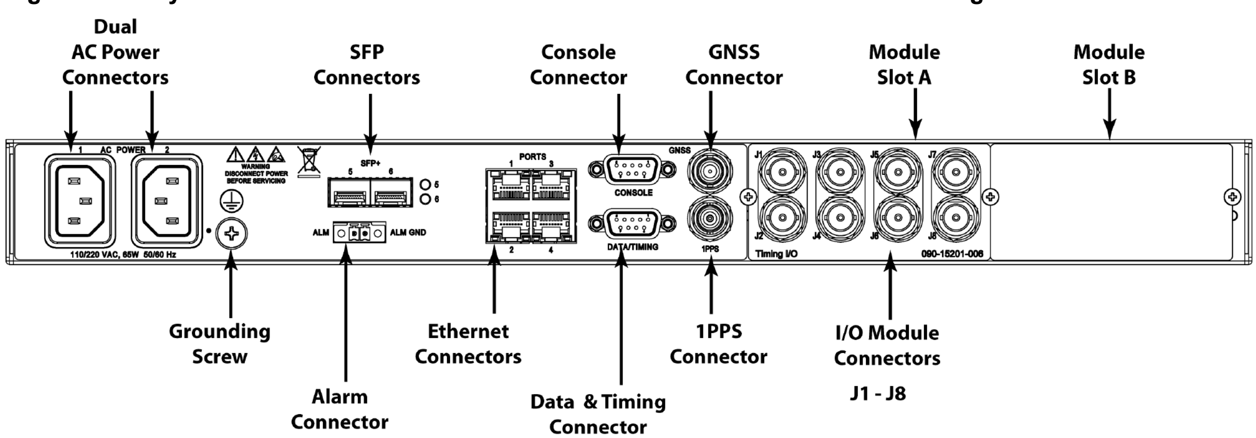


Figure 1-13. SyncServer S650 Rear Panel - Dual DC Version and a Timing I/O Module

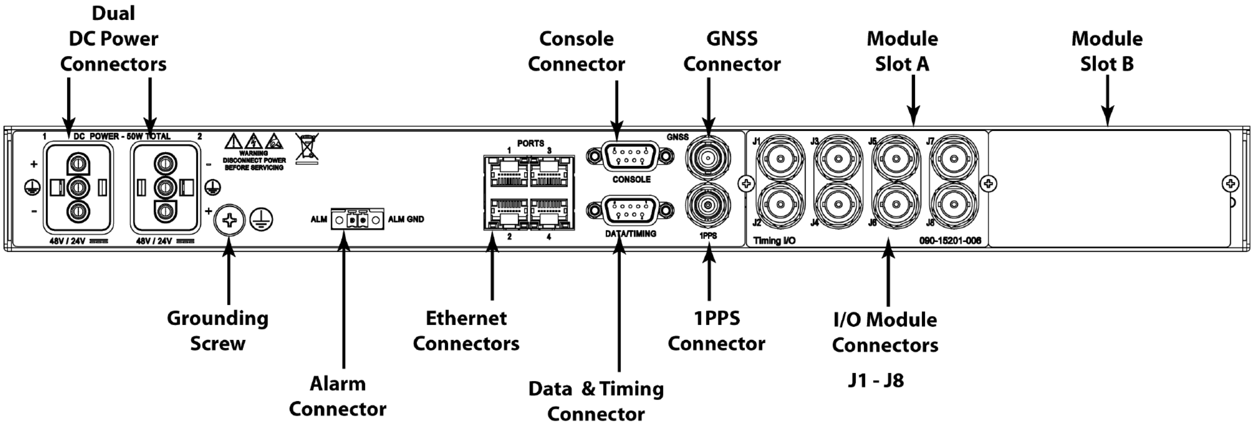


Figure 1-14. SyncServer S650 Rear Panel - Dual DC Version with 10 GbE and a Timing I/O Module

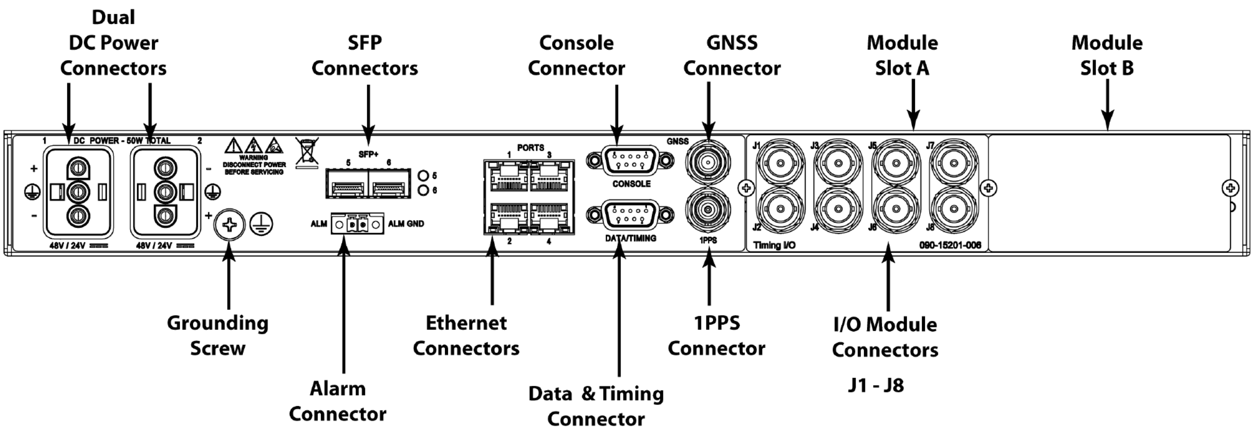


Figure 1-15. SyncServer S650i Front Panel

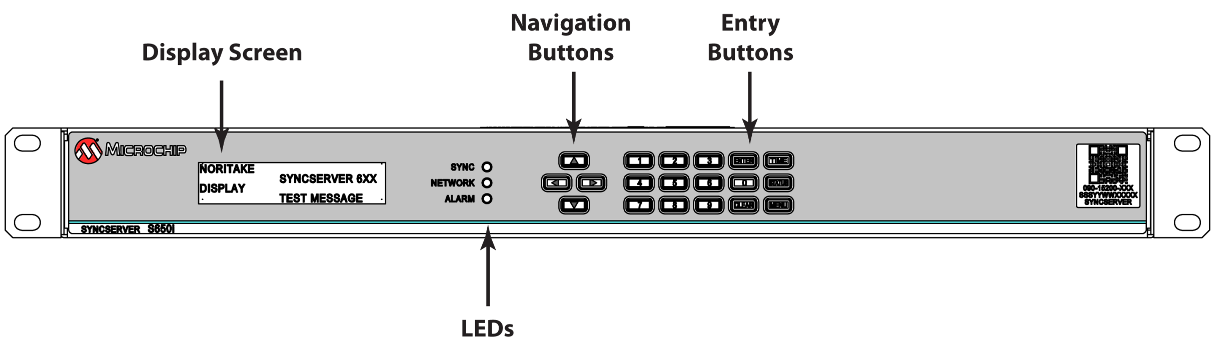


Figure 1-16. SyncServer S650i Rear Panel - Single AC Version

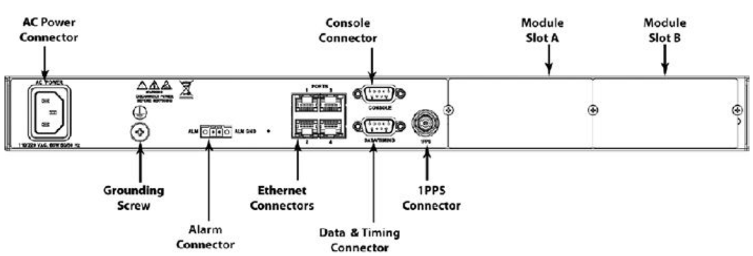
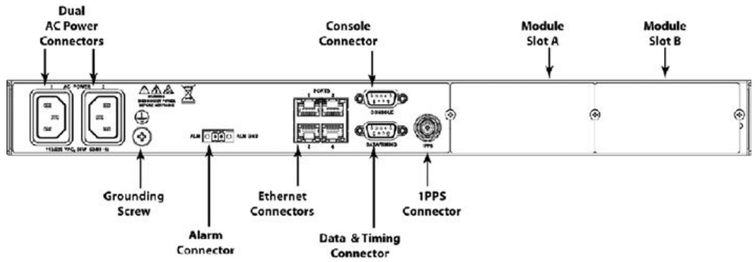


Figure 1-17. SyncServer S650i Rear Panel - Dual AC Version



1.3.1 Communications Connections

The SyncServer S6x0 is primarily controlled through the web interface available on LAN1. Limited functionality is available via the console serial port.

1.3.1.1 Ethernet Management Port - LAN1

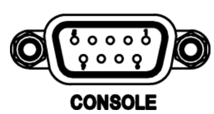
Ethernet port 1 is the management port that is used to access the web interface. This port is located on the rear panel of the SyncServer S6x0 and is a standard 100/1000 Base-T shielded RJ-45 receptacle. To connect the SyncServer S6x0 to an Ethernet network, use a standard twisted-pair Ethernet RJ-45 cable (CAT5 minimum). Configurable to 100_Full or 1000_Full or Auto :100_Full / 1000_Full.

1.3.1.2 Serial Console Port

The serial port connection is made through a DB-9 female connector on the rear panel of the SyncServer S6x0. This port, which supports a baud rate of 115.2k (115200-8-N-1), allows you to connect to a terminal or computer using a terminal emulation software package. When connecting to this port, use a shielded serial direct connect cable.

This port is also used for serial data (NENA ASCII time code, Response mode). shows the DB-9 female connector for the serial port.

Figure 1-18. Serial Port Connector



1.3.2 Output Connections

1.3.2.1 Serial Data/Timing Output Connection

The serial data/timing port connection is made through a DB-9 female connector on the rear panel of the SyncServer S6x0, as shown in the following image. When connecting to this port, use a shielded serial direct connect cable. The dedicated Data/Timing port is provided to output NMEA-0183 or NENA PSAP strings. If NENA is selected, the serial Console port also supports the two-way timing aspects of the standard. In addition, the F8 and F9 Microchip legacy time strings are available. With the optional time interval measurement option, this port can alternatively be used to send timestamps and measurements.

Figure 1-19. Serial Data/Timing Connection

1.3.2.2 1PPS Output Connection

The SyncServer S6x0 provides a BNC female, as shown in the following image.

Figure 1-20. 1PPS Output Connection

1.3.3 Input Connections

1.3.3.1 GNSS Connection

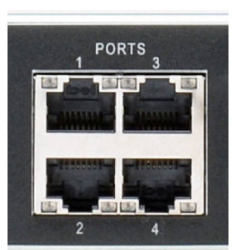
The SyncServer S6x0 features a BNC connector for input from GNSS navigation satellites to provide a frequency and time reference. This connector also provides 9.7V to power a Microchip GNSS antenna (see Antenna Kits Overview in Chapter 10, Installing GNSS Antennas). See the following image. This connector is not present on the SyncServer S650i.

Figure 1-21. GNSS Input Connection

1.3.3.2 NTP Input/Output Connections

The S600 / S650 has four dedicated and software isolated GbE Ethernet ports, each equipped with NTP hardware time stamping. These are connected to a very high-speed microprocessor and an accurate clock to assure high bandwidth NTP performance. See the following image. See Chapter 12: IP Port Details for information on Ethernet port isolation and management port rules.

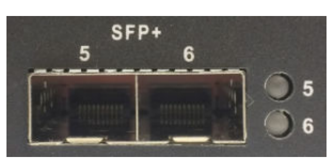
Figure 1-22. NTP Input/Output Connections



1.3.3.3 10 GbE Input/Output Connections

The S600 / S650 10 GbE option adds two SFP+ ports equipped with hardware timestamping that supports NTP, PTP, and NTP Reflector operations. The 10 GbE ports are in addition to the standard four 1 GbE ports for a total of 6 ports. These ports are ideal for interoperability with 10 GbE switches. SFP modules supported are limited to 10 GbE speeds only, and overall system time stamping capacity remains as specified.

Figure 1-23. 10 GbE Input/Output Connections



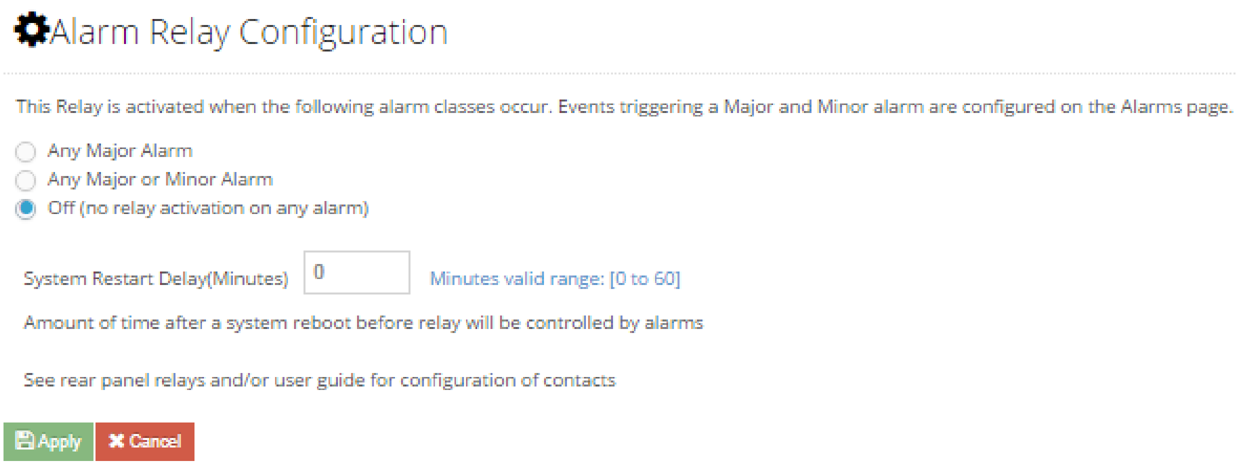
1.3.4 Alarm Relay

The SyncServer S6x0 features a Phoenix connector for an alarm relay output. See Figure 1-24. The relay is open when the configured alarm classes (Figure 1-25) occur. If the SyncServer S6x0 is not powered, then the alarm relay will be open. The relay is energized (shorted), when the SyncServer S6x0 is powered and no configured alarms are active.

Note:
The alarm relay is shorted when the alarm is active for firmware releases 1.0 and 1.1.

Figure 1-24. Alarm Relay Connector

Figure 1-25. Alarm Relay Configuration Web GUI



1.3.5 Timing I/O Card Connections

The Timing I/O Module is an exceedingly versatile time and frequency input and output option. In the standard configuration, it supports the most popular input and output time codes, sine waves, and rates.

The standard configuration offers a broad yet fixed selection of signal I/O on its eight BNC connectors (see). J1 is dedicated to time code and rate inputs, J2 to sine wave inputs, and J3-J8 to mixed signal outputs. The standard Timing I/O Module configuration is 1PPS or IRIG B AM-In, 10 MHz- In, IRIG AM and IRIG DCLS-Out, 1PPS-Out and 10 MHz-Out.

The FlexPort™ Technology option enables the 6 output BNCs (J3-J8) to output any supported signal (time codes, sine waves, programmable rates, etc.), all configurable in real time via the secure web interface. Similarly, the 2 input BNCs (J1-J2) can support a wide variety of input signal types. This uniquely flexible BNC by BNC configuration makes very efficient and cost effective use of the 1U space available.

See to view the signal types for the standard configuration and the configuration with the FlexPort™ option.

Figure 1-26. Timing I/O Module BNC Connectors

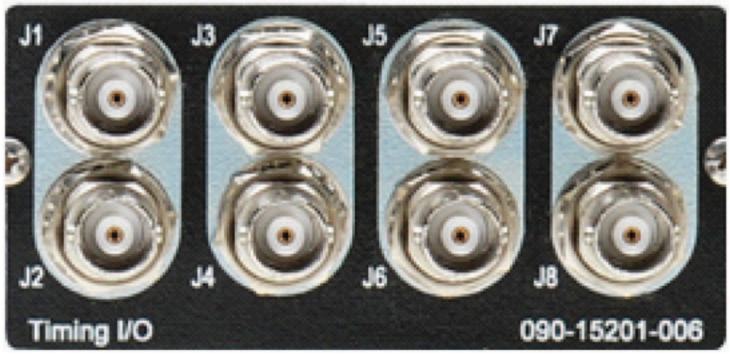
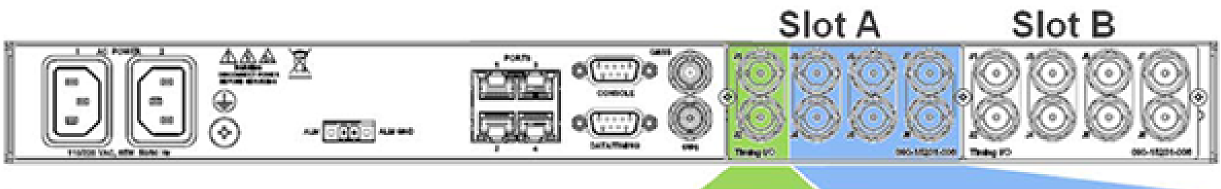


Figure 1-27. Signal Types for Timing I/O Module



→ BNC Connectors / ↓ Signals		Input J1	Input J2	Output J3	Output J4	Output J5	Output J6	Output J7	Output J8
Standard	1PPS	●					●	off	off
Standard	IRIG B AM	●		●				off	off
Standard	IRIG B DCLS					●		off	off
Standard	10 MHz		●		●			off	off
FlexPort	IRIG A/B/C37/E/G NASA/2137/XR3 AM/DCLS	■		■	■	■	■	■	■
FlexPort	Selectable/Programmable Rates	■		■	■	■	■	■	■
FlexPort	1/5/10 MHz Sine Waves		■	■	■	■	■	■	■

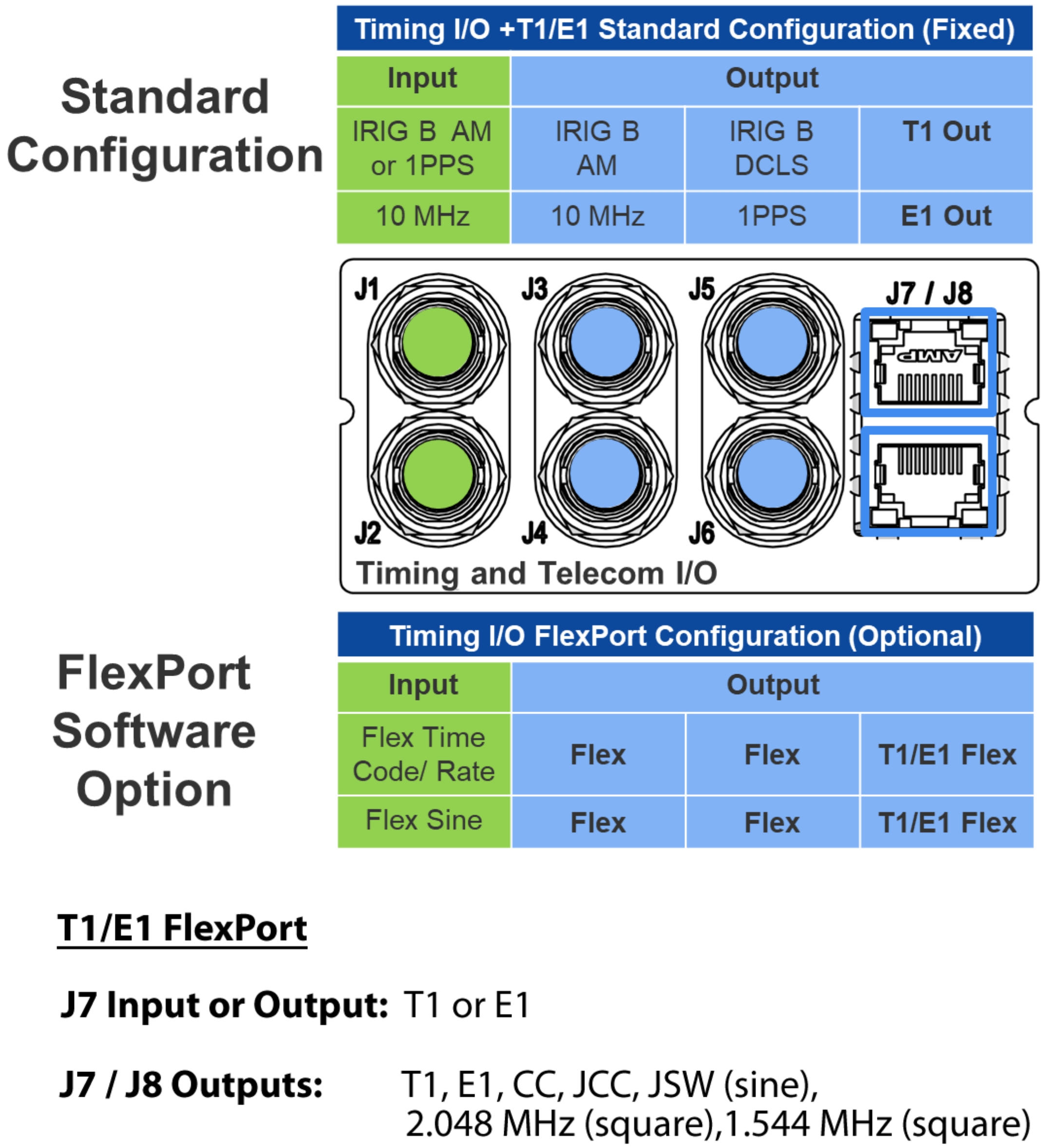
● = Fixed specific signal type
■ = User configurable Time Codes, Selectable/Programmable Rates or Sine Waves

1.3.5.1 Timing I/O Module with Telecom I/O Connections

The Timing I/O Module with Telecom I/O (090-15201-011) features six BNC ports in positions J1-J6 and two RJ-48c ports in position J7 and J8, as shown in . The standard configuration for the RJ-48C ports is J7=T1 Output and J8=E1 Output.

Ports are individually configurable for the signal formats in if FlexPorts are enabled with the FlexPort license. If the license is not installed, then J7 can only be configured for T1 output and J8 can only be configured for E1 output.

Figure 1-28. Timing I/O Module with Telecom I/O Connections



Ports J1-J6 have identical functionality to the basic Timing I/O module. See for details about configuration choices.

Table 1-1. 7 and J8 Connector Pin Assignments - Timing I/O Module with Telecom I/O Connections

Pin	Signal
1	Rx ring (not supported on J8)
2	Rx tip (not supported on J8)
3	N/C
4	Tx ring (not supported on J8)
5	Tx tip (not supported on J8)

6	N/C
7	N/C
8	N/C

1.3.5.2 Timing I/O Module with HaveQuick/PTTI Module Connections

The Timing I/O with HaveQuick/PTTI module (090-15201-012) adds support for a set of timing protocols and signals generally associated with the GPS User Equipment sector and timing interfaces intended for equipment interoperability. Within that sector definitions for a Precise Time and Time-Interval (PTTI) Interface cover an evolutionary range of signaling and protocols. A core set of revisioned documents (ICD-GPS-060) form a basis for the subject, including baseline HaveQuick and BCD interfaces and protocol definitions. This module supports many variations of this category of timing interfaces. References to STANAG (STANdard NATO AGreement) codes are variations of the core ICD-GPS-060A code.

Along with the unique HaveQuick/PTTI capabilities, this module supports all functionality that is available on J1 - J6 of the standard timing I/O module. Connections J7 and J8 uniquely provide balanced 2-wire PTTI BCD capabilities. The FlexPorts license comes pre-installed on a system containing a HaveQuick/PTTI module.

For details on HaveQuick input support on J1 and J2, see Provisioning HaveQuick Input on Timing I/O HaveQuick/PTTI Module.

For details on HaveQuick output support on J3 through J8, see Provisioning Outputs on Timing I/O HaveQuick/PTTI Module.

Figure 1-29. HaveQuick/PTTI Module Connections

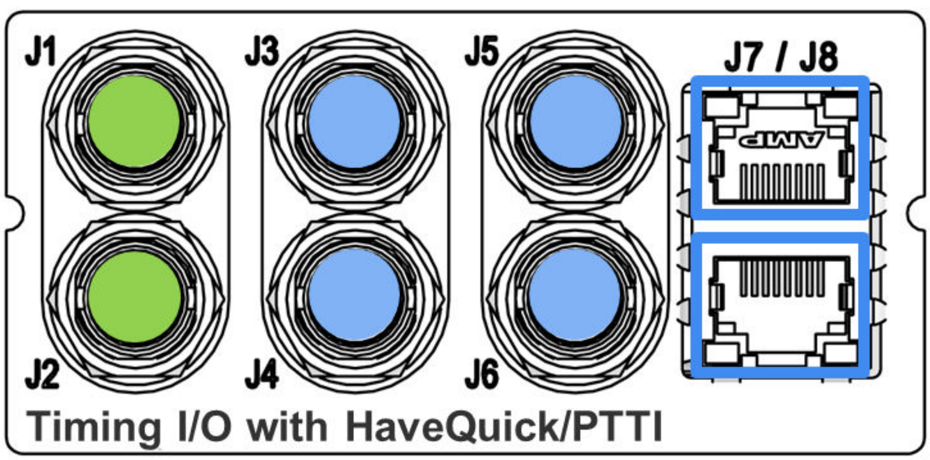


Table 1-2. HaveQuick/PTTI Module Port Descriptions

Port	Description
J1	Input same as Timing I/O module with FlexPort functionality always On, Supports TTL and 5V HaveQuick Input
J2	Input same as Timing I/O module with FlexPort functionality always On, used for 1PPS input when HaveQuick is configured on J1
J3	Output same as Timing I/O module with FlexPort functionality always On, Includes HaveQuick TTL or HaveQuick 5V outputs. Includes 10V PPS or 10V PPM output.
J4	Output same as Timing I/O module with FlexPort functionality always On, Includes HaveQuick TTL or HaveQuick 5V outputs. Includes 10V PPS or 10V PPM output.

J5	Output same as Timing I/O module with FlexPort functionality always On, Includes HaveQuick TTL or HaveQuick 5V output. Includes 10V PPS or 10V PPM output.
J6	Output same as Timing I/O module with FlexPort functionality always On, Includes HaveQuick TTL or HaveQuick 5V output. Includes 10V PPS or 10V PPM output.
J7	RS422 PTTI Output on RJ-48
J8	RS422 PTTI Output on RJ-48

Table 1-3. J7 & J8 Connector Pin Assignments - Timing I/O Module with HaveQuick/PTTI Connections

Pin	Signal
1	PTTI Tx+ (code out)
2	PTTI Tx- (code out)
3	1PPS/PPM out, TTL level (for test purposes only)
4	Ground
5	Reserved, do not connect
6	N/C
7	Reserved, do not connect
8	Reserved, do not connect

1.3.5.2.1 HaveQuickII (HQII) and Extended HaveQuick (XHQ) Timecodes

The following timecodes are supported with HaveQuick/PTTI module:

- STANAG 4246 HAVE QUICK I
- STANAG 4246 HAVE QUICK II
- STANAG 4430 Extended HAVE QUICK
- ICD-GPS-060A HAVE QUICK

1.3.5.2.2 PTTI Binary Coded Decimal (BCD)

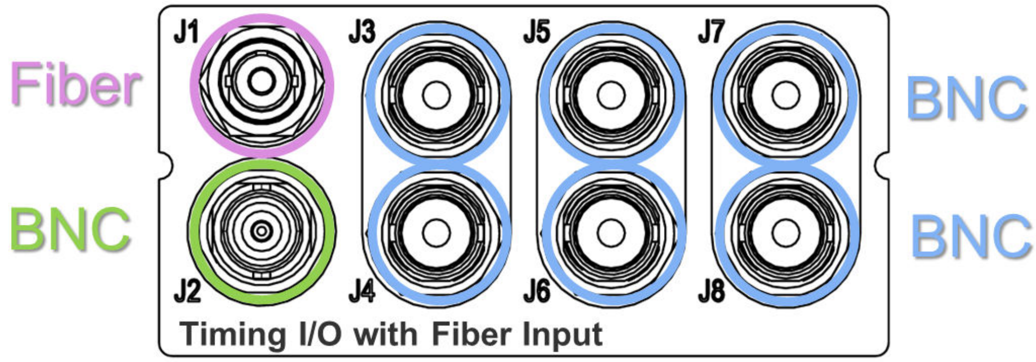
There are two different formats that are supported:

- Full - The PTTI BCD time code is a 50 bit message defining the UTC time of day, day of year, and TFOM transmitted at 50 bps.
- Abbreviated - The abbreviated PTTI BCD time code is a 24 bit message defining the UTC time of day. The day of year, and TFOM bits are set high (1) transmitted at 50 bps.

1.3.5.3 Timing I/O Modules with Fiber Connectors

There are two variations on the Timing I/O Module with fiber connectors. The 090-15201-013 has three output BNC multimode fiber connectors: J3, J5, and J7. The 090-15201-014 has a single multimode fiber connector, the J1 Input. See Figure 1-30.

Figure 1-30. Timing I/O Modules with Fiber Connections

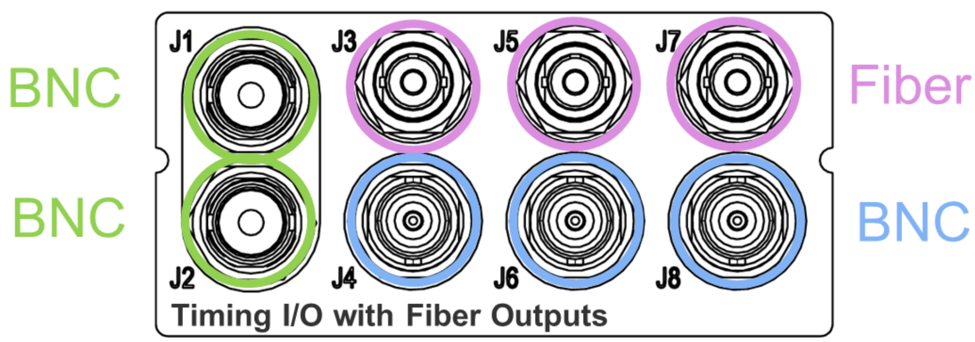


FlexPort Software Option

Timing I/O with Fiber FlexPort Configuration			
Input	Output		
DCLS IRIG + pulses	Flex	Flex	Flex
Flex Sine	Flex	Flex	Flex

Flex Timing License is Required

Figure 1-31. Timing I/O Modules with Fiber Outputs



FlexPort Software Option

Timing I/O with Fiber FlexPort Configuration			
Input	Output		
Flex Time Code/ Rate	Flex DCLS IRIG + pulses	Flex DCLS IRIG + pulses	Flex DCLS IRIG + pulses
Flex Sine	Flex	Flex	Flex

Only DCLS signals

Flex Timing License is Required

1.3.5.4 Low Phase Noise (LPN) Module Connections

The module has eight 10MHz LPN outputs (J1-J8). There are two different LPN modules available with different performance specifications.

If the S650 with the LPN or ULPN modules is equipped with an OCXO or Rb oscillator upgrade, then there is a web GUI selection to align the 10 MHz output with the 1PPS output for coherency purposes.

Figure 1-32. LPN Module Connections

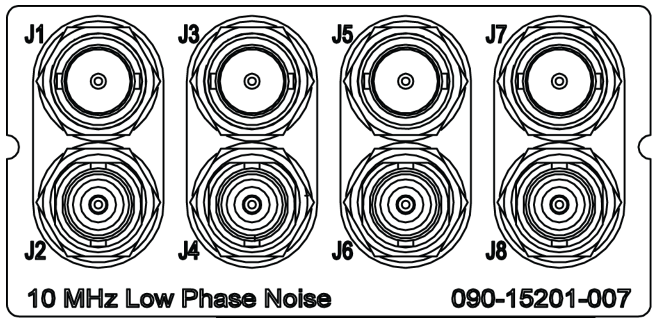
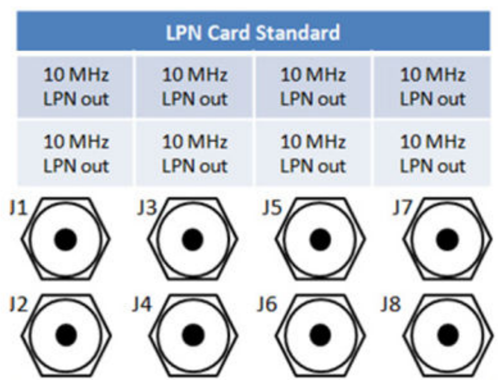


Figure 1-33. LPN Module Signal Types



1.3.6 Power and Ground Connections

The SyncServer S6x0 is available with either single or dual 120/240 VAC power, or dual DC power. The SyncServer S6x0 is not equipped with a Power switch. AC power is controlled by the unplugging the AC power cord. Frame ground connections on the SyncServer S6x0 are made on the grounding stud located on the left side of the rear panel, as identified with the international Ground marking, as shown in and .

Note:
To avoid serious personal injury or death, exercise caution when working near high voltage lines and follow local building electrical codes for grounding the chassis.

Figure 1-34. SyncServer S6x0 Single AC Version Power and Ground

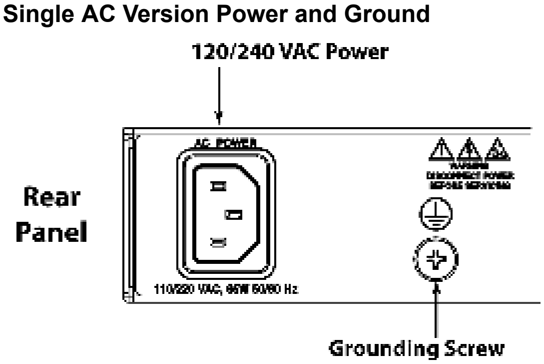


Figure 1-35. SyncServer S6x0 Dual AC Version Power and Ground

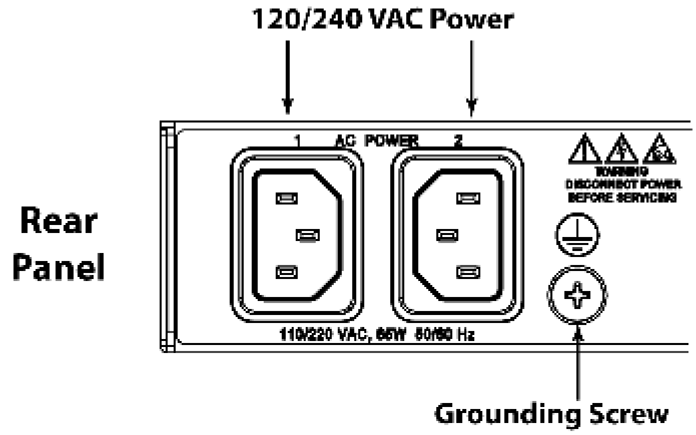
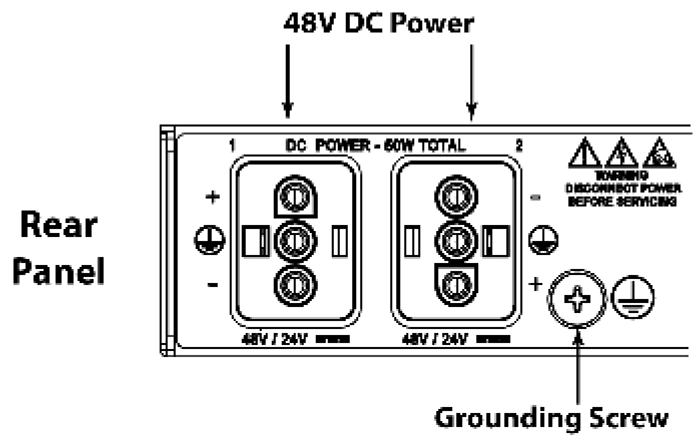


Figure 1-36. SyncServer S6x0 Dual DC Version Power and Ground



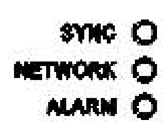
1.4 Functional Description

1.4.1 LEDs

The SyncServer S6x0 provides three LEDs on the front panel, as shown in , that indicate the following:

- Sync Status
- Network Status
- Alarm Status

Figure 1-37. LEDs for SyncServer S6x0



See for details about the LEDs.

1.4.2 Communication Ports

Communication ports on the SyncServer S6x0 allow you to provision, monitor, and troubleshoot the chassis with CLI commands.

1.4.2.1 Management Ethernet Port

The system web interface for full control is located on Ethernet port 1 (LAN1) and is used as the Management Ethernet connector to provide connectivity to an Ethernet local area network. The front panel can be used to configure an IPv4 address (static or DHCP) or enable DHCP for IPv6. Once the IP address is set and a connection is made to a Local Area Network (LAN), you can access the SyncServer S6x0 web interface.

1.4.2.2 Local Console Serial Port

The serial port supports very limited local control; you can configure the SyncServer S6x0 with CLI commands using a terminal or computer with terminal emulation software. The connector is located on the rear panel. The local port is configured as a DCE interface and the default settings are as follows:

- Baud = 115.2K
- Data Bits = 8 bits
- Parity = None
- Stop bits = 1
- Flow Control = None

1.4.3 Time Inputs

The SyncServer S6x0 can use GNSS, NTP, PTP, and IRIG as external input references (depending on model and configuration). The NTP signals use the RJ45 (1 - 4) connectors on the rear panel. The GNSS reference uses a BNC connector on the rear panel. PTP can optionally use RJ-45 (2-4). The IRIG signal uses a BNC connector (J1) on the optional Timing I/O module on the rear panel, as described in .

1.4.4 Frequency Inputs

The SyncServer S6x0 can use either 1PPS, 10 MPPS, 10 MHz, 5 MHz, or 1 MHz as external frequency input references. The 1PPS/10 MPPS use the J1 BNC and the 10 / 5 / 1 MHz signals use a BNC connector (J2) on the Timing I/O module on the rear panel, as described in .

1.4.5 Frequency and Timing Outputs

The SyncServer S6x0 can provide NTP,10 / 5 / 1 MHz, 1PPS, IRIG, or TOD output signals. The NTP signals use the RJ45 (1 - 4) connectors on the rear panel. PTP uses RJ45 (2-3) connectors on the rear panel. The serial TOD output connects to a DB9 connector (DATA/SERIAL) on the rear panel. The IRIG, PPS, 10 MPPS, and 10 / 5 / 1 MHz signals use BNC connectors (J3 - J8) on the Timing I/O module on the rear panel. A 1PPS output is also available using a BNC connector (1PPS) on the rear panel.

Table 1-4. Timing Input/Output Module

Config	Input BNCs		Output BNCs					
	J1	J2	J3	J4	J5	J6	J7	J8
Standard	IRIG B AM 124 or 1PPS	10 MHz	IRIG B AM 124	10 MHz	IRIG B B004 DCLS	1PPS	off	off

...........continued			
Config	**Input BNCs**		**Output BNCs**
FlexPort Option	A000/A004/ A130/ A134B000/ B001/B002/ B003B004/ B005/B006/ B007B120/ B121/B122/ B123B124/ B125/B126/ B127E115/ E125C37.11 8.1a-2014IE EE-1344 Rates:1 PPS10 MPPS	1 MHz 5 MHz 10 MHz	Pulse:Fixed rate: 10/5/1MPPS, 100/10/1kPPS, 100/10/1/0.5PPS, 1PPM, 1PPS falling edge Programmable period: 100 ns to 86400 s, step size of 10 ns Timecode: IRIG A 004/134 IRIG B 000/001/002/003/004/005/006/007/ C37.118.1a-2014/1344 DCLS IRIG B 120/122/123/124/125/126/127/1344 AM IRIG E 115/125 IRIG G 005/145 NASA 36 AM/DCLS, 2137 AM/DCLS, XR3 Sine: 1/5/10 MHz BNC-by-BNC output phase adjustment for timecodes and pulses

Notes:
The SyncServer S6x0 uses IRIG 1344 version C37.118.1a-2014.

- On the input side, the code performs a subtraction using control bits 14 - 19 from the supplied IRIG time with the expectation that this will produce UTC time. This aligns with the C37.118.1a-2014 definition.
- On the output side, control bits 14 - 19 will always be zero, and the encoded IRIG time will be UTC (if using an input 1344 IRIG as the reference the 2014 rules are applied to get that value). Hence, any code receiving S6x0 IRIG 1344 output should work regardless of which version they are decoding (since there is nothing to add or subtract).

1.5 Configuration Management

The SyncServer S6x0 can be configured using the keypad interface, web interface or Command Line Interface.

1.5.1 Keypad/Display Interface

The keypad/display interface displays the time, system status, and provides the following functions:

- Configuring and enabling/disabling the LAN1 network port
- Setting the time and entering freerun mode
- Adjusting the brightness
- Locking the keypad
- Shutting down the SyncServer

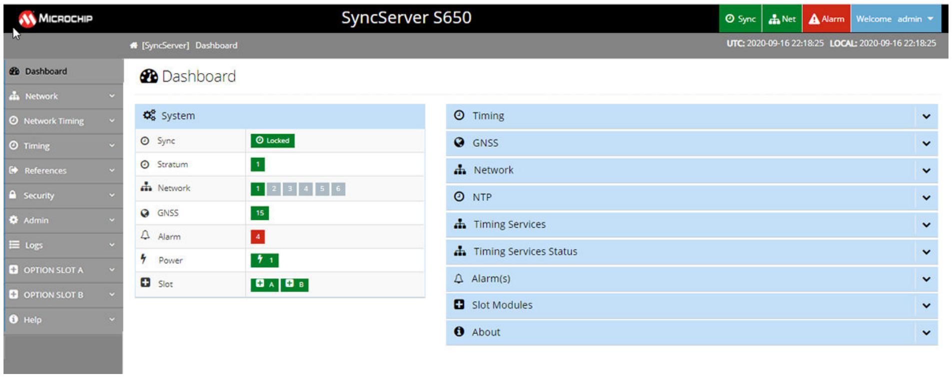
1.5.2 Web Interface

The SyncServer S6x0 also allows the user to access information via the LAN1 Ethernet port using HTTPS protocol. To use the SyncServer S6x0 web interface, enter the IP address for Ethernet port 1 into a web browser. Enter your user name and password for the SyncServer S6x0 when prompted.

1.5.2.1 Dashboard View

See for an example of the dashboard status screen that will appear.

Figure 1-38. Web Interface - Dashboard



1.5.3 Command Line Interface (CLI)

The Command Line Interface can be used to control specific function of the SyncServer S6x0 from a terminal connected to the EIA-232 serial port or the Ethernet LAN1 port. Refer to Chapter 4, Command Line Interface (CLI) for further details.

Note:
Before you can communicate with the SyncServer S6x0 through an Ethernet connection, you must first configure the Ethernet port using the serial connection or front panel (Provisioning the Ethernet Ports).

1.6 Alarms

The SyncServer S6x0 uses alarms to notify you when certain conditions are deteriorating below specified levels or when issues arise, such as loss of power , loss of connectivity, or excess traffic on a port. These alarms are indicated by LEDs, WebGUI status, CLI status, alarm connector (configurable), SNMP Trap (configurable), message log (configurable), and email (configurable). For more information, see Provisioning Alarms and Chapter 8: System Messages.

2. Installing

This chapter describes the procedures for installing the SyncServer S6x0.

2.1 Getting Started

Before you begin to install the SyncServer S6x0, review the information in this section.

If you encounter any difficulties during the installation process, contact Microchip Frequency and Time Systems (FTS) Services and Support. See Contacting Technical Support for telephone numbers. Contact Microchip FTS Services and Support for technical information. Contact Customer Service for information about your order, RMAs, and other information.

2.1.1 Security Considerations for SyncServer S6x0 Installation

- The SyncServer S6x0 should be installed in a physically secure and restricted location.
- Whenever possible, the SyncServer S6x0's Ethernet ports should be installed behind the company's firewall to prevent public access.

2.1.2 Site Survey

The SyncServer S6x0 can be installed in a wide variety of locations.

Before you begin installation, determine the chassis location, ensure the appropriate power source is available (120/240 VAC), and ensure that the equipment rack is properly grounded.

The SyncServer S6x0 is designed to mount in a 19-inch (48 cm) rack, occupies 1.75 in (4.5 cm, 1 RU) of vertical rack space, and has a depth of 15” (38.1 cm).

The SyncServer S6x0 is to be installed into a rack. The AC power connection is to be made to a 120 or 240 VAC power receptacle following local codes and requirements. An external Surge Protective Device is required to be used with the AC version of the SyncServer S6x0.

2.1.2.1 Environmental Requirements

To prevent the unit from malfunctioning or interfering with other equipment, install and operate the unit according to the following guidelines:

- Operating temperature: –40° F to 149° F (–20° C to 65° C) for SyncServer S6x0 with quartz oscillator (standard or OCXO); 23° F to 131° F (–5° C to 55° C) for SyncServer S6x0 with Rubidium oscillator.
- Operating Humidity: 5% to 95% RH, maximum, w/condensation
- Secure all cable screws to their corresponding connectors.

Note:
To avoid interference, you must consider the electromagnetic compatibility (EMC) of nearby equipment when you install the SyncServer S6x0. Electromagnetic interference can adversely affect the operation of nearby equipment.

2.1.3 Installation Tools and Equipment

You will need the following tools and equipment to install the SyncServer S6x0:

- Standard tool kit
- Cable ties, waxed string, or acceptable cable clamps
- 1 mm^2 / 16 AWG wire to connect grounding lug to permanent earth ground
- One UL listed Ring Lugs for grounding connections
- Crimping tool to crimp the ring lug
- Shielded cabling of the appropriate impedance required by the specific signal type for signal wiring (including GNSS)
- Mating connectors for terminating signal wiring
- ESD wrist strap for installing modules

- Fasteners for mounting the equipment in rack
- Digital multimeter or standard Voltmeter for verifying ground connections to the chassis

2.2 Unpacking the Unit

The SyncServer S6x0 is packaged to protect them from normal shock, vibration and handling damage. (Each unit is packaged separately.)

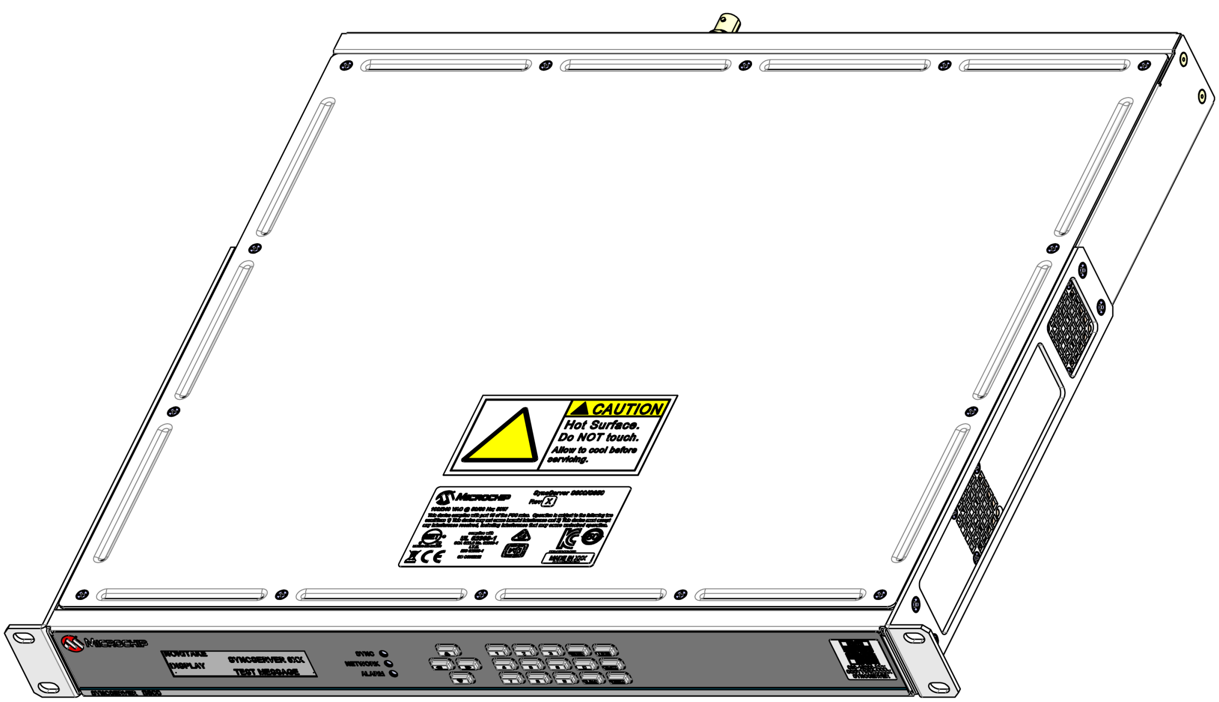
Note:
To avoid ESD damage to parts that are packaged with the SyncServer S6x0, observe the following procedures.

Unpack and inspect the unit as follows:

1. Wear a properly grounded protective wrist strap or other ESD device.
2. Inspect the container for signs of damage. If the container appears to be damaged, notify both the carrier and your Microchip distributor. Retain the shipping container and packing material for the carrier to inspect.
3. Open the container, being careful to cut only the packaging tape.
4. Locate and set aside the printed information and paperwork that is included in the container.
5. Remove the unit from the container and place it on an anti-static surface.
6. Locate and set aside small parts which may be packed in the container.
7. Remove the accessories from the container.
8. Remove the anti-static packaging from the unit and accessories.
9. Verify that the model and item number shown on the shipping list agrees with the model and item number on the equipment. The item number can be found on a label affixed to the top of the unit. See the following image for the location of the label on the SyncServer S6x0. Contact your Microchip distributor if the model or item number do not match.

For a complete listing of item numbers, see Table 7-4, Table 7-5 and Table 7-6.

Figure 2-1. SyncServer S6x0 - Location of Product Label on Top of Unit



2.3 Rack Mounting the SyncServer S6x0

The installation procedure described in this section provides general guidelines for installing the SyncServer S6x0. Always follow applicable local electrical standards.

SyncServer S6x0 is shipped with 19-inch rack mounting brackets attached.

Mount the chassis to the front of the equipment rack rails with four screws and associated hardware, as shown in . Use the proper screws for the equipment rack.

Figure 2-2. Dimensions for SyncServer S6x0

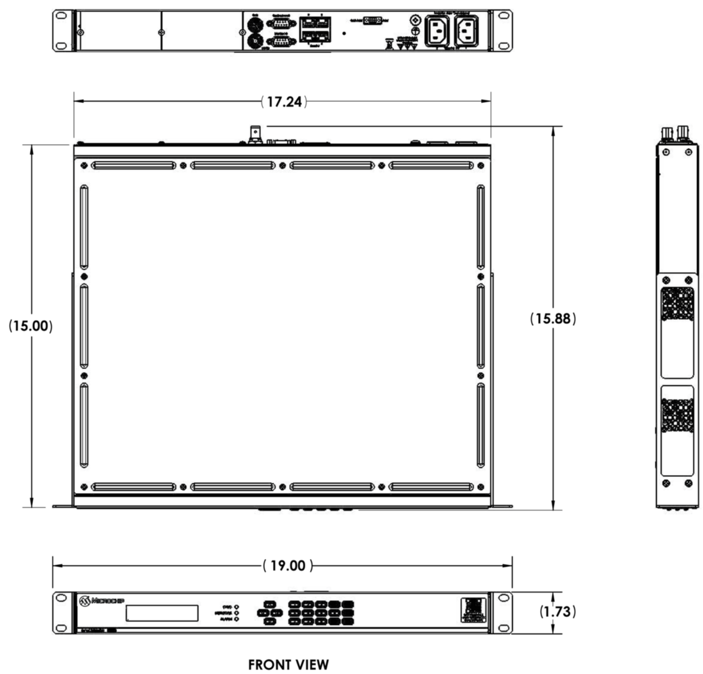
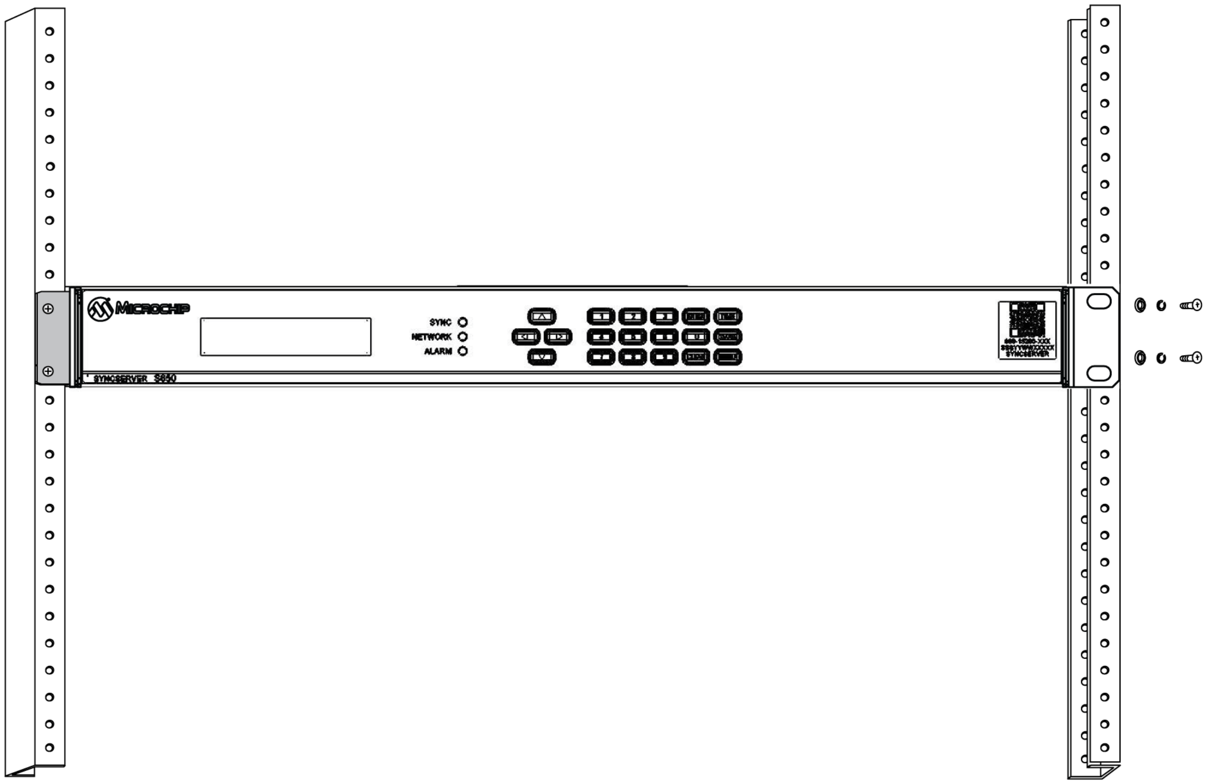


Figure 2-3. Rack Mounting the SyncServer S6x0



2.4 Making Ground and Power Connections

The SyncServer S6x0 has either one or two 120/240 VAC connectors, depending on the specific model, which are located on the left side of the rear panel. (see and).

2.4.1 Ground Connections

The frame ground connection is made using the grounding screw, which is marked with the universal ground symbol, as shown in . This screw is located on the left side of the rear panel for all models of the SyncServer S6x0, as shown in and .

Figure 2-4. SyncServer S600/S650 Power & Ground Connections - Single AC Version

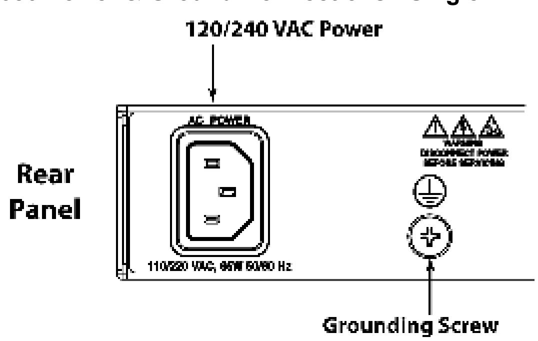


Figure 2-5. SyncServer S600/S650 Power & Ground Connections - Dual AC Version

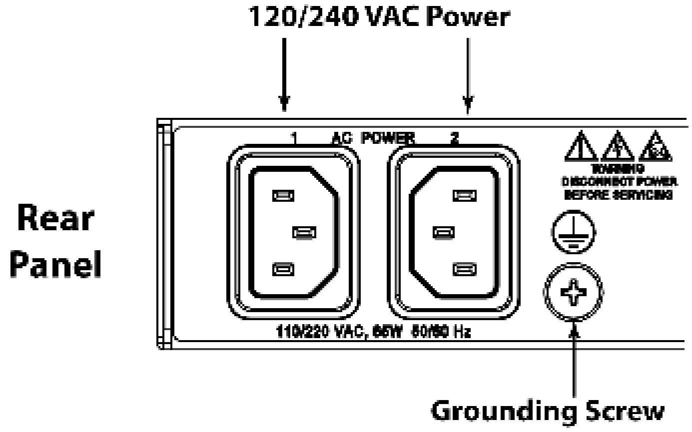


Figure 2-6. Universal Ground Symbol

After installing the SyncServer S6x0 into the rack, connect the chassis to the proper grounding zone or master ground bar per local building codes for grounding.

Run a 16 AWG green/yellow-striped insulated wire from the SyncServer S6x0 grounding lug to the earth Ground on the rack. The rack grounding method is below.

Note:
Although there are a number of methods for connecting the equipment to earth ground, Microchip recommends running a cable of the shortest possible length from the ground lug to earth ground.

1. Remove the grounding screw from the rear panel of the SyncServer S6x0.
2. Crimp the customer-supplied UL listed Ring Lug to one end of the 16 AWG wire. Coat the lug with an electrically conductive antioxidant compound such as Kopr-shield spray. Use the grounding screw to connect the ring lug to the left side of the rear panel. The surface of the SyncServer S6x0 rear panel and threads where the grounding screw attaches must be clean of contaminants and oxidation.
3. Connect the other end of the 1 mm² / 16 AWG green/yellow-striped wire to earth ground using local building electrical codes for grounding. The suggested method is to crimp the appropriate customer-supplied UL listed Ring Lug to the other end of the 1 mm² / 16 AWG green/yellow-striped wire. Remove the paint and sand the area around the screw hole to ensure the proper conductivity. Coat the connection with an electrically conductive antioxidant compound such as Kopr-shield spray. Connect this Ring Lug to the rack with appropriate customer supplied screws and external star lock washers, tightening to a torque value of 53.45 in-lbs.
4. Using a digital voltmeter, measure between the ground and chassis and verify that no voltage exists between them.

2.4.2 AC Power Connection

Use the following procedure to make the power connections for the AC version of the SyncServer S6x0. An Over-Current Protection Device must be placed in front of the shelf power.

Figure 2-7. SyncServer S6x0 Single AC Power Connector

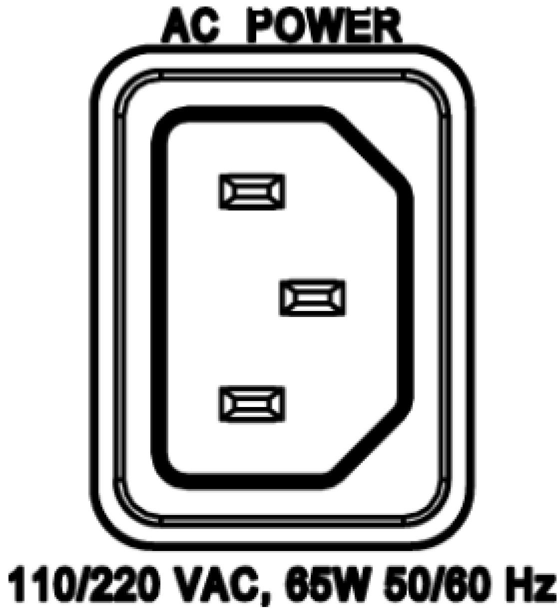
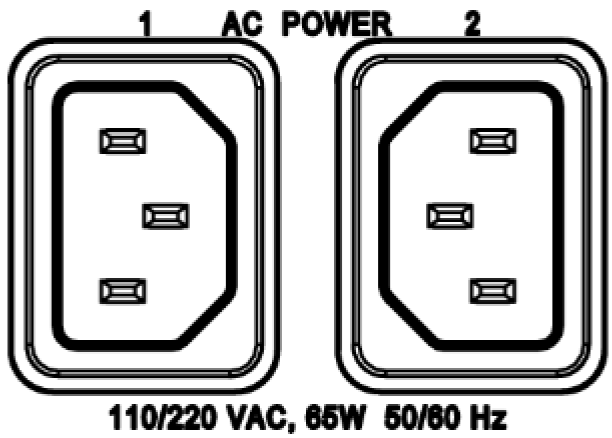


Figure 2-8. SyncServer S6x0 Dual AC Power Connector



Note:
To avoid possible damage to equipment, you must provide power source protective fusing as part of the installation. The SyncServer S6x0 is intended for installation in a restricted-access location.

1. Insert the female end of the AC power cord into the AC power connector on the SyncServer S6x0. The power receptacles support IEC cable with V-locks. The V-lock will latch the cable to prevent accidental removal of the power cord.
2. Plug the male end of the AC power cord into an active 120 VAC or 240 VAC power socket.
3. For dual AC versions, repeat steps 1-2 for the second AC power connector.

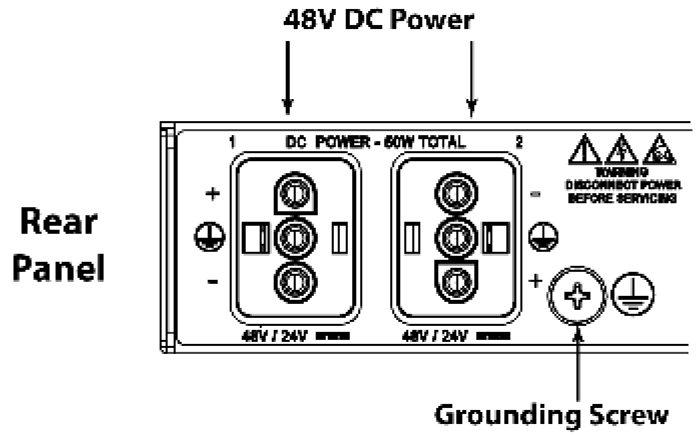
2.4.3 DC Power Connection

Use the following procedure to make the power connections for the DC version of the SyncServer S6x0. An Over-Current Protection Device must be placed in front of the shelf power. The SyncServer S6x0 uses a Molex HCS-125 series connector.

Note:
To avoid possible damage to equipment, you must provide power source protective fusing as part of the installation. The SyncServer S6x0 is intended for installation in a restricted-access location.

1. Create a custom cable using the supplied Molex connector housing and terminals. The terminals need to be crimped to the wires.
2. Connect the other end of the DC cable to nominal 24VDC or 48 VDC.
3. Repeat steps 1-2 for the second DC power connector.
4. The positive wire must be connected to the positive terminal (+) and the negative wire to the negative terminal (-). The ground connection should only be connected to ground and not to a power supply.

Figure 2-9. SyncServer S6x0 Dual DC Power Connectors



2.5 Signal Connections

The connectors for the SyncServer S6x0 are located on the rear panel.

2.5.1 Communications Connections

The communication connections allow user control of the SyncServer S6x0. The EIA-232 serial port and Ethernet port 1 (LAN1) are located on the rear panel are shown in .

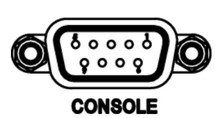
2.5.1.1 Ethernet Port 1

Ethernet port 1 is a standard 100/1000 Base-T shielded RJ-45 receptacle on the rear panel of the unit. It is used to provide connectivity to a web interface and to an Ethernet local area network (as well as for NTP input/output). To connect the SyncServer S6x0 to an Ethernet network, use an Ethernet RJ-45 cable. See for connector pinouts.

2.5.1.2 Serial (Console) Port

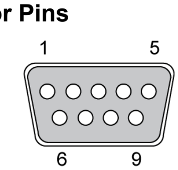
The serial port connection is made through a DB-9 female connector on the rear panel of the unit. This port, which supports a baud rate of 115.2k (115200-8-1-N-1), allows you to connect to a terminal or computer using a terminal emulation software package for remote monitoring and control. This port is also used for serial data (NENA ASCII time code, Response mode). When connecting to this port, use a shielded serial direct connect cable.

Figure 2-10. Serial Port Connector



shows the DB-9 male connector that mates with the serial port on the SyncServer S6x0.

Figure 2-11. Serial Port Male Mating Connector Pins



describes the DB-9 connector pin assignments for the serial port.

Table 2-1. Serial Port Connector Pin Assignments

Signal	Pin
TXD	2
RXD	3
Ground	5

2.5.2 SyncServer S6x0 Synchronization and Timing Connections

The SyncServer S6x0 has one GNSS input and four NTP input/output connections. The SyncServer S6x0 has one 1PPS output. The SyncServer S650 may also have optional Timing I/O Module(s).

2.5.2.1 GNSS Connection

To connect a GNSS signal to the SyncServer S6x0, you must install a GPS antenna. See Connecting the GNSS Antenna .

Note:
The GNSS cable should only be connected while the unit is properly earth grounded.

Note:
To avoid possible damage to equipment, you must provide external lightning protection when installing the GNSS antenna to prevent transients.

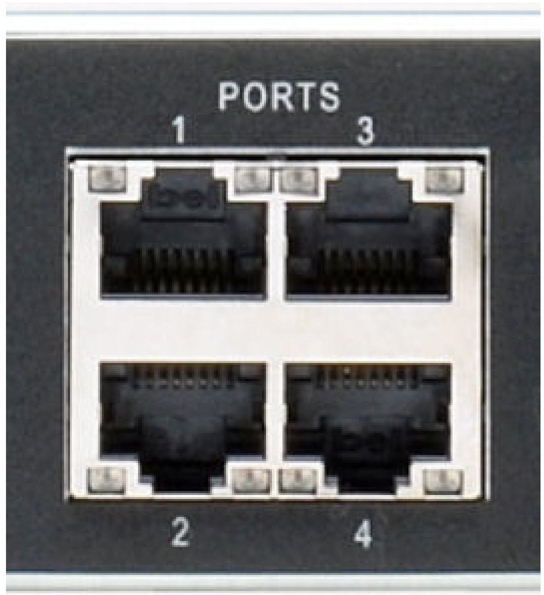
2.5.2.2 Ethernet Connections

The Ethernet ports are standard 100/1000 Base-T shielded RJ-45 receptacles, which are used for NTP inputs. To connect the SyncServer S6x0 to an Ethernet network, use an Ethernet RJ-45 cable. See for connector pinouts.

Table 2-2. System Management Ethernet Connector Pin Assignments

RJ-45 Pin	100Base-T Signal
1	TX+ (Transmit positive)
2	TX- (Transmit negative)
3	RX+ (Receive positive)
4	Not Used
5	Not Used
6	RX- (Receive negative)
7	Not Used
8	Not Used

Figure 2-12. Ethernet Connections



2.5.3 10 GbE Connections

The two SFP+ ports are only available with the 10 GbE option. These SFP+ ports are equipped with hardware timestamping that supports NTP, PTP, and NTP Reflector operations. These ports are ideal for interoperability with 10 GbE switches. SFP modules supported are limited to 10 GbE speeds only, See for a list or recommended and supported SFP+ transceivers.

Figure 2-13. 10 GbE Connections

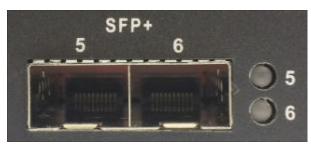


Table 2-3. Recommended and Supported SFP+ (10GbE) Transceivers

Vendor	Mode	Item Code or P/N
ALU	multi-mode	10GBASE-SR, PN: 3HE04824AA
ALU	single mode	10GBASE-LR, PN: 3HE04823AA
Finisar	multi-mode	PN: FTLX8573D3BTL
Finisar	multi-mode	PN: FTLX8574D3BCL
Finisar	single mode	PN: FTLX1471D3BCL
D-Link	multi-mode	10GBASE-SR, PN: DEM-431XT-DD
Cisco	multi-mode	SFP-10G-SR
Cisco	single mode	SFP-10G-LR
Juniper	multi-mode	SFPP-10G-SR
Juniper	single mode	SFPP-10G-LR

...........continued		
Vendor	**Mode**	**Item Code or P/N**
Juniper	multi-mode	EX-SFP-10G-SR
Juniper	single mode	EX-SFP-10G-LR

2.5.4 Timing I/O Module Connections

The standard configuration offers a broad yet fixed selection of signal I/O on its eight BNC connectors (see). J1 is dedicated to time code and rate inputs, J2 to sine wave inputs, and J3-J8 to mixed signal outputs. The standard Timing I/O Module configuration is 1PPS or IRIG B AM-In, 10 MHz- In, IRIG AM and IRIG DCLS-Out, 1PPS-Out and 10 MHz-Out.

The FlexPort™ Technology option enables the 6 output BNCs (J3-J8) to output any supported signal (time codes, sine waves, programmable rates, and so on.) on all configurable in real time via the secure web interface. Similarly, the 2 input BNCs (J1-J2) can support a wide variety of input signal types. This uniquely flexible BNC by BNC configuration makes very efficient and cost effective use of the 1U space available.

See to view the signal types for the standard configuration and the configuration with the FlexPort™ option. See Figure 2-14.

See for the signal types supported with the Telecom I/O module option. See .

See for the signal types supported with the HaveQuick/PTTI module option. See .

See for the fiber optic transmitter module options.

Figure 2-14. Timing I/O BNC Connections (090-15201-006)

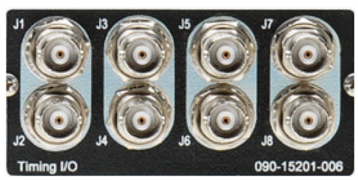
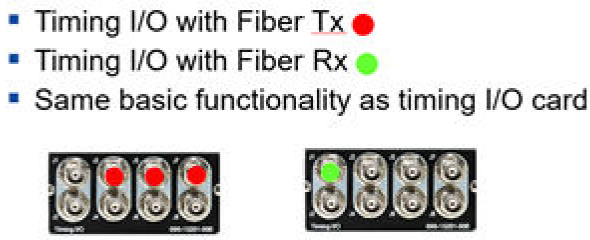


Figure 2-15. Timing I/O with Telecom I/O Connections (090-15201-011)

Figure 2-16. Timing I/O with HaveQuick/PTTI Connections (090-15201-012)

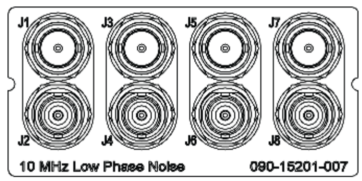
Figure 2-17. Timing I/O with Fiber Optic Transmitter Connections (090-15201-013 and -014)



2.5.5 LPN Module Connections

This module provides low phase noise 10 MHz signals on all eight ports (J1-J8). See

Figure 2-18. LPN BNC Connections



2.5.6 Serial Timing Connection

The SyncServer S6x0 features a DB-9 female connector on the rear panel of the unit. This port supports a baud rate of 4800 to 115.2k (115200-8-1-N-1). When connecting to this port, use a shielded serial direct connect cable. See the following image. See the following table for pin-outs for this DB-9 connector.

Figure 2-19. Data/Timing Connection

Table 2-4. Serial Data/Timing Port Pin-Outs - DB-9 Connector

Signal	Pin
TXD	2
RXD	3
Ground	5

See Table 9-26 in Chapter 9 for TOD format details.

2.5.6.1 1PPS Output Connection

The SyncServer S6x0 features a single BNC female connector for the 1PPS signal. See.

Figure 2-20. 1PPS Output Connection

2.6 Connecting the GNSS Antenna

Note:
The GNSS cables should only be connected while the unit is properly earth grounded.

The antenna connections for the SyncServer S6x0 are made at the BNC female connector labeled GNSS. Allow at least one hour for the unit to track and lock to GNSS satellites, though it typically takes far less time provided the antenna has an adequate view of the sky.

Note:
The SyncServer S650i does not include a GNSS antenna connector.

Figure 2-21. GNSS Input Connection

Proper cable, grounding techniques, and lightning arrestors should be used. Mount the antenna outside, preferably on the roof with an unobstructed view of the sky. Avoid mounting the antenna near a wall or other obstruction blocking part of the sky. Mount the antenna well above roads or parking lots.

Note:
For the best possible timing accuracy the cable delay must be determined and entered into SyncServer S6x0 with the web interface. See Table 10-1 for cable delay values of SyncServer S6x0 GNSS antenna kits.

Notes:
To avoid serious personal injury or death, exercise caution when working near high voltage lines. In particular:

- Use extreme caution when installing the antenna near, under, or around high voltage lines.
- Follow local building electrical codes for grounding the chassis.

2.7 Connecting Alarm Relay

The alarm relay output is open when an alarm activation on this page is configured and the alarm is in alarm state:

ALARM=OPEN

The external Alarm mating connector is not supplied. The mating connector is made by Phoenix Contact, and the manufacturer's part number is 1827703.

Figure 2-22. Alarm Connections

2.8 Installation Check List

To verify that the installation of the SyncServer S6x0 is complete, perform the checks and procedures in

Table 2-5. Installation Completeness Checklist

Operation	Complete
Ensure the SyncServer S6x0 chassis is securely attached to mounting rack	
Verify that all power and ground wires are installed correctly and securely	

...........continued	
Operation	**Complete**
Verify that all communications cables are properly installed	
Verify that all input and output cables are properly installed	

2.9 Applying Power to the SyncServer S6x0

The SyncServer S6x0 is not equipped with a Power switch. After installing the unit in a rack and making the necessary connections described in previous sections, turn on power at the distribution panel.

2.9.1 Normal Power Up Indications

As the SyncServer S6x0 powers up and begins normal operation, the LEDs all turn on. After the self-test is complete and the firmware is operational, the LED states may change to indicate the appropriate state or status. provides a description of the SyncServer S6x0 LEDs.

Table 2-6. LED Descriptions

Label	LED	Description
SYNC	Clock status	- Time or Frequency clock in Normal or Bridging state - Time or Frequency clock in Freerun or Holdover state
NETWORK	Network status	- Management port (LAN1) is not configured or is down - Some configured ports are down (LAN2 to LAN4) - All configured ports are up
ALARM	Alarm System alarm/ fault indicator	-Operating normally - Minor Alarm(s) - Major/Critical Alarm(s)

The SyncServer 6x0 does not contain a battery-backed real time clock. Therefore, it will always boot up with a default value for the system time. This time will be updated when it obtains time from a time reference such as GNSS, IRIG, PTP, or NTP. The default value for the date is the software build date. This date will be used for the first log entries when booting up the unit. The time will change to local time during the boot-up process if a time zone has been configured.

3. Keypad/Display Interface

3.1 Overview

The keypad / display interface displays the time, system status, and provides the following functions:

- Configuring and enabling/disabling the LAN1 network port.
- Setting the time and entering freerun mode.
- Adjusting the brightness.
- Locking the keypad.
- Shutting down the SyncServer.
  When the SyncServer starts, the display shows “Booting SyncServer please wait...”. Shortly thereafter, the SyncServer displays the default time screen.

  The following buttons are user-input devices for the keypad/display interface.
- ENTER: Use with MENU - Applies a menu selection or function setting.
- CLR: Use with MENU - Returns to the previous screen without saving changes.
- Left/Right Arrow Buttons: In functions, will change where the next number will be entered left or right. In status, scrolls a screen horizontally when “<previous:next>” is displayed.
- Up/Down Arrow Buttons: In functions, will change where the next number will be entered. In status, scrolls a screen vertically, displays the previous/next screen.
- Number Buttons: Enters a number, or selects a numbered menu item.
  The following three buttons change the function of the display.
- TIME: Changes the format and contents of the time display.
- STATUS: Displays status of basic SyncServer operational conditions.
- MENU: Displays a menu of functions.
  The following sections cover these three buttons in more detail.

3.2 TIME Button

Cycling the TIME button changes the predefined format and contents of the time display:

Large numeric time display on full screen. Hours:Minutes:Seconds

Medium numeric time display on the left, current reference and NTP Stratum on the right

Small date and time, reference, and NTP stratum.

The time display also indicates a time scale:

If the time zone setting on the TIMING - Time Zone web page is set to UTC, the time display shows “UTC” as the time scale.

If the time zone setting on TIMING - Time Zone page is set to a non-UTC (local) time zone, the time display leaves the time scale blank, or adds AM/PM if the user selects the 12-hour time scale. (Press the MENU button and select 2) Display > 3) 12/24 > 1) 12 (AM/PM).

If the Ignore UTC Corrections from GPS Reference setting on the TIMING - HW Clock page is enabled (selected), the time display shows “GPS” as the time scale.

Note: The TIMING - Time Zone page configures the display for UTC or local time. The TIMING -

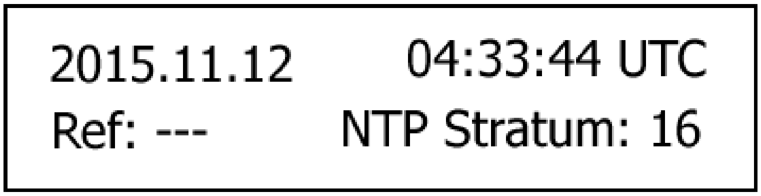
3.3 STATUS Button

Pressing the STATUS button repeatedly displays a series of status screens for:

- NTP

- Alarms
- Network Ports
- Clock
- GNSS Receiver
- SyncServer model, serial number, software version, and software upgrade availability. If installed, the configuration for each port of the timing/IO module.

Figure 3-1. NTP Status Screen



Some screens have a “Next>” in the upper right. This means more information is available by pressing the right arrow button. This cycles through screens on that topic.

3.3.1 NTP Status Screen

Network Time Protocol (NTP) status.

Stratum: The Stratum number of the SyncServer. Stratum 1 means it is locked to a Hardware Clock.

Hardware Clock Input Reference that is a Stratum 0 source. Stratum 2-15 means the SyncServer is locked to another NTP time source. Stratum 16 means that the SyncServer is unsynchronized.

Reference: This field identifies the “system peer”. While stratum is 16, this field shows the progression of the NTP clock PLL. The field starts with a value of “INIT”. Once a peer has been selected, the clock may be stepped, in which case the reference ID field changes to “STEP”.

Once the PLL is locked, the stratum is updated and the reference ID provides information about the selected peer. When the SyncServer is operating at stratum 1, the reference ID displays the name of the Hardware Clock reference input.

NTP Packet I/O: The number of NTP packets the SyncServer has replied to and initiated. The SyncServer replies to clients that send NTP requests. The SyncServer also sends NTP requests when the NTP daemon isn't synchronized (i.e., Sync LED is RED) and when it is configured to synchronize to an NTP association (e.g., a Server type association).

3.3.2 Alarm Status Screen

Current alarm status. Use the right or left arrow to show details about the alarms.

Major: List of up to three current major alarms

Minor: List of up to three current minor alarms

3.3.3 LAN Status Screens

Multiple screens, four for each network port. There are two screen for IPv4 and two for IPv6. Use Next> to see the entire IP address configuration.

State: Shows “Up” if the port is enabled and “Down” if the port is disabled.

IP: IP address for the port

SM: Subnet mask

GW: Gateway address

3.3.4 Clock Status Screen

Hardware Clock and Input Reference status.

3.3.5 GNSS Receiver Status Screen

GNSS receiver status.

Antenna: OK

GNSS: Operational

GNSS SATELLITES

- GPS: number of GPS satellites currently being tracked.
- GLONASS: number of GLONASS satellites currently being tracked
- SBAS: number of SBAS satellites currently being tracked
- Max CNo: The highest CNo (Carrier-to-Noise ratio) of all satellites (value given for each satellite type)

GNSS SOLUTION

Status: OK Service 3D

Mode: Auto or Manual

3.3.6 SyncServer Status Screen

Hardware and software identification. Software upgrade availability.

Model: The model number.

S.N.: The serial number.

Version: The software “Release Version” number.

3.3.7 Option Slot A/B Status Screens

Shows the configuration of each of the slot A/B input and output connections.

Option: Description of installed module (if any)

Flex I/O Option: Enabled | Disabled

J1 Input: Configuration of input

J2: Input: Configuration of input

J3 Output: Configuration of output

J4 Output: Configuration of output

J5 Output: Configuration of output

J6 Output: Configuration of output

J7 Output: Configuration of output

J8 Output:Configuration of output

3.4 MENU Button

Pressing the MENU button presents a numbered menu of functions, as shown in the following image.

Figure 3-2. Menu of Functions

3.4.1 LAN1

Selecting LAN1 brings up the Display menu screen on the display, as shown in the following image.

Figure 3-3. Configure LAN1 Screen

```
Configure LAN1
1) Configure        2) On / Off
```

1. **Configure**: Use to select IPv4 or IPv6 address mode for LAN1 port. IPv6 automatically configures LAN1 with a dynamic IPv6 address.
   If Configure is selected, the Select LAN1 screen will appear, as shown in Figure 3-4.
2. **On/Off**: Use On to enable the LAN1 network port. Off disables the LAN1 network port for all traffic types.

   Figure 3-4. Select LAN1 IP Mode Screen

   ```
   Select  LAN1
   1) IPv4       2) IPv6 (DHCPv6)
   ```

3. **IPv4**: Select IPv4address mode for LAN1 port.
   If IPv4 is selected, the Select Addressing Type screen will appear, as shown in Figure 3-5.
4. **IPv6**: Select IPv6 address mode for LAN1 port.
   If IPv6 (DHCPv6) is selected, the SyncServer automatically configures LAN1 with a dynamic IPv6 address.

   Figure 3-5. Select IPv4 Addressing Type Screen

   ```
   Select  Addressing Type:
   1) Static Addr         2) DHCP
   ```

5. **Static Addr**: Select IPv4address mode for LAN1 port.
   If Static Address is selected, the Enter LAN1 Address screen will appear, as shown in Figure 3-6. After the address is entered press the ENTER button and you will be prompted to enter the Subnet mask (then ENTER) followed by the Gateway address. Once the gateway address has been entered the LAN 1 port will be reconfigured.
6. **DHCP**: Select DHCP addressing type for LAN1 port. DHCP automatically configures LAN1 with a dynamic IPv4 address.

   Figure 3-6. Enter LAN1 Static IPv4 Address Screen

   ```
   Enter  LAN1  Address:
               192.168.107.122
   ```

Note: LAN1 can be configured even if the port is down or unconnected. However, the LAN1 status display will not reflect the new configuration until the LAN1 link is up.

3.4.2 Display

Selecting Display brings up the Display menu screen on the display, as shown in the following image.

Figure 3-7. Display Menu Screen

1) Set Time   2) Brightness
3) 12/24 (non-UTC only)

1. **Set Time**: Enter the UTC date and time using 24-hour format. Select ENTER to apply the entered time to the system clock. The system must have previously been set to the "Forced Manual Time Entry " mode on the Timing->Input Control web page. See the following image..

   Figure 3-8. Set Time Screen

   Enter 24h time:
   2015-11-12, 11:32.30

2. **Brightness**: Adjust the brightness of the front panel display. See the following image.

   Figure 3-9. Set Brightness Screen

   Select Brightness Level:
   1) Low   2) Medium   3) High

3. **12/24 (non-UTC Only)**: Select a 12 (AM/PM) or 24-hour clock format. See the following image.
   Note: The 12/24 and 24 Hour only appear if a local time zone has been specified via the web inteface.

   Figure 3-10. Select Time Format Screen

   Select Format:
   1) 12 (AM/PM)   2) 24 Hour

   Many keypad functions timeout after approximately 10 seconds of inactivity (no user inputs).

3.4.3 Sys Control

Selecting Sys Control brings up the Shutdown / Factory Default screen on the display, as shown in the following image.

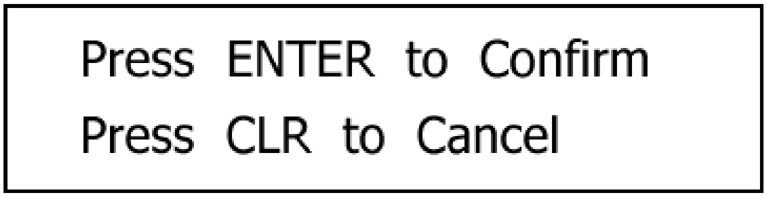
Figure 3-11. Shutdown / Factory Default Screen

1) Shutdown
2) Factory Default

See Factory Defaults in Chaper 9 for default settings.

1. **Shutdown**: Halts the SyncServer. The message Press the ENTER button to Confirm appears in the display, as shown in the following image.
2. Factory Default

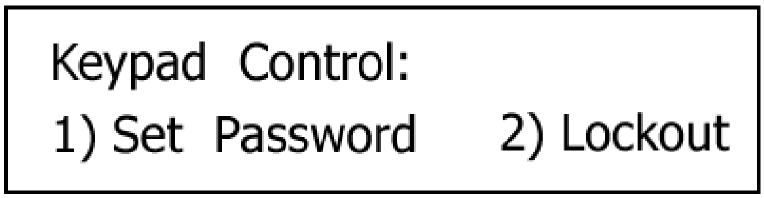
Figure 3-12. Confirmation Screen



3.4.4 Keypad

Selecting Keypad brings up the Keypad Control screen on the display, as shown in the following image.

Figure 3-13. Keypad Control Display Screen



1. **Set Password**: Sets the password for the Lockout function. The *first time* the interface asks for the “Current Password”, enter 95134. No password recover or reset feature is available for the keypad, except to reset factory defaults using the Sys Control - Factory Reset page.
2. **Lockout**: The Lockout function password protects the keypad from changes. Asks for confirmation. The factory default password for the keypad is “95134”.

4. CLI Commands

This chapter describes the CLI command conventions, the prompts, line editing functions, and command syntax. The CLI command functions and features are listed alphabetically.

4.1 SyncServer S6x0 CLI Command Set

This section provides an alphabetical listing and details of all CLI commands. Both the serial CONSOLE CLI commands and SSH CLI commands should be identical.

4.1.1 set clock

This command provides an ability to set the time.

Command Syntax:

```
set clock date-time <date-time>
```

where <date-time> = YYYY-MM-DD,HH:MM:SS

The time is presumed to be UTC.

4.1.2 set configuration

Use this command to replaces the current configuration with the factory default configuration. On SyncServer, user is prompted with “Y” to confirm that they really want to do it.

Command Syntax:

```
set configuration factory
```

Returning the configuration to factory defaults also includes:

- Loss of configured user logins
- Loss of configured network settings (addresses, firewall, etc.)

Installed licenses remain installed.

The SyncServer S6x0 reboots as part of this process.

The behavior with this command is identical to using the WebGUI to reset to factory default (Dashboard > Admin> Configuration Backup/Restore/Reset).

4.1.3 F9 - Time on Request

The F9 command is used to record the time the SyncServer S6x0 receives a request from the user. The general behavior is covered in the following table. This function is configurable through the command line interface only. It is not configurable from the keypad.

Table 4-1. F9 Syntax Basic Behavior

Syntax	Behavior
`F9<CR>`	Enables the connection for “time on request” operation. When enabled, the only inputs the connection will respond to are ctrl-C and SHIFT-T (see next 2 rows).
`ctrl - C`	Disables the connection for “time on request” operation
`SHIFT-T`	If “time on request” enabled, this triggers a time response on the connection. **Note**: The “T” does not appear (it is not echoed back by SyncServer S6x0).

Enter the command F9<CR> to prepare the SyncServer S6x0 for the user's request. At the desired moment, send the request to the SyncServer S6x0 by entering an upper case “T”. The SyncServer S6x0 saves the current time-of-day, accurate to within 1 microsecond, to a buffer, and then outputs it to the command line interface. The SyncServer S6x0 continues to provide the time-of-day each time it receives a “T” until F9 is cancelled. To cancel F9, enter ctrl-C on your keyboard. The command line disregards all input other than SHIFT-T and ctrl-C (hex 03).

The time-of-day output is only available on the network or serial port used to give the F9 command.

The format of the default string returned with SHIFT-T is entered (assuming time on request is enabled) is as follows:

```
<SOH>DDD:HH:MM:SS.mmmQ<CR><LF>
```

where:

- <SOH>=ASCII Start-of-Heading character
- <CR>=ASCII Carriage Return character
- <LF>=ASCII Line Feed character
- YYYY=Year
- DDD=day-of-year.
- HH=hours.
- MM=minutes.
- SS=seconds.
- mmm=milliseconds.
- :=colon separator.
- Q=time quality character, as shown below
  SPACE = Time error is less than time quality flag 1's threshold

  . = Time error has exceeded time quality flag 1's threshold

  ***** = Time error has exceeded time quality flag 2's threshold

  # = Time error has exceeded time quality flag 3's threshold

  ? = Time error has exceeded time quality flag 4's threshold, or a reference source is unavailable

  Example:

To prepare Time on Request, enter:

```
SyncServer> F9
```

Then, to request the current time, enter SHIFT-T on your keyboard. (“T” does not appear).

Response:

```
<SOH>128:20:30:04.357*<CR><LF>
```

To exit F9, press Ctrl-C on your keyboard.

4.1.4 F50 - GPS Receiver LLA/XYZ Position

GPS Receiver LLA/XYZ Position

Use function F50 to display the current GPS position, as well as the following:

- Select the positional coordinate system, Latitude Longitude Altitude (LLA) or XYZ (Earth- Centered, Earth-Fixed XYZ coordinates).
- If LLA is selected, Altitude Mode shows the elevation in given meters.

Use the following format to display the current position of the GPS receiver in LLA coordinates:

```
F50<S>B<N><SEP>LLA<CR>
```

SyncServer S6x0 responds with the coordinate information in the following format:

```
F50<S>B<N><SIGN><S><DEG>d<MIN>'<SEC>"<S><SIGN><S><DEG>d<MIN>'<SEC>"<S><ALT><UNITS><CR><LF>
```

where:

- F50 = Function 50
- <S> = ASCII space character one or more.
- B = ASCII letter to denote Option Bay number follows
- <N> = Option Bay Number, 1.
- <SEP> = Separator
- LLA = LLA mode
- <CR> = carriage return character.
- <SIGN> = N or S for latitude; E or W for longitude;
- - for negative altitude and <S> or + for positive altitude.
- <DEG> = two-digit degrees for latitude or three-digit degrees for longitude.
- d = ASCII character d
- <MIN> = two-digit minutes.
- ' = ASCII character '
- <SEC> = two-digit seconds + 1 digit 10ths of seconds.
- “ = ASCII character ”
- <ALT> = altitude in meter
- <UNITS> = unit of altitude, ¡§m¡¦ for meters
- <LF> = line feed character.

For example, to display the LLA coordinates of the antenna, enter:

```
F50 B1 LLA<CR>
```

SyncServer S6x0 responds:

```
F50 B1 N 38d23'51.3" W 122d42'53.2" 58m<CR><LF>
```

To display the present antenna position using ECEF XYZ coordinates in meters, use the following format:

```
F50<S>B<N><SEP>XYZ<CR>
```

SyncServer S6x0 responds using the following format:

```
F50B<N><S><SIGN><S><MX>m<S><SIGN><S><MY>m<S><SIGN><MZ>m<CR><LF>
```

where:

- F = ASCII character F
- 50 = function number
- <S> = ASCII space character
- B = ASCII letter to denote Option Bay number follows
- <N> = Option Bay Number, SyncServer S6x0 only has 1
- <SIGN> = Either + or - for the position of the ECEF XYZ coordinates
- <MX> = Antenna X-position in meters to tenths of a meter
- <MY> = Antenna Y-position in meters to tenths of a meter
- <MZ> = Antenna Z-position in meters to tenths of a meter
- M = ASCII character m for Meters
- <ALT> = altitude in meters
- <CR> = carriage return character
- <LF> = line feed character

Example:

```
SynsServer> F50 B1 XYZ
```

Response:

```
: F50 B1 X 1334872.770000m Y 6073285.070000m Z 1418334.470000m
```

4.1.5 F73 - Alarm Status

Use function F73 to view alarm status. The SyncServer S6x0 will return a response in the follow format:

```
F73<SP>S<STATUS><SOURCE><SP><123456789ABCDEFGHIJ><CR><LF>
```

The alphanumeric characters 1-9 and A-J represent specific positions in the response string shown above. The following table describes F73's alarm indicators based on their position in the response string.

Table 4-2. F73 Alarm Indicators

Syntax	Alarm	Indicators	Description
`F`	n/a	n/a	ASCII character F
`7`	n/a	n/a	ASCII character 7
`3`	n/a	n/a	ASCII character 3
`<SP>`	n/a	n/a	ASCII space character, one or more
`S`	n/a	n/a	ASCII character S, Status delimiter
`<STATUS>`	Clock Status	"L" = Locked "U" = Unlocked	The Clock Status indicator reports "Locked" when the SyncServer S6x0 clock is locked to a reference source (e.g., GPS, IRIG, etc.). This is the normal operational state of the clock. While locked, the clock steers its internal oscillator to the reference source. The Clock Status indicator reports "Unlocked" when the SyncServer S6x0 clock is not locked to a reference source. This may be because the reference source is unlocked or unstable. While unlocked from a reference source, the SyncServer S6x0 uses its internal oscillator to keep time until a reference becomes available again.

...........continued

Syntax	Alarm	Indicators	Description
`<SOURCE>`	Clock Source	"A" = Clock to Timing I/O Slot A (J1A) "B" = Clock to Timing I/O Slot B (J1B) "P" = Clock to GNSS "R" = Clock to External Input Reference (J2A/B) "T" = Clock to NTP "F"= None	Same as WebGUI "Current Reference" row in Dashboard > Timing. This is also equivalent to the "Time input selected" notification. "A" and "B" encoding can also occur if the BNC is configured for 1PPS.
`<SP>`			ASCII space character, one or more
`1`	PLL Synthesizer	"–" = Locked "C" = Unlocked	The PLL Synthesizer indicator reports "Locked" during normal operation while the system clock's PLL is locked to the internal oscillator. The PLL indicator reports "Unlocked" if the SyncServer S6x0 clock's hardware PLL has failed. While the PLL indicator is "Unlocked", all SyncServer S6x0 clock timing parameters are unreliable and should not be used. Contact Microchip FTD Services and Support.
`2`		"–" = Locked	Always "–" for initial release.
`3`	Primary	"–" = OK "P" = Fault	Indicates OK when GNSS input qualified for time, which is equivalent to Green indication for GNSS on Dashboard > Timing> Timing Reference row. Note that disabling of GNSS will also generate "P".
`4`	(For future use)	"–" = OK	Always "–" for initial release.
`5`	IRIG - Slot A J1	"–" = OK "I" = Fault	Indicates OK when the Slot A-J1 input is qualified for time. This connector supports all IRIG inputs. • This is equivalent to Green indication for Slot A - J1 on Dashboard>Timing >Timing Reference row. • Note that disabling of AJ1 will also generate "I". • If this input is configured for PPS/10MPPS this alarm will react based on the condition of the input • This only applies to slot A.

...........continued

Syntax	Alarm	Indicators	Description
`6`	External Input Reference - Slot A J2	"–" = OK "A" = Fault	Indicates OK when the Slot A - J2 input is qualified for frequency. This connector supports only frequency inputs (1/5/10MHz). This is equivalent to Green indication for Slot A - J2 in WebGUI Dashboard > Timing > Holdover References row. Note that: • Disabling of Slot A - J2 will also generate "A". • This only applies to slot A.
`7`	Primary Power	"–" = OK "W" = Fault	The Primary Power indicator reports "OK" when the power supply voltages are normal. It reports "Fault" when the internal power supply voltages exceed +/-10% of nominal supply regulation. While the Primary Power indicator reports a fault, all outputs from the SyncServer S6x0 are unreliable and should not be used.
`8`	Secondary Power	Dual AC or Dual DC version "–" = OK "w" = Fault Single AC version "–" = OK	This alarm can only be set for a unit that has Dual AC or Dual DC installed. This field is set to "Fault" if either of the dual power supply inputs does not have valid power connected.
`9`	Rb Oscillator	Unit with Rb "–" = OK "R" = Fault Unit without Rb "–" = OK	The Rubidium Oscillator indicator reports "OK" when the Rubidium Oscillator is operating normally. It reports "Fault" when the Rubidium Oscillator is warming up or has a PLL fault. Faults that occur during the warm up period after the unit is started up are not significant. This is normal behavior as the oscillator must perform an initial transition from unlocked to locked. This alarm can only set on a unit that contains an Rb oscillator.
`A`	Excessive Frequency Adjustment	"–" = OK "X" = Fault	"X" is indicated when the "Excessive Frequency Adjustment" alarm is set.
`B`	Clock Status - First time lock	"–" = First time lock OK "A" = Clock Status has not locked since power on	"A"is indicated until the "First normal-track since power up" transient alarm has occurred. Thereafter it remains "–".
`C`	Time Error	"–" = OK "U" = Fault	"U" is indicated when the "Holdover time error threshold exceeded" condition is set. The severity setting has no impact. The condition for what will set this alarm is defined on the WebGUI Dashboard > Timing > Holdover form.
`D`	Timeout		Always "–"

...........continued

Syntax	Alarm	Indicators	Description
`E`	NTP		Always "–"
`F`	IRIG - Slot B J1	"–" = OK "I" = Fault	Indicates OK when the Slot B-J1 input is qualified for time. This connector supports all IRIG inputs. This is equivalent to Green indication for Slot B - J1 on Dashboard>Timing >Timing Reference row. Note that disabling of BJ1 will also generate "I". If this input is configured for PPS/10MPPS this alarm will react based on the condition of the input This only applies to slot B.
`G`	External Input Reference - Slot B J2	"–" = OK "A" = Fault	Indicates OK when the Slot B - J2 input is qualified for frequency. This connector supports only frequency inputs (1/5/10MHz). This is equivalent to Green indication for Slot B - J2 in WebGUI Dashboard > Timing > Holdover References row. Note that disabling of Slot B - J2 will also generate "A" This only applies to slot B.
`H`	(For future use)	"–" = OK	Always "–"
`I`	(For future use)	"–" = OK	Always "–"
`J`	(For future use)	"–" = OK	Always "–"
`<CR>`	n/a		Carriage return
`<LF>`	n/a		Line feed

Example:

```
SyncServer> F73
```

Response:

```
F73 : SLP X---IA-w-----------
```

4.1.6 show gnss status

This command provides GPS satellite tracking information:

```
show gnss status
```

Example:

```
SyncServer> show gnss status
```

Response:

```
Gnss Status
Latitude : 12 21 06.39 N
Longitude : 76 35 05.17 E
HGT Val Ellipsoid : 712.4 m
HDOP : 0.970000
PDOP : 1.980000
Fix Quality : 1
Used Satellites : 8
Receiver Status : Tracking
Operation Mode : Survey
Antenna Status : OK
SBAS Constellation : Not Tracking
Current GNSS Satellite View:
+-----------------------------------------------------------+
|Index |GnssID |SatID |SNR |Azimuth |Elev |PrRes |
|------ |------ |----- |----- |------- |-------- |--------- |
|1 |GPS |14 |25 |349 |50 | -10 |
|...... |...... |..... |..... |....... |........ |.......... |
|2 |GPS |18 |23 |65 |35 | 63 |
|...... |...... |..... |..... |....... |........ |......... |
|3 |GPS |21 |32 |146 |43 | -68 |
|...... |...... |..... |..... |....... |........ |......... |
|4 |GPS |22 |22 |13 |44 | 69 |
|...... |...... |..... |..... |....... |........ |......... |
|5 |GPS |25 |34 |108 |12 | 9 |
|...... |...... |..... |..... |....... |........ |......... |
|6 |GPS |26 |26 |191 |7 | -42 |
|...... |...... |..... |..... |....... |........ |......... |
|7 |GPS |27 |27 |255 |25 | 35 |
|...... |...... |..... |..... |....... |........ |......... |
|8 |GPS |31 |31 |185 |52 | 13 |
+-----------------------------------------------------------+
```

4.1.7 halt system

Use this command to shut down the operating system as a preparatory step before power-off. This command does not reboot the system.

Command Syntax:

```
halt system
```

The behavior of this command is the same as using the Web GUI to perform a Halt (Dashboard>Security>Services).

Example 1:

If using via serial connection to console port:

```
SyncServer> halt system
The system is being HALTED NOW
.............................
```

<now numerious messages will be received as processes are stopped>

```
reboot: System halted
```

Example 2:

If using SSH session:

```
S650> halt system
The system is being shutdown now
The system can be powered off in 60 seconds
.........................................
SyncServer>
```

The connection is lost and on the front panel the following message appears:

```
System shutting down...
The system can be powered
off after 60 seconds.
```

At this point SyncServer S6x0 must be re-powered for further operation.

4.1.8 history

The command provides a listing of user entries during this session, regardless of their validity. If a configuration command provides the configuration value(s) on the same entry line as the command, then the configuration value(s) will be shown in the history.

Responses are not shown in the history list.

Command Syntax:

```
history
```

Example:

SyncServer> history

Response:

```
0 2015-11-19 18:49:28 set ip address-mode LAN3 ipv4 dhcp
1 2015-11-19 18:49:37 F73
2 2015-11-19 18:49:46 this is not a legal command
3 2015-11-19 18:50:08 show gnss status
4 2015-11-19 18:50:38 set-session-timeout
5 2015-11-19 18:50:47 show-session-timeout
6 2015-11-19 18:50:58 history
```

- The DHCP configuration (item 0) is shown in history because it is accomplished on the same line as the command.
- The configured session timeout value does not appear (item 4) because the CLI prompts for that value on a response line.
- Responses to F73 (item 1) and show... requests (items 3,5) do not appear in history
- Anything entered, even if not valid syntax (item 2) will be maintained in the history.

4.1.9 show image

Use this command to display current version in active and backup locations, as well as which image will be used on boot.

Command Syntax:

```
show image
```

Example

```
SyncServer> show image
```

Response

```
SYSTEM IMAGE DETAILS
Active Image : 1
Backup Image : 2
Active Image Ver : 1.0.4
Backup Image Ver : 1.0.3.7
Next Boot Image : 1
```

This example tells us that:

- The active image (what is currently running in SyncServer S6x0) is 1.0.4. Note that this version is also displayed with the `show system` command.

- There is a backup image (2) and it contains software version 1.0.3.7.
- Next Boot Image identifies that if a reboot occurs it will load image 1, which we can deduce is the image we are currently running.

4.1.10 show ip

Use this command to display the current IP settings for all LAN ports.

Command Syntax:

```
show ip config
```

The information displayed is consistent with the content shown in the Web Interface (Dashboard>Network>Ethernet).

Example:

```
SyncServer> show ip config
```

Response:

```
Eth port config
---------------------------------------------------------
|Port|Speed |IPVersion |IPv4Mode|IPv6Mode|AutoConfig|
|----|----------|----------|--------|--------|----------|
|LAN1|AUTO |ipv4 |DHCP |STATIC |enable |
|....|..........|..........|........|........|..........|
|LAN2|AUTO |ipv4 |STATIC |STATIC |enable |
|....|..........|..........|........|........|..........|
|LAN3|AUTO |ipv4_ipv6 |STATIC |STATIC |enable |
|....|..........|..........|........|........|..........|
|LAN4|AUTO |ipv4_ipv6 |DHCP |DHCP |disable |
---------------------------------------------------------
IPv4 config
---------------------------------------------------------
|Port|Address |Subnet Mask |Gateway |
|----|----------------|----------------|----------------|
|LAN1|192.168.1.100 |255.255.255.0 |192.168.1.1 |
|....|................|................|................|
|LAN2|192.168.99.7 |255.255.255.0 |192.168.99.1 |
|....|................|................|................|
|LAN3|192.168.1.99 |255.255.255.0 |192.168.1.1 |
|....|................|................|................|
|LAN4|192.168.4.100 |255.255.255.0 |192.168.4.1 |
---------------------------------------------------------
```

```
IPv6 config
-----------------------------------------------------------------------------
|Port|Address |Pref|Gateway |
|----|--------------------------------|----|--------------------------------|
|LAN1| |0 | |
|....|................................|....|................................|
|LAN2| |0 | |
|....|................................|....|................................|
|LAN3|2001:db9:ac10:fe10::2 |64 |2002:0DB9:AC10:FE10::1 |
|....|................................|....|................................|
|LAN4| |0 | |
-----------------------------------------------------------------------------
```

Example 2:

```
SyncServer> show ip status
```

Response 2:

```
Ethernet MAC
-------------------------
|Port|MAC |
|----|------------------|
|LAN1|00:B0:AE:00:36:0B |
|....|..................|
```

```
|LAN2|00:B0:AE:00:36:0C |
|....|..................|
|LAN3|00:B0:AE:00:36:0D |
|....|..................|
|LAN4|00:B0:AE:00:36:0E |
-------------------------
Eth Status-IPv4
---------------------------------------------------------
|Port|Address |Subnet Mask |Gateway |
|----|----------------|----------------|----------------|
|LAN1|192.168.107.122 |255.255.255.0 |192.168.107.1 |
---------------------------------------------------------
Eth Status-IPv6
-----------------------------------------------------------
|Port|Address |Pref|Gateway |
|----|-------------------------------|----|---------------|
|LAN4|2001::120 |64 | |
------------------------------------------------------------
```

4.1.11 set ip

Use this command to set the address mode to DHCP (IPv4 or IPv6) for the LAN1-LAN6 ports. Use this command to provision the Host, Mask, and Gateway for IPv4 static addresses.

Command Syntax:

- To provision the IPv4 or IPv6 address mode on the specified LAN port as DHCP:

  ```
  set ip address-mode lan{1|2|3|4|5|6} {ipv4|ipv6} dhcp
  ```

  For changes to take effect, the specified LAN port must be restarted.
- To set the IPv4 address, mask and gateway of the Ethernet interfaces for the specified port:

  ```
  set ip ip-address lan{1|2|3|4|5|6} ipv4 address
  <addrv4_value> netmask <maskv4_value> gateway
  <gatewayv4_value>
  ```

  Note: Setting the IPv4 static address for a LAN port with this command automatically disables the DHCP address mode for that port.

  Example 1:

To set the address-mode of the Port 1 Ethernet interface to DHCP:

```
SyncServer> set ip address-mode lan1 ipv4 dhcp
```

Example 2:

To set the static IPv4 address for LAN1 to 192.168.2.11, the mask to 255.255.255.0, and the gateway 192.168.2.1:

```
SyncServer> set ip ip-address lan1 ipv4 address 192.168.2.11 netmask 255.255.255.0 gateway
192.168.2.1
```

4.1.12 set nena active

Use this command to enable the NENA response mode on this connection.

Command Syntax:

```
set nena active
```

Example:

```
SyncServer>set nena active
```

Response:

```
NENA response active: CR to trigger, ctrl-c to deactivate
2016 349 07:40:19 S+00
2016 349 07:40:21 S+00
```

```
2016 349 07:40:22 S+00
2016 349 07:40:22 S+00
2016 349 07:40:23 S+00
SyncServer >
```

4.1.13 set nena-format

Use this command to set the NENA format for the CLI connection.

Command Syntax:

```
set nena-format [0|1|8]
```

Example:

To set the NENA format to 8 for the serial timing output:

```
SyncServer>set nena-format 8
```

4.1.14 reboot system

This command halts current operation, then reboots the SyncServer S6x0. Except for no loss of power, this is functionally equivalent to power-up of the SyncServer S6x0.

```
reboot system
```

The behavior of this command is the same as using the Web GUI to perform a Reboot (Dashboard>Security>Services).

Example 1:

If using console port serial connection:

```
S650> reboot system
```

Response:

```
The system is going down for REBOOT NOW!
........................................
SyncServer login:
```

Example 2:

If using SSH session:

```
S650> reboot system
```

Response 2:

```
The system is going down for REBOOT NOW!
........................................
```

The connection will be lost after the REBOOT NOW! message.

4.1.15 set-session-timeout

Use this command to define a timeout for a CLI session. The session will auto-terminate if there is no session activity (i.e. user entries) for the configured duration. If the connection is remote SSH, the connection will terminate upon timeout. If the session is direct to the CONSOLE serial port, auto-logout will occur upon timeout.

Command Syntax:

```
set-session-timeout
```

The system will prompt for the timeout value.

Example:

To set the session timeout to one hour (3600 seconds):

```
SyncServer> set-session-timeout
```

The system will prompt for the timeout value.

```
Timeout ( 0 - 86400 sec):
```

Enter the following, then press Enter.

```
3600
```

Response:

```
3600 sec timeout set succcessfuly
```

4.1.16 show-session-timeout

Use this command to display the session timeout value.

Command Syntax:

```
show-session-timeout
```

Example:

```
SyncServer> show-session-timeout
```

Response:

```
The current session timeout - 3600 sec
```

4.1.17 show system

Use this command to display basic facts about the SyncServer S6x0.

Command Syntax:

```
show system
```

Example

```
SyncServer> show system
```

Response

```
Host Name : SyncServer
Serial Num : MSK102
Model Num : S650
Build : 1.0.4
Uname : Linux SyncServer 3.13.0 #1 SMP Tue Nov 17 13:19:51
PST 2015 armv7l
Uptime : 0 day(s) 0 hour(s) 24 minute(s) 48 second(s)
Load Avg : 0.69 0.42 0.38
Free Mem : 87.83 %
CPU Model : ARMv7 Processor rev 0 (v7l)
CPU Identifier : Altera SOCFPGA
Total Mem : 1007 MB
Oscillator Type : Rubidium
Update Available : Up to date
```

5. Web Interface

Note:
For security reasons, the SyncServer S6x0 only supports https However, the user will get warnings from most web browsers that a self-signed certificate is being used (not from a recognized certificate authority). Users should accept the warnings and proceed to the login page. The internal self-signed certificate can be renewed and updated on the Security->https page. Users can also request and install a https certificate

For security reasons, the SyncServer S6x0 will lock out a user if an invalid password is entered three times. The user is locked out for 1 hour. The lockout is also removed if the unit is rebooted. The lockout feature can be enabled/ disabled and the invalid password lockout count can be configured on the Admin->General page.

Note:
The default user name is “admin” and the default password is: Microsemi . To avoid unauthorized access, you should change the default password. When logging in for the first time, or after a factory default, the system will force you to change the password.

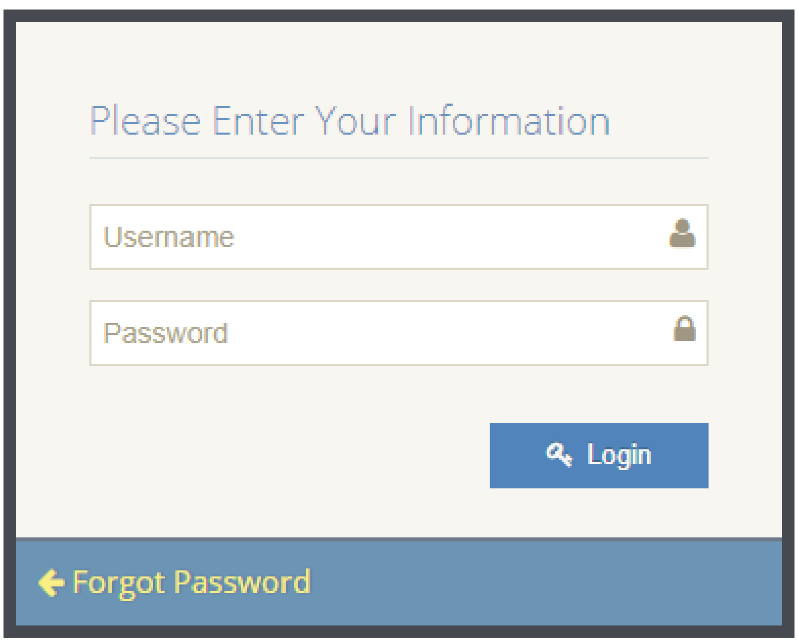
5.1 Web Interface

This chapter describes the web interface for the SyncServer S6x0.

See Communicating Through LAN1 Ethernet Port in Chapter 6 for details on how to access the web interface.

Note: For security reasons, the SyncServer S6x0 only supports https However, the user will get warnings from most web browsers that a self-signed certificate is being used (not from a recognized certificate authority). Users should accept the warnings and proceed to the login page.
The internal self-signed certificate can be renewed and updated on the Security->https page. Users can also generate a CSR and install a https certificate

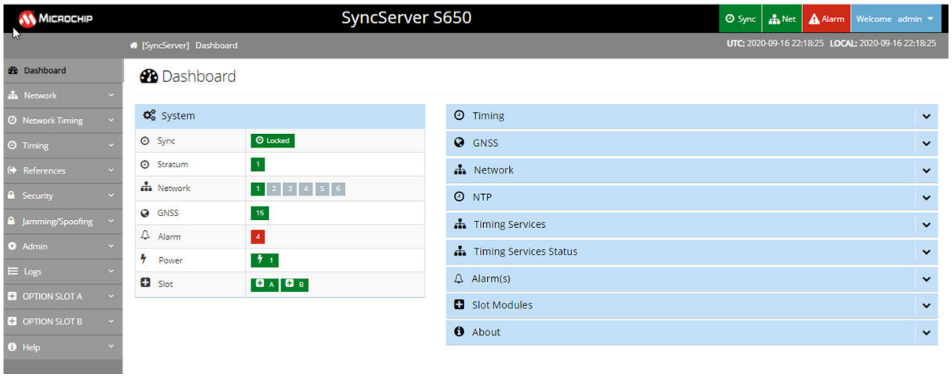
Figure 5-1. Login



For security reasons, the SyncServer S6x0 will lock out a user if an invalid password is entered three times. The user is locked out for 1 hour. The lockout is also removed if the unit is rebooted. The lockout can be configured on the Admin->General page.

Note: The default user name is “admin” and the default password is: Microsemi .
To avoid unauthorized access, you should change the default password. When logging in for the first time, or after a factory default, the system will force you to change the password.

Figure 5-2. Dashboard Screen



Note: UTC and local time are displayed in the upper right portion of the page. Local time is based on the timezone setting in the SyncServer unit. Daylight saving time is also applied to the local time if applicable. Local time is not determined by the location of the web browser.

Note: If the browser is displaying a busy indicator, then please wait until the previous action is complete before starting another action. Depending on the browser used, the web page responsiveness will vary due to the use of the encryption cipher suite used in the S6x0. Microchip recommends using the Google Chrome browser. Under heavy network traffic load, the web responsiveness will degrade.

Note: When system is under full rated load, opening more than one web session is not recommended. Doing so will have a large performance impact.

5.2 Status / Information Windows

The Status/Information windows in the dashboard, as shown in the following image, displays status details and information regarding the following:

- Timing
- GNSS
- Network
- NTP
- Timing Services
- Timing Services Status
- Alarms
- Slot Modules
- About

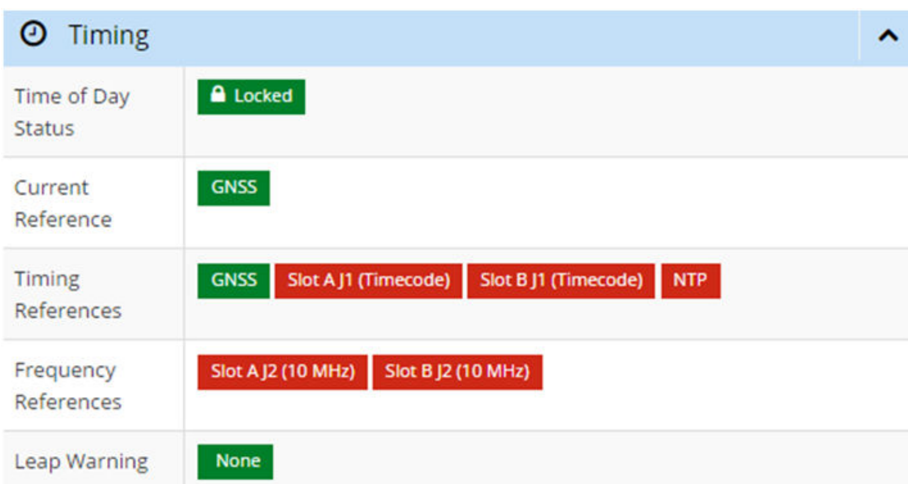
Clicking on the down arrow on a window expands the information under that topic.

Figure 5-3. Status/Information Windows

5.2.1 Timing Status & Information

The Timing window in the dashboard, as shown in the following image, displays status details and information about system timing, including current reference, lock status, and status of input references. See Table 5-1.

Figure 5-4. Timing Window



Note: The SyncServer 6x0 does not contain a battery-backed real time clock. Therefore, it will always boot up with a default value for the system time. This time will be updated when it obtains time from a time reference such as GNSS, IRIG, or NTP. The default value for the date is the software build date. This date will be used for the first log entries when booting up the unit. The time will change to local time during the boot-up process if a time zone has been configured.

Table 5-1. Timing Window Descriptions

Item	Details	Color Scheme
Time of Day Status	This row is essentially showing the time clock state. See Table 5-2 for descriptions of clock states.	Warmup Freerun Handset Locking Locked Bridging Holdover Holdover Recovering
Current Reference	This row shows the input reference that is currently “driving” the SyncServer. It could be a timing source (best case), an external holdover source, or the SyncServer internal reference (worst case). See Table 5-3 for details of current sources.	Green if any externally selected reference, Amber color only if internal oscillator.
Timing References	This row shows all enabled time references.	If a time reference is ready to be used it will be green. If it is not ready it will be red.
Frequency References	This row shows all enabled frequency-only references. The use of a frequency reference is thought of as a method for holding-over time when there either was never an active time source or it was lost.	If a holdover source is ready to be used it will be green. If it is not ready it will be red.
Leap Pending	This row indicates if a Leap second is pending.	If there is no warning of a Leap second pending it will be green. If there is a warning of a Leap second pending it will be red.

The SyncServer S600/S650 has separate timing and frequency clock controls. The time and frequency clocks are usually in the same clock state. If they are different, then the “Current Reference” row will include text after the icon which displays the frequency clock state. The “Time of Day Status” always shows the time clock state.

While locking to a new reference, the two states may be different for a brief time.

If there are no valid timing references, but there is a valid frequency reference, then there should be text shown since the frequency and time clock states are different.

The system time locks, but does not frequency lock to an NTP reference. Therefore, the frequency status will display free-run while the system is locked to an NTP reference and there are no frequency references connected.

Table 5-2. Status - Clock State Descriptions

Status Indication	Meaning	Details
Warmup	SyncServer not ready for any type of synchronization functionality. This is a one-time status following power-up	Directly equal to the common warmup clock state (to both freq and time)
Freerun	SyncServer does not have a time reference and never has had one since powerup.	

...........continued

Status Indication	Meaning	Details
Handset	For future use.	
Locking	SyncServer has selected a qualified active time input for use and is now in process of aligning all outputs to it.	In this status, the Current Source row will, by definition, have a “green” item that has a match to it in the Timing Sources row. An “active” time source just means one that is continuously providing time (where continuous is a relative term – in general it is an update per second).
Locked	SyncServer outputs are now aligned to a selected active time source.	
Bridging	SyncServer no longer has a selected active time source, but it hasn’t been that way for very long.	This is really just the beginning of holdover, but is a period where the output performance should be as good as when in Locked. It provides a hysteresis buffer to prevent nuisance Locked-Holdover-Locked transitions. In this state the Current Source row will NOT have a green item from the Timing Sources row.
Holdover	SyncServer no longer has a selected active time source, and it has been that way for longer than the Bridging duration. Also the condition for “red holdover” (next row) is not met.	Either we are holdover using an external frequency reference OR we are in holdover using the SyncServer internal reference AND the duration is less than a user-specified time duration.(1)
Holdover	Same as prior row but specific additional conditions are met. This condition occurs if the current source is the internal oscillator and the duration in time holdover has exceeded the time defined by user in the Timing > Holdover window.	The unit has been in holdover for more than a user-specified duration and the holdover is based on the SyncServer internal reference. In this case the Holdover Sources row will not contain any green items.
Relocking	SyncServer has selected a qualified active time input for use and is now in process of aligning all outputs to it.	

(1) The main purpose of holdover is to allow the S6xx time server to continue to operate as “normal” using the internal oscillator or external frequency reference even though the connection the GNSS is lost. The user defines how long this holdover period will last. During this time the NTP Reference Time Stamp is updated regularly indicating the S6xx is still connected to a time reference. Once the user defined holdover period is exceeded the reference time stamp is no longer updated. This is important information to provide to NTP clients as they can then determine whether or not to continue to synchronize to the S6xx. Once the S6xx reacquires GNSS and relocks, the NTP Reference Time Stamp will again be updated regularly.
By NTP protocol definition, once an NTP server locks to a time reference and sets the Leap Indicator to 00 from 11 it never returns to 11. In other words, once the unit has left stratum 16 it should never return to stratum 16. Instead it uses the reference time stamp behavior mentioned above.

Table 5-3. Status - Current Source Details

Item	Status Where it Will Happen	Details
No current source	Warmup	Directly equal to the common warmup clock state (to both freq and time)
Current Source taken from Timing References	Locking Locked Relocking	When the status is any of these there MUST be a selected time source, which takes precedence in the Current Reference row (more important than if there is also a qualified frequency reference). There must be at least one green item in the Timing References row. The leftmost green one will be identically indicated in the Current Reference row. This is because the leftmost green item in Timing References is the highest priority time source and therefore must be selected. For example, if it is GNSS it will appear identically as Current Reference and in Timing References row.
Current Source taken from Frequency References	Freerun Bridging Holdover Holdover	For any Status in this category there cannot be a qualified Timing Reference (nothing green in that row), so it is certain that SyncServer is using frequency-only reference. If there is a qualified Frequency Reference (meaning something green in this row), then the leftmost green one will be the current source. If there is no qualified Frequency Reference (nothing green in that row) then all that remains is the SyncServer internal reference, which is what appears in the Current Reference row. In this case the entry will be one of the following, depending on the specific SyncServer product oscillator type: • Internal Rb, • Internal OCXO • Standard

5.2.2 GNSS Status & Information

The GNSS window in the dashboard, as shown in the following image, displays status details and information about GNSS. C/No is the carrier-to-noise density which is defined as the carrier power divided by the noise power spectral density. Higher C/No results in better tracking and performance.

The GNSS signal strength (C/No) can vary from 1 to 63. Typical values for a good GNSS installation will be between 35 and 55. A satellite ID of "0?" may be temporarily displayed if the system is not fully tracking the satellite.

Figure 5-5. GNSS Window

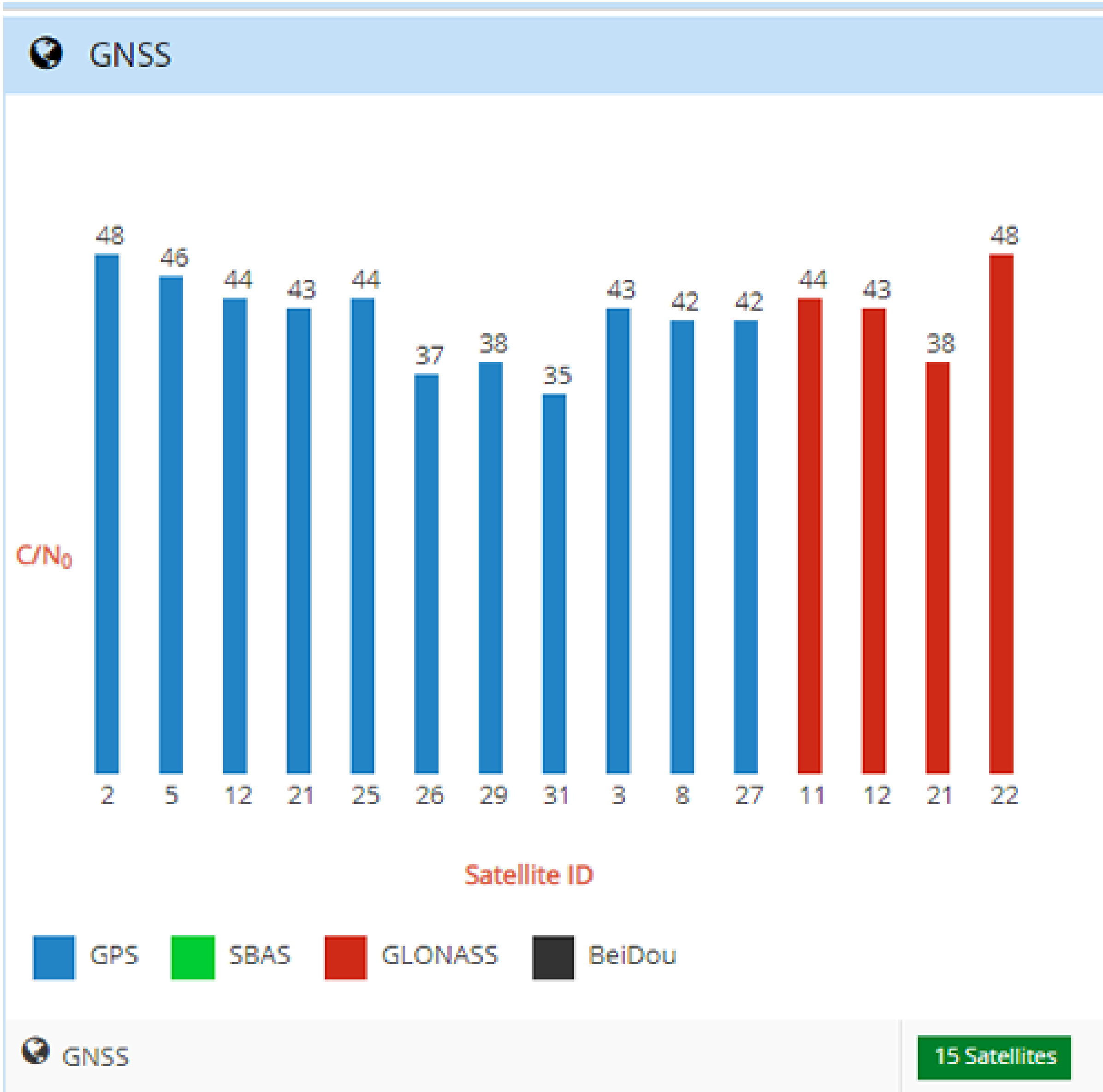


Table 5-4. GNSS Window - Descriptions

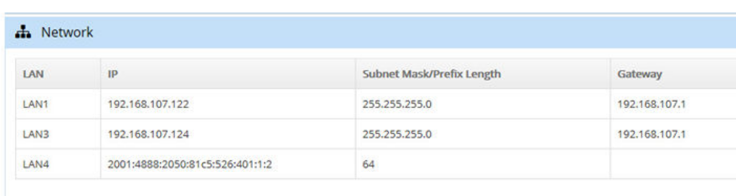
Field	Potential Values	Notes
GNSS	Lists number of satellites being tracked	
Antenna Status	• OK - operating normally • Open - open circuit in antenna cable or no DC load in splitter • Short - short circuit in antenna cable • Initializing - temporary condition	

...........continued		
Field	**Potential Values**	**Notes**
Receiver Status	• Invalid - not tracking • Tracking NO UTC - tracking, but UTC offset not known • Tracking - tracking	
Position Status	• No Data - no position data • Survey 2D - calculated 2D position, lat/lon but no elevation • Survey - calculating position and surveying to average position • Position Fix - position fixed, either manual or to surveyed position	
Position	Position - latitude, longitude, and height/ elevation	
GNSS Receiver Firmware Upgrade	• Never run - upgrade process has not run • In progress - GNSS receiver being upgraded • Not required - GNSS receiver firmware is at correct revision • Successful - GNSS receiver firmware upgraded • Failed - GNSS receiver firmware upgrade failed • Interrupted - GNSS receiver firmware upgrade failed	If failed or interrupted conditions persist, the unit should be rebooted.

5.2.3 Network Status & Information

The Network window in the dashboard, as shown in the following image, displays status details and information about the network ports in use.

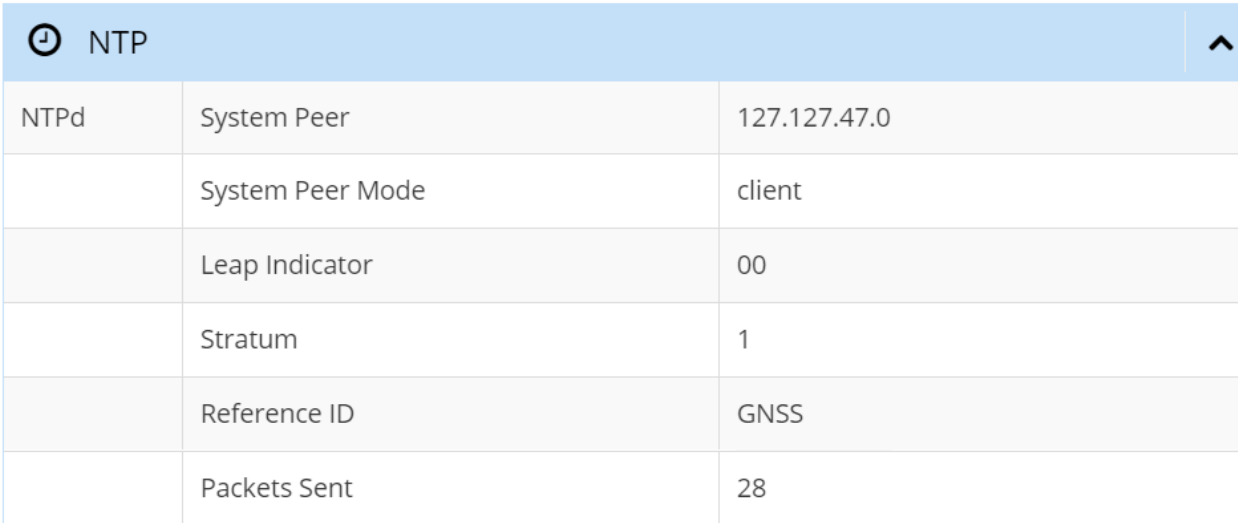
Figure 5-6. Network Window



5.2.4 NTP Status & Information

The NTP window in the dashboard, as shown in the following image, displays status details and information about the NTP configuration.

Figure 5-7. NTP Window



NTP

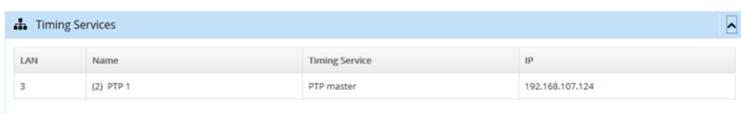
NTPd	System Peer	127.127.47.0
	System Peer Mode	client
	Leap Indicator	00
	Stratum	1
	Reference ID	GNSS
	Packets Sent	28

Note: The dashboard will provide Leap indicator information as soon as it is available. For GPS, this is usually many months ahead.
The Leap indicator information in the NTP messages sent out the Ethernet port(s) will only be sent out the last 24 hours before the event for the “01” or “10” values of this parameter. See Table 5-5 for more details about the Leap indicator.

5.2.5 Timing Services Information

The Timing Services window in the dashboard, as shown in the following image, displays status details and information about the timing service on each port.

Figure 5-8. Timing Services Window



Timing Services

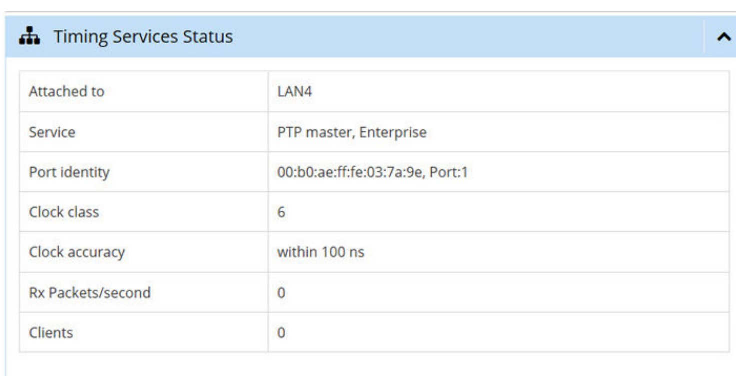
LAN	Name	Timing Service	IP
3	(2) PTP 1	PTP master	192.168.107.124

5.2.6 Timing Services Status

The Timing Services Status window in the dashboard, as shown in the following image, displays status details and information for the NTP reflector and PTP.

Note: The row labeled with “Service” is a configuration of the port. The Timing Services Status window shows this configuration. For PTP, the actual PTP Grandmaster operational state as either Passive or Master is found in the window Network Timing > NTPr/PTP Status, in the row “Port State”. See Figure 5-27.

Figure 5-9. Timing Services Status Window



Timing Services Status

Attached to	LAN4
Service	PTP master, Enterprise
Port identity	00:b0:ae:ff:fe:03:7a:9e, Port:1
Clock class	6
Clock accuracy	within 100 ns
Rx Packets/second	0
Clients	0

5.2.7 Alarm Information

The Alarms window in the dashboard, as shown in the following image, displays active alarms.

Note: The alarm time is always displayed using UTC time, regardless of any configured local timezone.

Figure 5-10. Alarms Window

Alarm(s)

#	Time	Severity	Name
1	2016-05-02 21:38:009	MINOR	J2B input loss of signal
2	2016-05-02 21:36:041	MAJOR	Ethernet port 2 link down

5.2.8 Slot Modules Status & Information

The Slot Modules window in the dashboard, as shown in the following image, displays status details about the modules installed in the Options Slots.

Figure 5-11. Slot Modules Window

Slot Modules

Modules	Type	Status
Slot A	Timing I/O + HaveQuick/PTTI Card	Installed
Slot B	Timing I/O + Fiber Input Card	Installed
10G	10G Ethernet Card	Installed

5.2.9 "About" Device Information

The "About" window in the dashboard, as shown in the following image, displays system information about the unit.

Figure 5-12. About Window

About

Hostname	SyncServer
Model	SyncServer S650
Serial Number	RKT-15309034
Release Version	3.0.6
Up Time	11 day(s) 8 hour(s) 32 minute(s) 59 second(s)
Memory Free	81.36 %
Oscillator	Rubidium
Update Availability Status	Unavailable: last check unsuccessful

Note: The update available feature will only function if LAN1 has been configured with an IPv4 address and a DNS server is configured. The DNS server can be either automatically configured via DHCP or manually when using a static IP address. The update available feature can be disabled on the Admin->General page.

Note: You can check for the latest version number of SyncServer S600 and S650 software at these URLs:
http://update.microsemi.com/SyncServer_S600

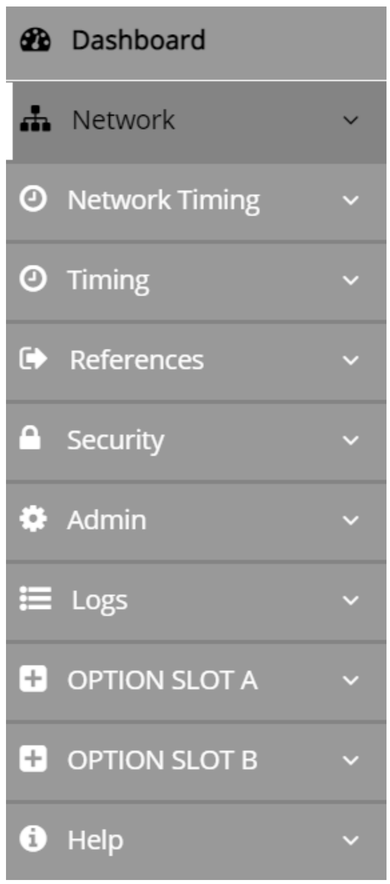
http://update.microsemi.com/SyncServer_S650

The number of the most current version of the software will appear. You can compare this to the version number installed in the SyncServer by proceeding to the web GUI Dashboard and finding the version number in the About drop down on the right side. If you do not have the latest version installed consider contacting Technical Support.

5.3 Navigation Windows

The navigation portion of the web interface is used to access the various pages to configure different aspects of the SyncServer S6x0 and to view status information. See the following image. The navigation menu will expand and contract depending on the current selection.

Figure 5-13. Navigation Portion of Dashboard



5.3.1 Network Configuration Windows

The Network tab on the dashboard provides access to windows for Ethernet, SNMP, SNMP Trap configuration, and Ping.

5.3.1.1 Network - Ethernet Configuration

Use this window to configure or modify the Ethernet setting for LAN1 - LAN6, and to manually set the DNS server address for LAN1. There is a separate “Apply” button for each Ethernet port and the DNS server address configuration.

The following Ethernet parameters can be configured:

- Speed

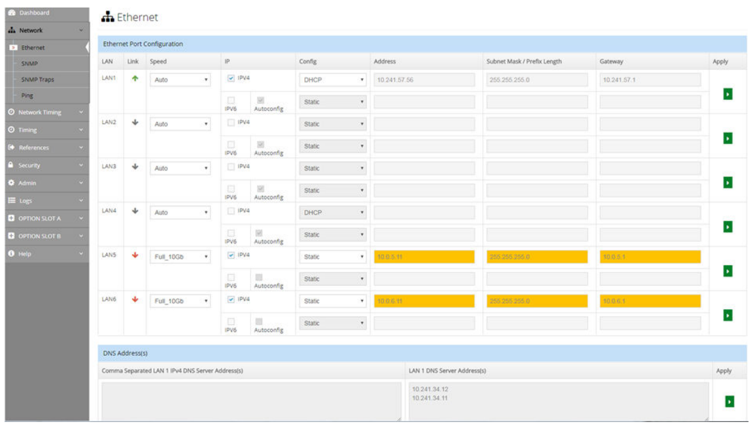
- Auto | Full 100 | Full 1000
- IP format
  - IPv4 | IPv6
- Config
  - Static | Dynamic
  - IPv6 Auto Config
- IP address
- Subnet mask for IPv4, prefix length for IPv6
- Gateway address

DNS server addresses can be added for LAN1. This will usually be necessary if LAN1 is configured with a static IP address.

See the following image. See Chapter 12 for information on Ethernet port isolation, management port rules, and timing port rules.

Note: Each Ethernet port should be configured on a different subnet.

Figure 5-14. Network - Ethernet Configuration Window



5.3.1.2 Network - SNMP Configuration

Use this window to add, edit or delete v2 communities, and to add or delete SNMP users. See the following image.

The following SNMP parameters can be configured:

- Basic Configuration
  - sysLocation, 1-49 characters
  - sysName, 1-49 characters
  - sysContact, 1-49 characters
  - Read Community, 1-49 characters, or blank to disable SNMPv2c reads
  - Write Community, 1-49 characters, or blank to disable SNMPv2c writes

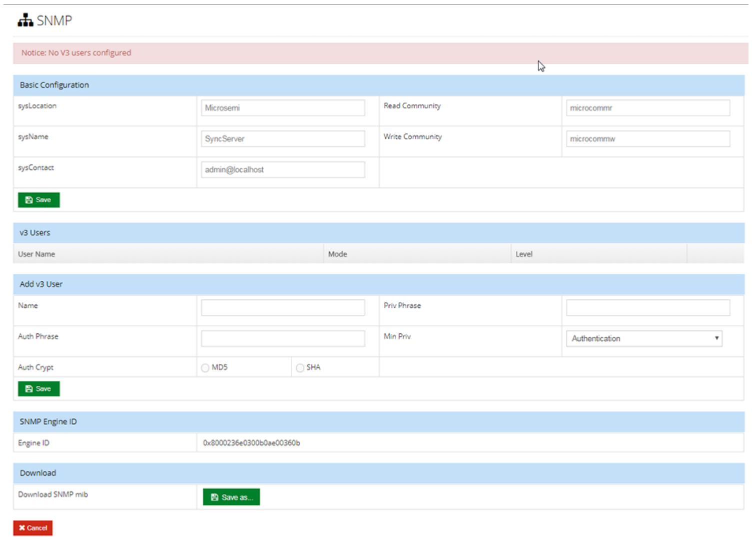
Note: SNMPv2 can be disabled by configuring blank read and write community names.

- Add v3 User - up to 10 users can be added
  - Name, 1-32 characters
  - Authentication Phrase, 1-49 characters
  - Authentication Encryption: MD5 or SHA
  - Privacy Phrase, 8-99 characters
  - Privacy Selection: “Authentication” or “Authentication & Privacy”.
    Privacy uses AES128
    Note: SNMP user names, community names, and privacy/authentication phrases can contain all ASCII characters except (<), (&), (>), (“), (').

The SNMP engine ID is displayed for the user's convenience. The SNMP MIB files for use with the SyncServer can be downloaded on this page.

Note: Changing an SNMP configuration parameter (such as community or SNMPv3 user), will cause SNMP to restart and the MIB2 sysuptime will restart counting upward.

Figure 5-15. Network - SNMP Window



5.3.1.3 Network - SNMP Trap Configuration

Use this window add or edit SNMP trap recipients. Up to 10 trap managers can be added.

The following parameters can be configured:

- IP Address - IPv4 or IPv6 address of trap manager
- Trap Version: v2c or v3
- User / Community, 1-32 characters
- Authentication Phrase (v3 only), 1-32 characters
- Privacy Phrase (v3 only, privacy uses AES128), 1-32 characters
- Authentication Encryption: MD5 or SHA (v3 only)
- Checkbox enable to send SNMP inform instead of SNMP trap

See the following image.

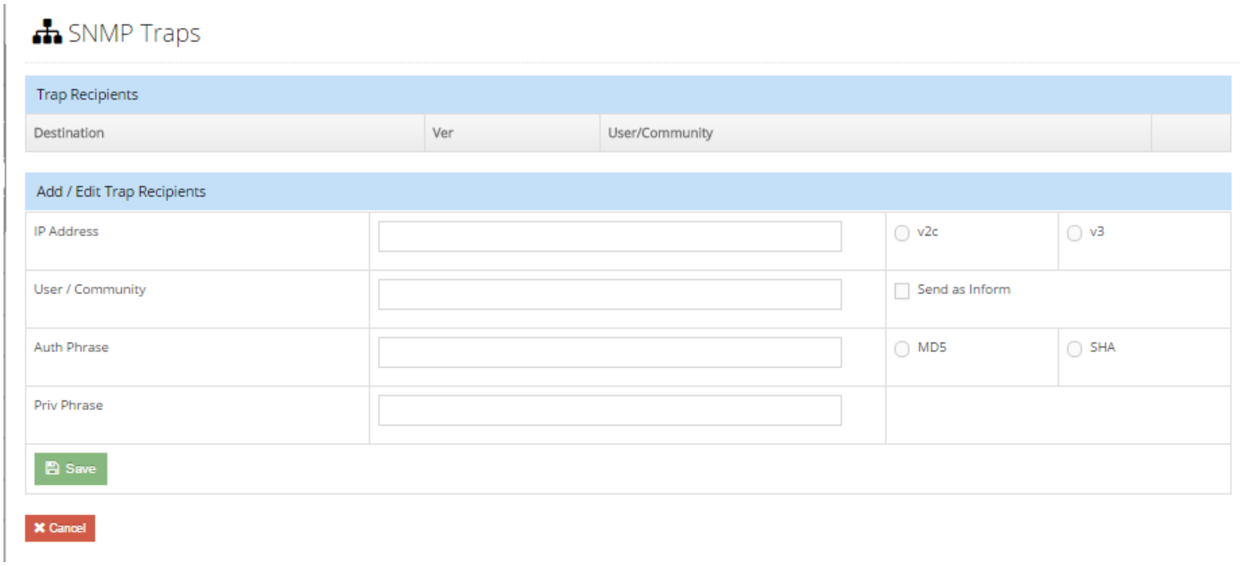
Note: Some SNMP browsers and trap managers require that an SNMPv3 user be created with the same username and authentication as used for the trap configuration in order for the SNMPv3 discovery process to complete properly.

Note: SNMP is designed to be used with LAN1. Do not configure a SNMP manager address in a subnet used by the other LAN ports (LAN2 - LAN6).

Note: Up to 10 SNMP trap recipients can be configured.

Note: Changing an SNMP configuration parameter (such as community or SNMPv3 user), will cause SNMP to restart and the MIB2 sysuptime will restart counting upward.

Figure 5-16. Network - SNMP Traps

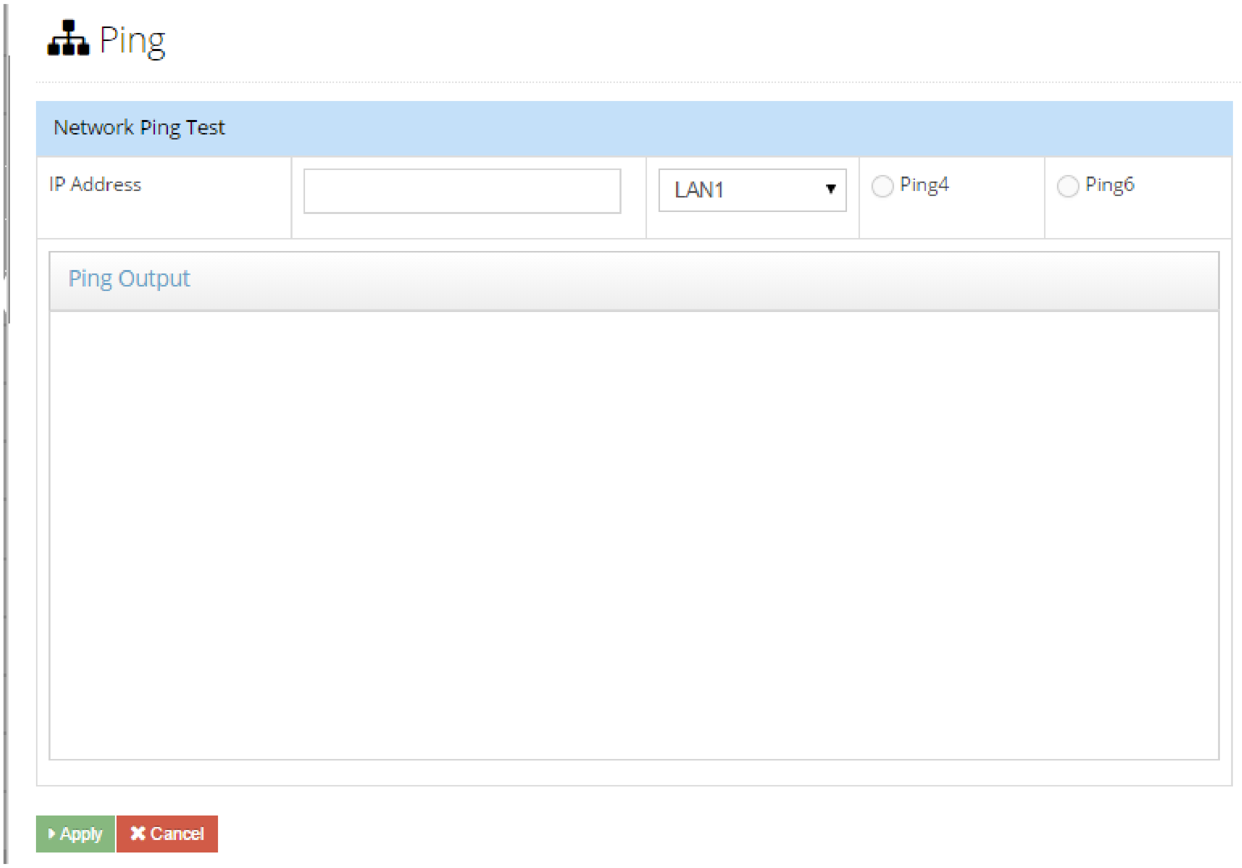


5.3.1.4 Network - Ping

Use this window to perform network ping tests. Use ping to test network connectivity out the LAN ports as needed. The result of the ping will be displayed in the window when completed. An IPv4 or IPv6 address should be entered in the IP address field. See the following image.

Ping may not operate as expected when IPv6 auto-config is enabled. An IPv6 source address may be used that doesn't route correctly to the destination address.

Figure 5-17. Network - Ping Window



5.3.2 Network Timing Windows

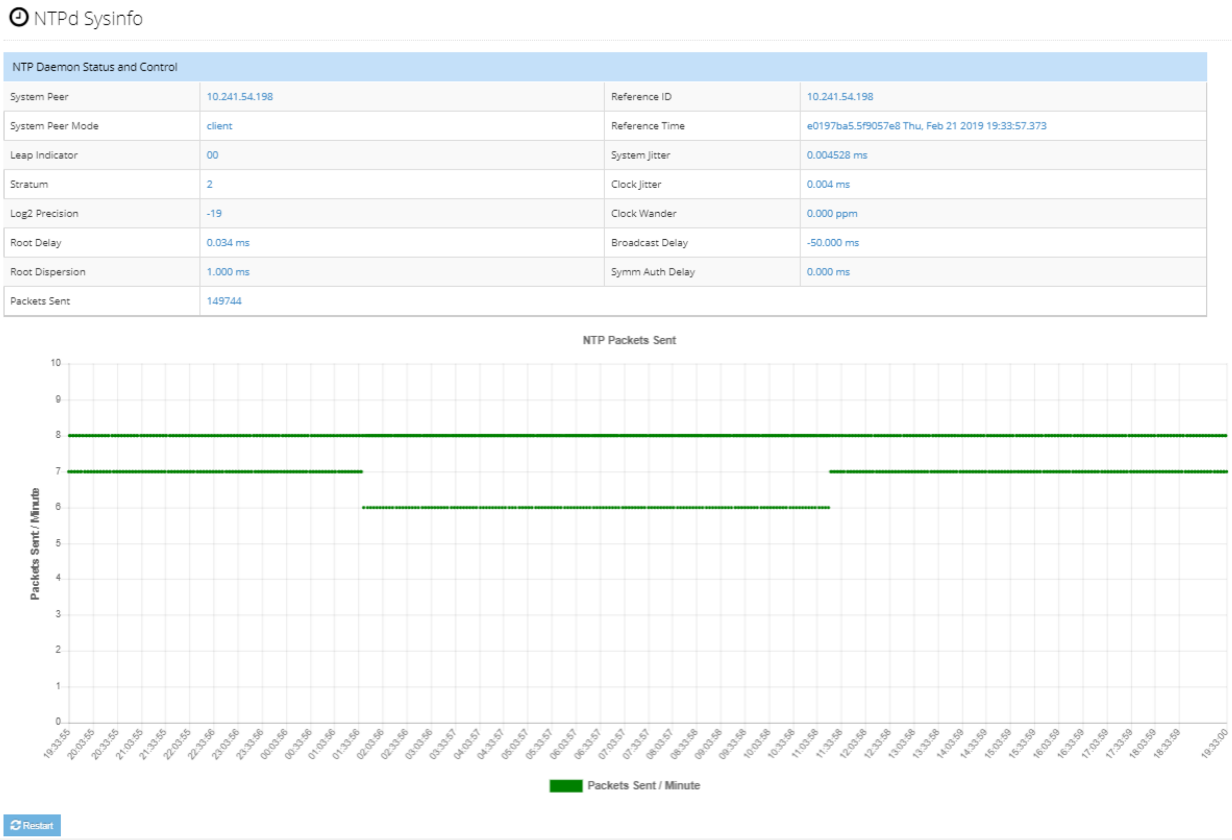
The Network Timing tab on the dashboard provides access to windows to configure NTP, view NTP Daemon Status and Control, view NTP Associations, to configure PTP and NTP reflector, and get status for PTP and NTP reflector.

5.3.2.1 NTP SysInfo Window

Use this window to view NTP Daemon Status and Control.

See the following image. See Table 5-5 for descriptions of NTP Daemon Status and Control parameters.

Figure 5-18. NTP SysInfo Window



At the bottom of the Sysinfo page, a graph is included that shows the NTP packet load. It displays the number of packets per minute sent each minute over the last 24 hours.

The restart button at the bottom of the page will restart NTPd. This will also clear the statistics and the graph.

Table 5-5. NTPd SysInfo Parameter Descriptions

Parameter	Description
System Peer	The IP address of the clock source. The source is selected by the NTP daemon that is most likely to provide the best timing information based on: stratum, distance, dispersion and confidence interval. The address of the local SyncServer Hardware Clock can be viewed in the hardware reference clock section of the NTP associations page.

...........continued

Parameter	Description
System Peer Mode	The relationship of the SyncServer to a system peer, usually a "client". Depending the configuration, the mode can be: • **Client**: A host operating in this mode sends periodic messages regardless of the reachability state or stratum of its peer. By operating in this mode the host, usually a LAN workstation, announces its willingness to be synchronized by, but not to synchronize the peer. • **Symmetric Active**: A host operating in this mode sends periodic messages regardless of the reachability state or stratum of its peer. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer. • **Symmetric Passive**: This type of association is ordinarily created upon arrival of a message from a peer operating in the symmetric active mode and persists only as long as the peer is reachable and operating at a stratum level less than or equal to the host; otherwise, the association is dissolved. However, the association will always persist until at least one message has been sent in reply. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer. A host operating in client mode (a workstation, for example) occasionally sends an NTP message to a host operating in server mode (the SyncServer), perhaps right after rebooting and at periodic intervals thereafter. The server responds by simply interchanging addresses and ports, filling in the required time information and returning the message to the client. Servers need retain no state information between client requests, while clients are free to manage the intervals between sending NTP messages to suit local conditions. In the symmetric modes, the client/server distinction (almost) disappears. Symmetric passive mode is intended for use by time servers operating near the root nodes (lowest stratum) of the synchronization subnet and with a relatively large number of peers on an intermittent basis. In this mode the identity of the peer need not be known in advance, since the association with its state variables is created only when an NTP message arrives. Furthermore, the state storage can be reused when the peer becomes unreachable or is operating at a higher stratum level and thus ineligible as a synchronization source. Symmetric active mode is intended for use by time servers operating near the end nodes (highest stratum) of the synchronization subnet. Reliable time service can usually be maintained with two peers at the next lower stratum level and one peer at the same stratum level, so the rate of ongoing polls is usually not significant, even when connectivity is lost and error messages are being returned for every poll.

...........continued	
Parameter	**Description**
Leap Indicator	The Leap Indicator (LI) is a two-bit binary number in the NTP packet header that provides the following information: • Advance warning that a leap second adjustment will be made to the UTC timescale at the end of the current day. Leap seconds are events mandated by the world time authority (BIPM) in order to synchronize the UTC time scale with the earth's rotation. • Whether the NTP daemon is synchronized to a timing reference. LI Meaning 00 No Warning 01 Leap second insertion: Last minute of the day has 61 seconds. 10 Leap second deletion: Last minute of the day has 59 seconds. 11 Alarm condition (Not synchronized) When the SyncServer or NTP daemon is started or restarted, the leap indicator is set to “11”, the alarm condition. This alarm condition makes it possible for NTP clients to recognize that an NTP server (the SyncServer) is present, but that it has yet to validate its time from its time sources. Once the SyncServer finds a valid source of time and sets its clock, it sets the leap indicator to an appropriate value. The NTP Leap Change Alarm on the ADMIN - Alarms page can be configured to generate an alarm and send notifications each time the leap indicator changes state.
Stratum	This is an eight-bit integer that indicates the position of an NTP node within an NTP timing hierarchy. It is calculated by adding 1 to the stratum of the NTP system peer. For the SyncServer, the stratum values are defined as follows: Stratum Meaning 0 Hardware Clock when locked 1 Primary server 2-15 Secondary server 16-255 Unsynchronized, unreachable For example, the SyncServer is: • stratum 1 when the Hardware Clock (stratum 0) is synchronized to an input reference, in holdover mode, or in freerun mode. • stratum 2 through 15 when it is synchronized to a remote NTP server. • stratum 16 when it is unsynchronized, indicating that it is searching for a valid source of timing information.
Log2 Precision	This is a signed integer indicating the precision of the selected peer clock, in seconds to the nearest power of two. A typical value is -18 for a Hardware Clock where the uppermost 18 bits of the time stamp fractional component have value, indicating a precision in the microsecond range.
Root Delay	This is a measure of the total round trip delay to the root of the synchronization tree. A typical value for a SyncServer operating at stratum 1 would be 0 since the SyncServer is a root of the synchronization tree For other stratum levels, an appropriate value is displayed. Depending on clock skew and dispersion, this value could be positive or negative.
Root Dispersion	This is a signed fixed-point number indicating the maximum error relative to the primary reference source at the root of the synchronization subnet, in seconds. Only positive values greater than zero are possible.
Packets Sent	Count of the number of NTP packets sent since NTPd was last restarted.

...........continued	
Parameter	**Description**
Reference ID	This is a four-byte field used to identify the reference clock source. At initialization, while the stratum is 16, this field shows the progression of the NTP clock PLL. The field will start with a value of INIT (may be displayed as 73.78.73.84, the ASCII decimal values). Once a peer has been selected, the clock may be stepped, in which case the reference ID field will change to STEP (or 83.84.69.80). Once the PLL is locked, the stratum will be updated and the reference ID will identify the selected peer. In the case of a SyncServer operating at stratum 1, the reference ID will display the source for the local timing reference (such as GNSS). In the case where the selected peer is another NTP server, the reference ID will display the IP address of the server or a hash unique to the association between the SyncServer and the remote server.
Reference Time	The time when the SyncServer last received an update from the selected peer. Represented using time stamp format in local time. If the local clock has never been synchronized, the value is zero. A time stamp of zero corresponds to a local time of Thu, Feb 7 2036 6:28:16.000. This value is typically updated every 16 seconds for a locally attached hardware reference (e.g., GNSS, IRIG) and in an interval of 64- 1024 seconds for a readily accessible remote NTP server.
System Jitter	Jitter (also called timing jitter) refers to short-term variations in frequency with components greater than 10 Hz.
Clock Jitter	Jitter (also called timing jitter) refers to short-term variations in frequency with components greater than 10 Hz.
Clock Wander	Wander refers to variations in frequency with components less than 10 Hz.
Broadcast Delay	The broadcast and multicast modes require a special calibration to determine the network delay between the local and remote servers. Typically, this is done automatically by the initial protocol exchanges between the client and server. This is the broadcast or multicast delay reported by the NTP daemon.
Symm Auth Delay	When NTP authentication is enabled and performed on outgoing NTP packets, this adds a trivial amount of fixed delay that can be removed based on the authdelay value. This value is always set to zero on the SyncServer.

Note: If the system is using NTP as the reference and the NTP server is performing a leap smear, then all non-NTP outputs of the system will be degraded, especially outputs on the optional I/O modules.

5.3.2.2 NTP Associations

Use this window to view NTP Associations.

See the following image. See Table 5-6 for descriptions of NTPd Associations parameters.

Figure 5-19. NTPd Associations Window

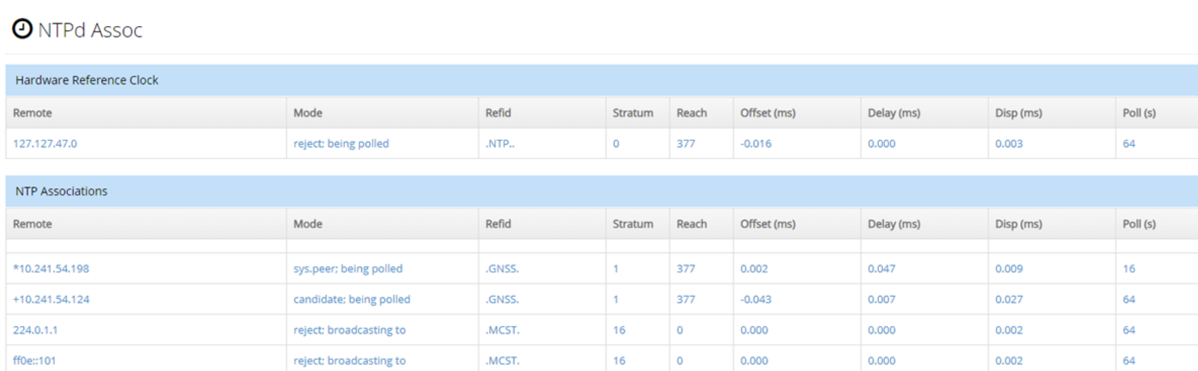


Table 5-6. NTPd Associations Parameters

Parameter	Description
Remote	The domain name or IP address of the remote end of the NTP association. “Hardware Clock” is the SyncServer's Hardware Clock. In the case of a remote NTP connection, this will be the IP address of the remote end. The character in the left margin indicates the mode in which this peer entry is operating: • (space) reject The peer is discarded as unreachable, synchronized to this server (synch loop) or outrageous synchronization distance. • x = falsetick The peer is discarded by the intersection algorithm as a falseticker. • ,(period) = excess The peer is discarded as not among the first ten peers sorted by synchronization distance and so is probably a poor candidate for further consideration. • - (minus) = outlier The peer is discarded by the clustering algorithm as an outlier. • + (plus) = candidate The peer is a survivor and a candidate for the combining algorithm. • # (pound sign) = selected The peer is a survivor, but not among the first six peers sorted by synchronization distance. If the association is ephemeral, it may be demobilized to conserve resources. • * (asterisk) = sys.peer The peer has been declared the system peer and lends its variables to the system variables. • o = pps.peer The peer has been declared the system peer and lends its variables to thesystem variables. However, the actual system synchronization is derived from a pulse-per-second (PPS) signal, either indirectly via the PPS reference clock driver or directly via kernel interface.
Mode	
Ref Id	This is a four-byte field used to identify the reference clock source. At initialization, while the stratum is 16, this field shows the progression of the NTP clock PLL. The field will start with a value of INIT (may be displayed as 73.78.73.84, the ASCII decimal values). Once a peer has been selected, the clock may be stepped, in which case the reference ID field will change to STEP (or 83.84.69.80). Once the PLL is locked, the stratum will be updated and the reference ID will identify the selected peer. In the case of a SyncServer operating at stratum 1, the reference ID will display the source for the local timing reference (e.g., GNSS, IRIG, FREE). In the case where the selected peer is another NTP server, the reference ID will display the IP address of the server or a hash unique to the association between the SyncServer and the remote server.
Stratum	The stratum level of the remote clock in the NTP hierarchy. Lower values are given more emphasis. For the local Hardware Clock, stratum 0 is a special value that indicates the Hardware Clock it is synchronized by a “timing root” reference such as GNSS. Values in the range of 1 through 15 indicate the number of steps the remote NTP connection is from its timing root. Stratum 16 is a special value that indicates that the remote connection is not synchronized. The stratum reported by the SyncServer is incremented by one from its synchronizing peer. For example, while synchronized to the Hardware Clock (Stratum 0), the stratum of the SyncServer is one (Stratum 1).

...........continued

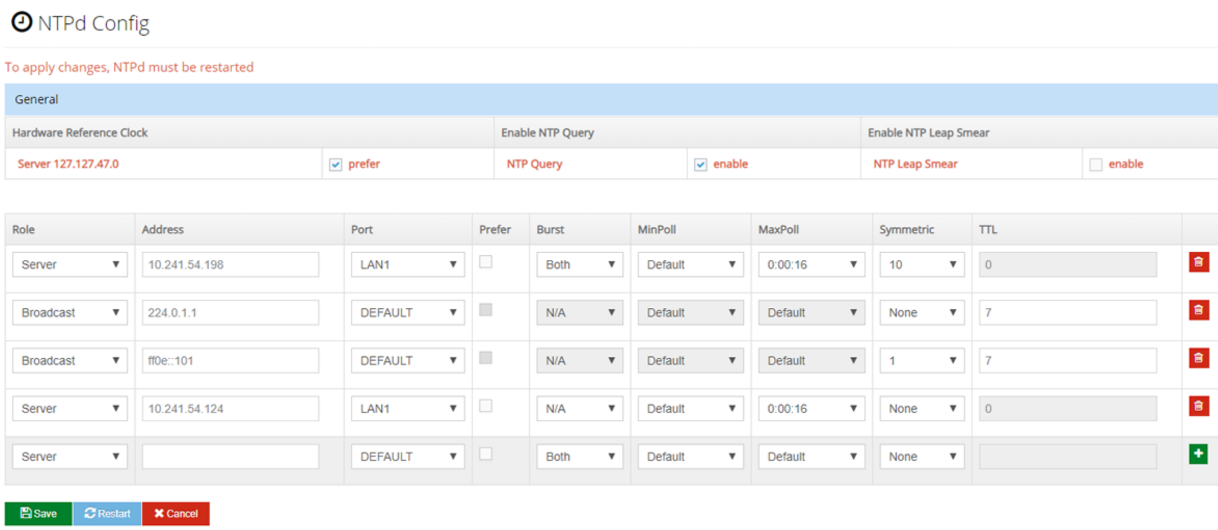
Parameter	Description
Reach	This is an 8-bit shift register that keeps track of the last 8 attempts to reach the remote end of the association. New bits are added to the rightmost end of the register (1 for reached or 0 for unreached) and old bits “fall off” the left hand side. The shift register is represented in octal. For example, by converting “377” from octal to binary, one gets “11111111”, indicating 8 successful polls. For a sequence of eight successful polling attempts on a new association, the octal value of Reach increases as follows: 1, 3, 7, 17, 37, 77, 177, 377. If the value isn't one of those just shown, there may be a problem polling the remote end of the association. If the value remains at 0, or decreases to 0, the association is becoming unreachable. The reach value stays 0 if the SyncServer is a broadcast or multicast server.
Offset (ms)	The time offset between the SyncServer and the remote server, in seconds, of the last poll. The NTP daemon's clock selection algorithm gives preference to lower Offset values. The Offset for the Hardware Clock is usually in the microsecond range. For external NTP associations, the offset is affected by the time base of the remote node and the characteristics of the network path, with values typically in the 1 - 10 millisecond range.
Delay (ms)	The total delay, in seconds, of the round trip to the remote end of the NTP association. For example, a value of “0.07817” equals approximately 78 milliseconds. The Delay for the Hardware Clock is “0”. For most NTP associations, typical values range from tens to hundreds of milliseconds. The NTP daemon's clock selection algorithm gives preference to lower Delay values.
Disp (ms)	Dispersion represents the maximum error of the SyncServer relative to the NTP association.There are two components in dispersion, those determined by the peer relative to the primary reference source of standard time and those measured by the SyncServer relative to the peer. They provide not only precision measurements of offset and delay, but also definitive maximum error bounds, so that the SyncServer can determine not only the time, but the quality of the time as well.
Poll (s)	The length of the interval (in seconds) with which the SyncServer polls the remote server, usually starting at 64 seconds and gradually increasing to 1024 seconds. Valid values range from 16 to 65535, increasing by powers of 2. The polling interval for the Hardware Clock is fixed at 16 seconds. The user-configured Minimum and Maximum Poll Interval settings on the NTP - Config page limit this interval.

5.3.2.3 NTP Configuration Window

Use this window to configure NTP parameters, including the Role (Server, Peer, or Broadcast), Address, and Port.

See the following image. See the following table for descriptions of NTP Configuration parameters.

Figure 5-20. NTP Configuration Window



Click the Save button after making changes to save the changes. Click the Restart button to apply the changes.

NTP Query Parameter: If the NTP Query checkbox is enabled, then the SyncServer will respond to queries sent to it from ntpq. Ntpq is used to query the state of an NTP server.

NTP UTC Leap Second Smear: If the NTP Leap Smear checkbox is checked, then the SyncServer will implement a UTC leap second smear function at any forthcoming UTC leap second event. The unit will smear the NTP time stamps for the 24-hour interval before the leap second event. The operation is as defined in the NTPd reference implementation. This functionality is supported as a master NTP clock and will only affect the NTP responses for NTPd and NTP Reflector operations. It will not affect any other time-of-day functions such as IRIG outputs, etc. Behavior of the system is not defined if the system is an NTP client to an NTP server that is smearing.

Table 5-7. NTPd Association Configuration Parameters

Parameter	Description
Role	Server Creates a persistent association between the SyncServer (client) and an NTP node (server). The client synchronizes with the server if the client's clock selection algorithm selects this server as the best clock. Typical server associations include: the hardware clock, the factory default NTP servers, and servers added by the user. The user creates a Server association to designate an NTP node that has an NTP Stratum better or equal to that of the SyncServer (client). Often, the NTP server is another Stratum 1 server with a GPS reference that is outside the user's administrative jurisdiction.
	Peer Creates a persistent symmetric-active association between the SyncServer (peer1) with an NTP node (peer2). For the NTP node running in symmetric-passive mode, there is nothing needs to be done on the NTP node. However, the NTP node can be configured in symmetric active mode too. When configured, the two nodes can synchronize with each other in a variety of failure scenarios, such as loss of GPS and Internet connectivity. The user configures NTP associations on two NTP nodes that point to the each other. The two nodes are usually of equal stratum and have independent references, such as two separate GPS installations or two separate network paths to NTP servers on the Internet. In the event of a reference failure, the peerscan synchronize to the node that has the best remaining reference.
	Broadcast Creates a broadcast server association. When configured with a broadcast address (e.g., 192.168.61.255), the association broadcasts NTP messages from the network interface with the matching IP address (e.g., 192.168.61.58). Broadcast messages go out to all nodes on the subnet, and are usually blocked by routers from reaching adjacent subnets. Consult with the network administrator to select a correctly-scoped address and Time-to-Live (TTL) value. Typical Usage: Broadcast associations to reduce network traffic with a large number of NTP clients. **Note:** Do not peer to an NTP server on an Ethernet port that is configured for a non-NTPd timing service, such as PTP GM or NTP reflector.
Address	The IP address or DNS name of the NTP association.
Port	With the default setting, the NTP daemon automatically detects and uses a valid network port to communicate with configured NTP server(s). Depending on the IP routing infrastructure, this is typically LAN1. The user can override this by selecting a specific network port. If so, the address must be specified using an IP address instead of a DNS name. The Port setting is only available for Server, Peer, Broadcast, and Multicast associations. (Factory Default = “Default”)

...........continued

Parameter	Description
Prefer	The NTP daemon will synchronize with an association marked prefer over an equivalent association that is not. The internal hardware reference clock prefer setting can be cleared in order to allow an external NTP server to be preferred over the internal hardware reference clock. By default the SyncServer S600 Series has the NTP Prefer selected for the local hardware reference clock. In most operating scenarios the local hardware reference clock (which more often than not will be tracking GNSS) will be the only reference being used. With the Prefer being selected, and no statistically better reference available, the time server will achieve Stratum 1 status on startup or restart as rapidly as possible. If the Prefer is not selected for the hardware reference clock then the NTP daemon will go through a standard validation procedure for a reference clock. This procedure will take several minutes and should happen by the time the reach indicates 377 on the reference clock association. For optimal operation, Microchip recommends the local hardware reference remain selected as a Prefer in the configuration.
Burst	Burst When the server is reachable, send a burst of eight packets instead of the usual one. The packet spacing is about two seconds. This is designed to improve timekeeping quality for server associations. This setting should only be used in agreement with the administrator of the remote NTP device as the traffic load may be onerous.
	iBurst When the server is unreachable, send a burst of eight packets instead of the usual one. As long as the server is unreachable, the packet spacing is about 16s to allow a modem call to complete. Once the server is reachable, the packet spacing is about two seconds. This is designed to speed the initial synchronization acquisition with the server command.
MinPoll	This option specifies the minimum poll interval for NTP messages, in seconds to the power of two. The minimum poll interval defaults to 6 (64 s), but can be decreased to a lower limit of 4 (16 s).
MaxPoll	This option specifies the maximum poll interval for NTP messages, in seconds to the power of two. The maximum poll interval defaults to 10 (1,024 s), but can be increased to an upper limit of 17 (36.4 h).
Symmetric	This option specifies an optional MD5 or SHA symmetric key ID. The MD5 key should be 20 characters. The SHA key should be 40 hex characters.
TTL	This field is used to specify the TTL in the IP header for broadcast packets. This will control the number of hops that the packet can be sent.

After changing the NTP configuration, click the save button and then the RESTART button to put the new configuration into effect. While the NTP daemon restarts, its services are temporarily unavailable, and it generates the following alarm events: NTP Stratum Change, NTP System Peer Change, NTP Leap Change.

The SyncServer S6x0 supports both broadcast and multicast.

- For broadcast, the IP address is the local subnet broadcast address.
- For multicast, the IP address is an IPv4 or IPv6 multicast address. This can beeither the IANA designated NTP multicast address (224.0.1.1 IPv4 or FF0X:0:0:0:0:0:0:101 IPv6) or any unassigned multicast address (typically in the range 224.0.1.0 to 238.255.255.255 for IPv4 or FF0X:x:x:x:x:x:x:x for IPv6).
- You can configure multiple multicast addresses but only one broadcast address on a SyncServer S6x0.
- SyncServer S6x0 does NOT support broadcast and multicast with Autokey.

The TTL used for multicast is in the range: [1, 7].

5.3.2.4 NTPd Most Recently Used (MRU) List Window

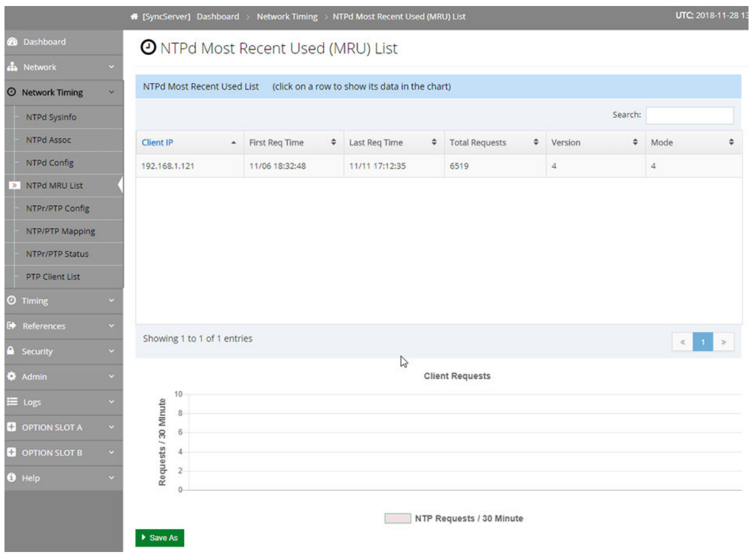
Use this window to display a list of the most recently used clients.See the following image.

The data displayed includes the following:

- Client IP
- First Request Time
- Last Request Time
- Total Requests
- Version of NTP
- Mode of NTP

This window also displays a graph of Client Requests / 30 minutes. There is a separate bar for each 30-minute interval, and the graph will display data for up to the last 24 hours.

Figure 5-21. NTP MRU List Window



5.3.2.5 NTP / PTP Services Configuration Window

Use this window to configure NTP reflector and PTP services. See the following image.

This page can be used to configure multiple NTPr and PTP configurations. However, only one timing service can be mapped to each port.

Figure 5-22. NTP / PTP Service Configuration Window

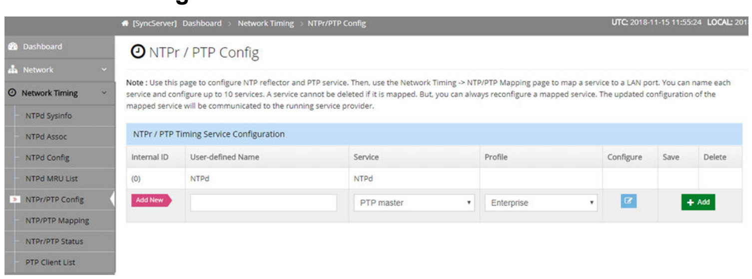


Table 5-8. NTP / PTP Services Configuration Parameters

Parameter / Column	Description
Internal ID	The S6x0 automatically assigns this number as a unique identifier to reference this specific timing service when it appears on other forms. The assigned values will not necessarily be consecutive.

...........continued

Parameter / Column	Description
User-defined Name	Use this entry to provide a helpful name to describe the specific service. Maximum number of characters in the name is 47. Although probably not a good idea, multiple rows can have the same entry. The internal ID assures that they are always unique.
Service	This selection provides a top-level control for the type of network timing service being defined. The drop-down list provides all candidates. The selections are NTPr (NTP reflector), PTP client and PTP master. See note below about NTPd **Note**: These columns are context-aware based on the current Service column selection. Configure column may be additionally context-aware based on the selected Profile. Hence the best way to work with these 3 columns (Service, Profile, Configure) is left-to-right.
Profile	When appropriate, this column is used to further refine the categorization of the timing service. A good example is a PTP master (top-level service), which always operates with a specific PTP profile.
Configure	For a timing service that has additional configuration parameters, this selection brings up a form where all remaining parameters can set as desired. Selecting OK on the configure form maintains this configuration as long as the associated timing service row is being worked on. When (if) the Save selection in that row is executed, then the configuration becomes part of that service.
Save	Use this to save the timing service configured on this row. This also saves the settings (if any) that are associated with Configure for this same row.
Delete	Remove the specific timing service configuration associated with this row. If the row being deleted is currently mapped for use on a physical port, this action will not be allowed. If you really want to do it, first unmap it on the Network Timing'NTP/PTP Mapping form.

IEEE 1588 2.1 should only be configured for the PTP master configuration when using with a 1588 2.1 client.

Reflector capability is only available when the existing Security License option is installed. PTP is only available with the appropriate PTP license option.

The reflector does not support symmetric security keys or Autokey.

The timing service will only support one IP address. When using IPv6, there could be multiple IPv6 addresses associated with the Ethernet port. The IPv6 address can be selected by the user or automatically selected by the system in the following order.

1. Configured static IPv6
2. First available global address - DHCP or autoconfig
3. Link-local

The unit will not respond to IPv4 NTP packets if the reflector is enabled for IPv6. The unit will not respond to IPv6 NTP packets if the reflector is enabled for IPv4.

The SyncServer S6x0 Series implements real-time, hardware-based network packet processing in tandem with accurate hardware based NTP/PTP time stamping, general packet limiting and alarming. The reflector protects the SyncServer CPU from excessive network traffic Denial of Service (DoS) attacks, while concurrently providing high-bandwidth, high-accuracy NTP/PTP operations.

The system uses a real-time, hardware-based NTP/PTP packet identification and time-stamping engine. The high capacity hardware uses the extremely accurate S6x0 Series clock to deliver the best possible NTP/PTP timestamps. At line speed, NTP/PTP client packets are identified, the precise and accurate time stamps are added and the packets returned to the requesting NTP/PTP client, while also bandwidth-limiting all other packets to the CPU. Since all operations are in hardware operating at 1GbE or 10 GbE line speed the packet capacity is in excess of 360,000 packets per second.

The NTP Reflector supports the most common NTP Mode 3 NTP client requests for time. The NTP daemon running on the embedded CPU on the other hand is capable of more NTP features and functions. The advantage of the SyncServer S6x0 Series is that it can simultaneously perform NTP reflector operations on one user-selectable port while conducting traditional NTP Daemon operations on the other ports. This provides the best of both NTP operational models including common NTP daemon functions, such as peering, clustering, selection, MD5 and Autokey authentication. The primary trade-offs are shown in Table 4-9.

Figure 5-23. NTP Packet Reflector

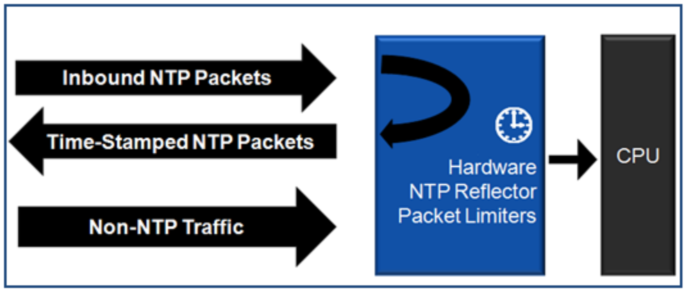


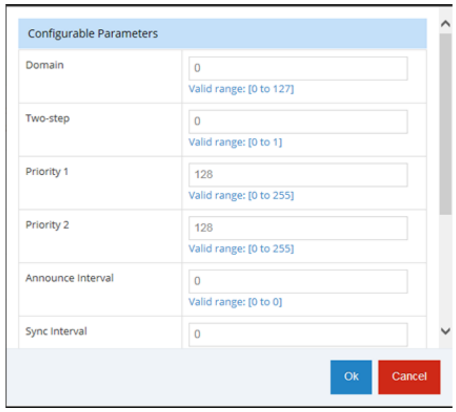
Table 5-9. NTP Reflector vs. NTP Daemon Performance Trade-Offs

Feature	NTP Reflector	NTP Daemon
Enhanced Security	X	
360,000 NTP requests/second	X	
Enhanced Time Stamp Accuracy	X	
DoS Detection/Alarming	X	
CPU Protection	X	
NTP Peering, Clustering, Selection		X
MD5 and Autokey Functions		X

It is important to note that NTP is UDP/IP and is by nature susceptible to DoS attacks as no TCP/IP connection is required. The Security-Hardening of the line speed NTP Reflector is such that in the event of an NTP DoS attack the NTP packets will not reach the CPU and compromise the server operation. Instead, all NTP packets can be responded to (or limited) and if the NTP load is in excess of what is expected an alarm is sent notifying the user. The alarm threshold can be set on the packet monitoring page, which is part of the Security section tab..

When changing the configuration between IPv4 and IPv6, the reflector will be disabled for up to 15 seconds. During this time, the traffic will be forwarded to the CPU. If the traffic rate exceeds the all-packets threshold, then the traffic will be dropped and an alarm generated.

Figure 5-24. PTP Configuration Parameters



For a list of PTP parameters, including default value and range, see Table 9-43 through Table 9-55 in Chapter 9.

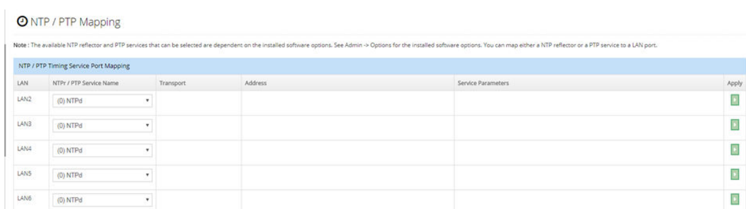
5.3.2.6 NTP / PTP Mapping Window

Use this window to map either a NTP reflector or a PTP service to a LAN port. See the following image. A license is required for all timing services, other than NTPd. NTP reflector requires security license. PTP input requires PTP input license. PTP master requires PTP master license.

The NTP Reflector and PTP capability is supported on the LAN2, LAN3, LAN4, LAN5, and LAN6 ports, but it is not supported on LAN1.

GNSS must be configured, enabled, and connected if the “Auto-Asymmetry Correction” is enabled for the PTP client. The asymmetry correction feature allows the system to learn and correct for asymmetry in the network between the PTP master and the PTP client in the SyncServer. If asymmetry correction is enabled without GPS, then the PTP client will only be used to adjust the system frequency and won't adjust the system time. Calibration will take at least one hour and up to two hours.

Figure 5-25. NTP / PTP Mapping Window

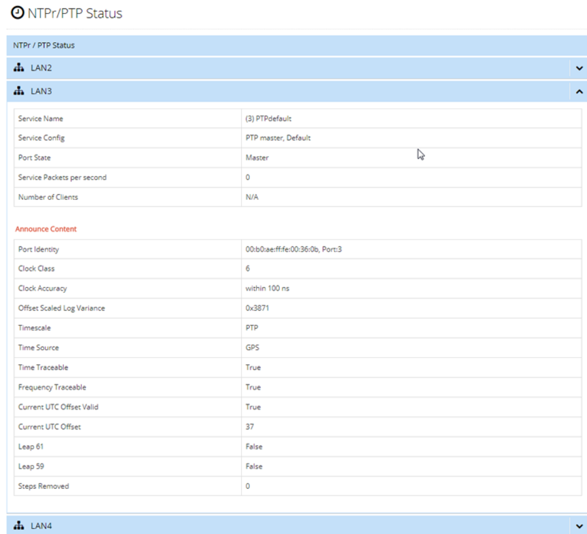


5.3.2.7 NTPr / PTP Status Window

Use this window to view status of ports with NTP reflector or PTP service. See the following images.

Figure 5-26. NTPr / PTP Status Window

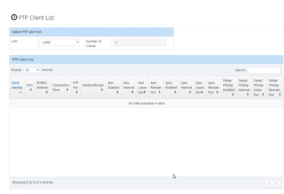
Figure 5-27. NTPr/PTP Status Window - Port Details



5.3.2.8 PTP Client List Window

Use this window to display a list of PTP clients and client details. See the following image. The PTP client list is useful for initial PTP network setup, to assure expected PTP clients are connected to expected SyncServer LAN port(s). and to check PTP client settings from one location. The PTP client list is not available for the Enterprise profile in multicast mode.

Figure 5-28. PTP Client List Window



Client details displayed include the following:

- Clock Identity
- Port
- IP/MAC Address
- Connection Time
- PTP Version
- Vendor/Router
- Announce Enabled
- Announce Interval
- Announce Lease Duration
- Announce Duration Remaining
- Sync Enabled
- Sync Interval
- Sync Lease Duration
- Sync Duration Remaining
- Delay/PDelay Enabled
- Delay/PDelay Interval
- Delay/PDelay Lease Duration
- Delay/PDelay Duration Remaining

5.3.3 Timing Configuration Windows

The Timing tab on the dashboard provides access to windows to enable time and holdover sources, manually set time, set the time zone, and to configure format of the serial output.

Note: The SyncServer 6x0 does not contain a battery-backed real time clock. Therefore, it will always boot up with a default value for the system time. This time will be updated when it obtains time from a time reference such as GNSS, IRIG, or NTP. The default value for the date is the software build date. This date will be used for the first log entries when booting up the unit. The time will change to local time during the boot-up process if a time zone has been configured.

The system will monitor all inputs and determine if there is a valid signal on each input. The system only uses one reference at a time. The highest priority valid input will be used. This is specified on the Timing->Input Control page. Each reference has a different priority - the slot A and slot B references will have different priorities. With release 2.1, the priorities can be changed. All releases allow individual input references to be enabled/disabled. A frequency reference is only used if there are no valid timing references.

5.3.3.1 Timing - Input Control Window

Use this window to enable external time and frequency references, and manually set the time when no external time reference will be supplied. There are special limitations associated with this mode of operation, as described on the form itself. If “Ignore UTC corrections” is enabled, then local time is not available on the front panel or the web page.

Use this window to manually set the IRIG input year, UTC offset from TAI, and Leap Second Notification. See Provisioning Inputs with Manual Entry Controls for details.

When using the forced manual time entry mode, the unit should not have NTP configured as an input reference. Therefore, no NTP devices should configured on the NTP config page if using this mode.

Note: If “Forced Manual Time Entry” is selected on the Input Control form (while Time of Day status = Freerun), or if time is set from front-panel, the unit may not lock to GNSS upon return to the “External Time Sources” setting on the Input Control form.
The workaround for this is to disable GNSS (and apply) after setting the unit to “External Time Sources”. Then enable GNSS again (and apply).

It is recommended that the SyncServer S6x0 be rebooted when leaving manual time mode.

See the following images.

Figure 5-29. Timing - Input Control Window - Upper Portion

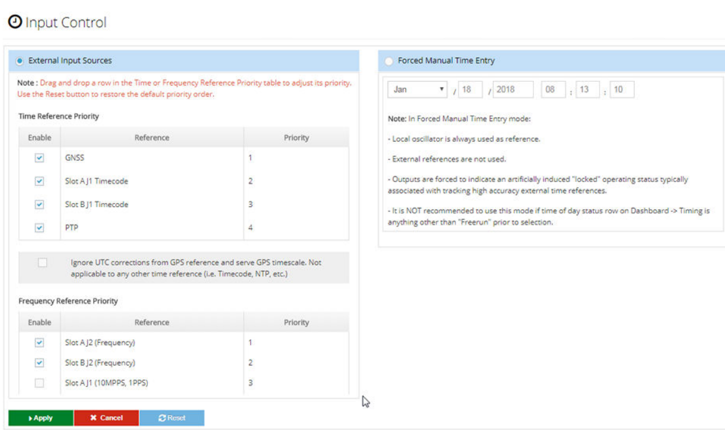
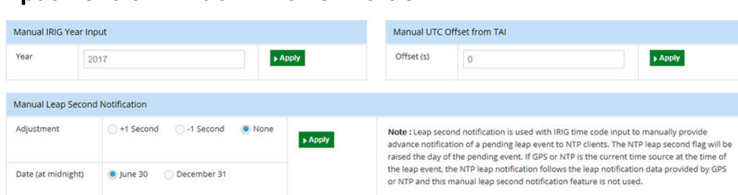


Figure 5-30. Timing - Input Control Window - Lower Portion

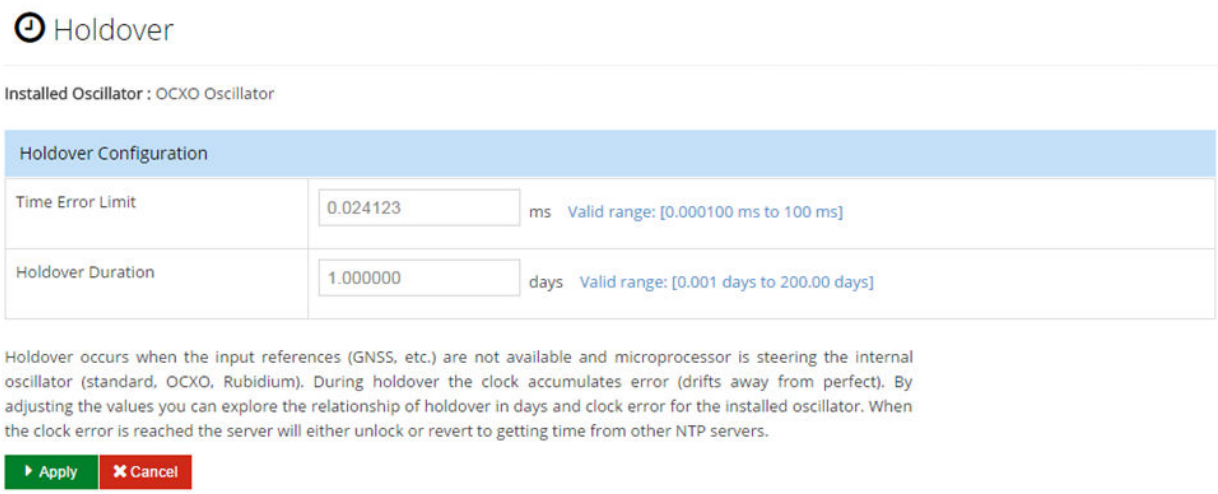


5.3.3.2 Timing - Holdover Configuration Window

Use this window to configure a duration in holdover (loss of stratum 0 reference) until the server either unlocks or attempts to get time from other NTP servers (if configured to do so). After this holdover period is exceeded, then the unit will attempt to lock to external NTP servers.

See the following image.

Figure 5-31. Timing - Holdover Window

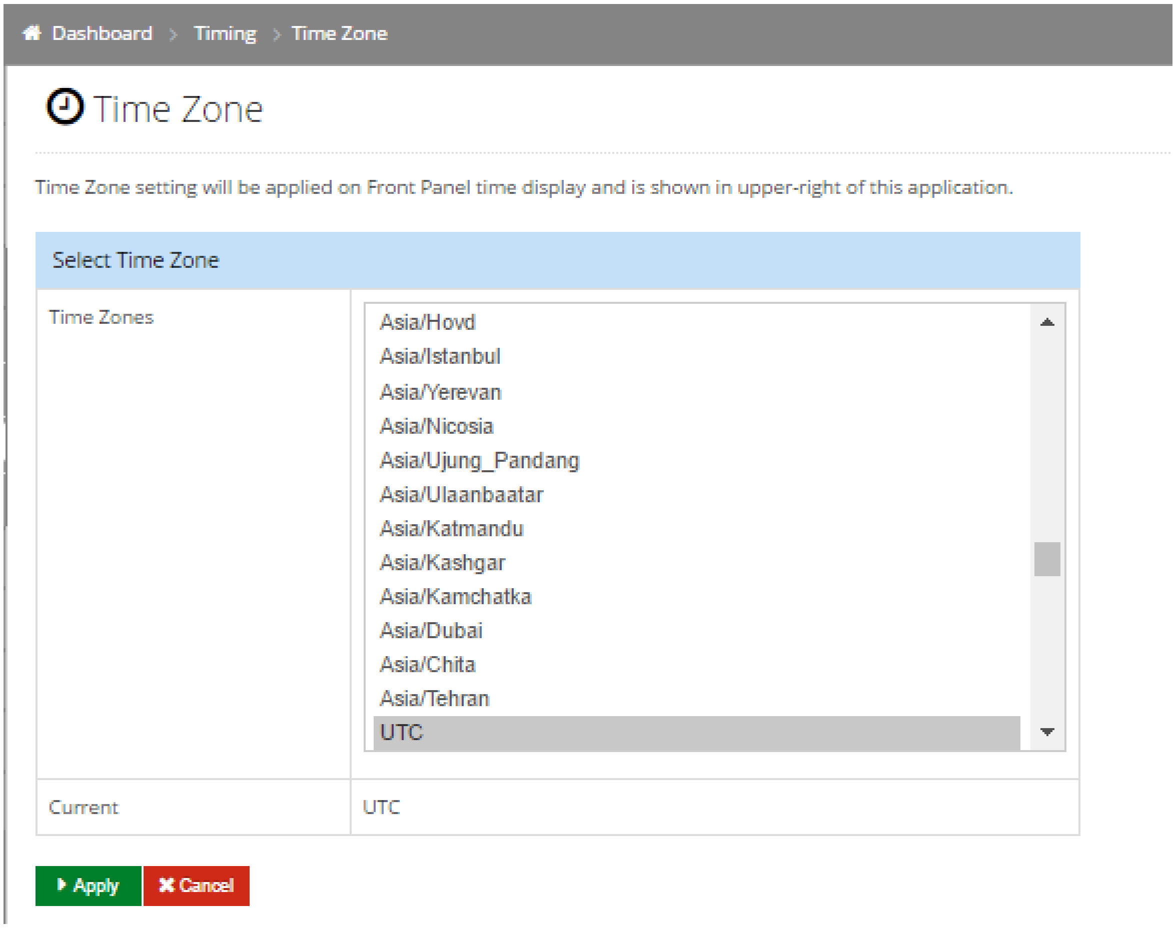


Holdover occurs when the input references (GNSS, etc.) are not available and microprocessor is steering the internal oscillator (standard, OCXO, Rubidium). During holdover the clock accumulates error (drifts away from perfect). By adjusting the values you can explore the relationship of holdover in days and clock error for the installed oscillator. When the clock error is reached the server will stop updating the NTP reference time. If other NTP servers are configured, it will then start getting time from other NTP servers. The value obtained with this estimator is a conservative estimate of the performance of the unit. Actual performance may vary and will typically be better than this estimate.

5.3.3.3 Timing - Time Zone Configuration Window

Use this window to select the desired time zone for the SyncServer S6x0. See the following image. The time zone is only for the front panel display. NTP time will continue to be served in UTC.

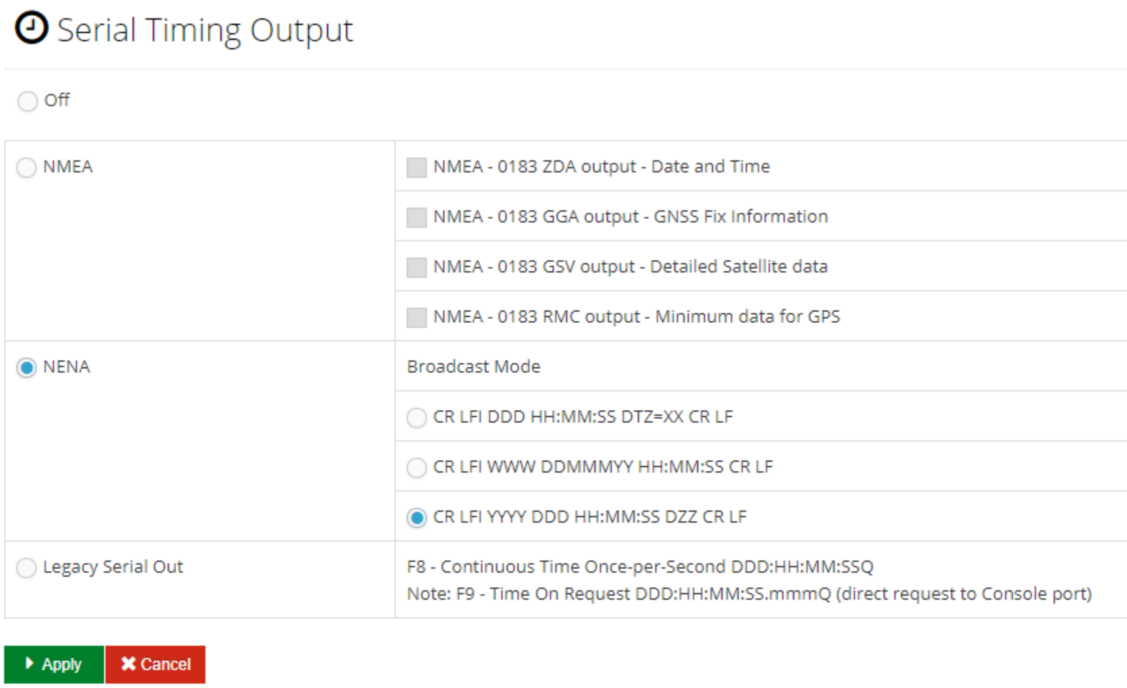
Figure 5-32. Timing - Time Zone Window



5.3.3.4 Timing - Serial Output Configuration Window

This window is used to select the format for the serial timing output for the SyncServer S6x0. See the following image.

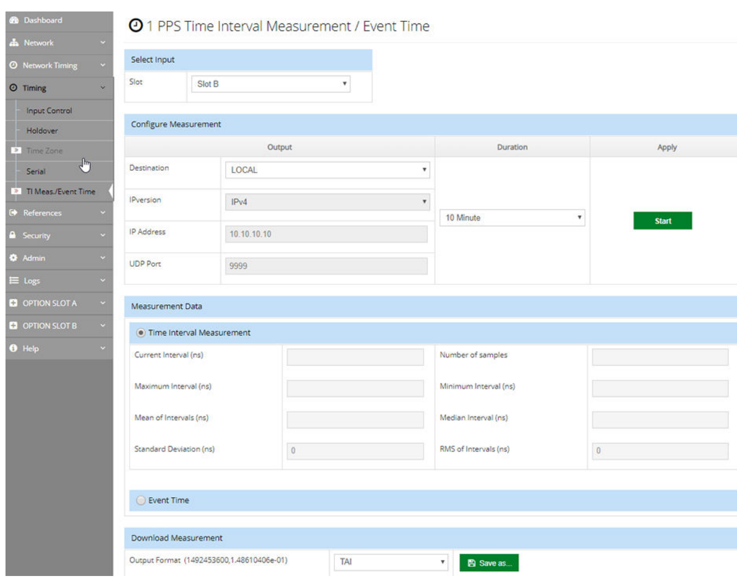
Figure 5-33. Timing - Serial Output Window



5.3.3.5 Timing - 1 PPS Time Interval Measurement / Event Time Window

Use this window to set up 1PPS time interval measurements and event time. See the following image. See Making Time Interval or Event Timestamp Measurements for details on using this feature.

Figure 5-35. 1 PPS Time Interval Measurement / Event Time Window



5.3.3.5.1 Requirements

- Software license
- SyncServer S650 with optional timing I/O module

5.3.3.5.2 Capabilities

- Make measurements on a 1PPS signal connected to J1 port of either module A or module B. Measures the rising edge of the signal compared to the SyncServer system time.

- Calculate statistics and display results - current measurement, number of measurements, maximum, minimum, mean, median, standard deviation, and RMS
- Take measurements and calculate statistics over a user-selected duration from 10 minutes to 24 hours, or continuous. Web interface button to start and stop measurement. Statistics are only available if measurements are stored locally, rather than streamed on an Ethernet port or serial port.
- Store results locally or either send results to IP address with selected UDP port number, or to the timing/event serial port. Time interval results are sent once a second with the UTC time and measurement result. Event timing results are sent as they are obtained. Note that the serial port may limit the rate of measurement results. For example, a baud rate of 9600 may limit results to 25 per second. A program will need to run on the remote computer to collect the data. For example, SocketTest could be used. It is available from https://sourceforge.net/projects/sockettest/
  – Example: 2017-10-30,17:57:35,-1.30000000e-07
- Download locally stored data to a file in either UTC or TAI format. Results can only be downloaded if the measurement was stored locally instead of streaming to serial or Ethernet port.
  – TAI: Each measurement is on a separate line containing the time and the measurement with units of seconds. This download output format lists the time using the TAI timescale and in the UNIX time format, which is the integer number of seconds since January 1, 1970, 00:00:00.

    Example: 1509386292,-1.30000000e-07
  – UTC: Each measurement is on a separate line containing the date/time and the measurement with units of seconds. This download output format lists the time using the UTC timescale in a format of year-month-day, hours:minutes:seconds..

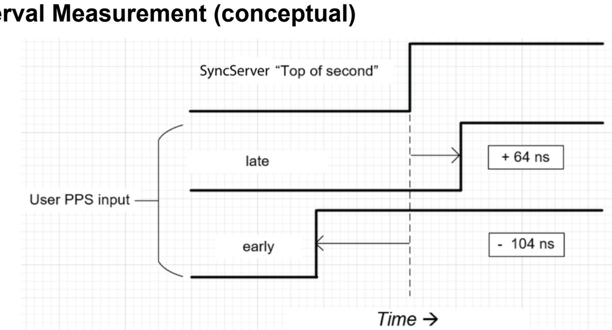
    Example: 2017-10-30,17:57:35,-1.30000000e-07
- Microchip's TimeMonitor Analyzer application can be used to analyze the results. Either download the results, or capture results to a file from the serial port or IP port streams.
  – TimeMonitor Analyzer can load the UTC-format file with "Load Other Data->Load Single/Dual Column File …"
  – TimeMonitor Analyzer can load the GMT-format file with "Load Other Data->Load Date Phase/Freq File …"
    Note: The 1PPS input should be disabled on the Timing->Input control page. The measurement is not useful if the SyncServer is using the 1PPS as the reference.

    Note: Measurements are not useful if the SyncServer system clock has not been set or is changing. Therefore, it is not recommended to use the measurement feature when the SyncServer is in warmup, free-run, or locking clock states.

    Note: If the user 1PPS input is later than the internal 1PPS, then the measurement will be positive. If the user 1PPS is early, then the measurement result will be negative. See the following image.

    Note: Input LOS alarms could be generated if the input is slower than 1PPS. Microchip recommends disabling the LOS alarm actions on the Admin->Alarms page under this condition.

Figure 5-36. Time-Interval Measurement (conceptual)



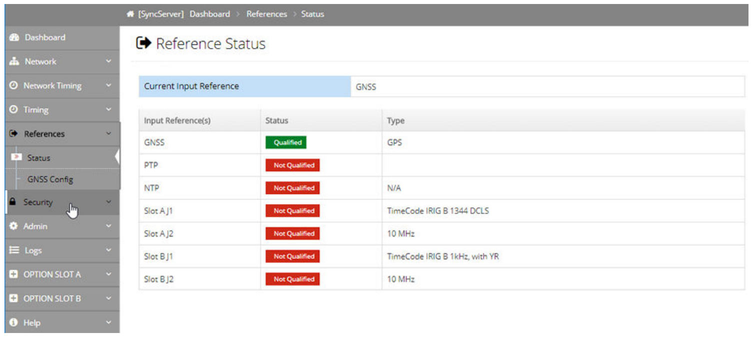
5.3.4 References Configuration Window

The References tab on the dashboard provides access to configure GNSS position and operating mode, as well as view Reference Status.

5.3.4.1 References - Reference Status Window

Use this window to view status information for system References. See the following image.

Figure 5-37. References - Status Window



5.3.4.2 References - Reference GNSS Window

Use this window to configure GNSS position and operating mode. See the following image.

Note: For accurate timing, it is important to accurately enter the delay of the antenna and cable. If the system has already locked to a reference, then it is recommended that the user restart the SyncServer after changing the cable delay. Otherwise, it may take an extended period of time before the change is fully incorporated.

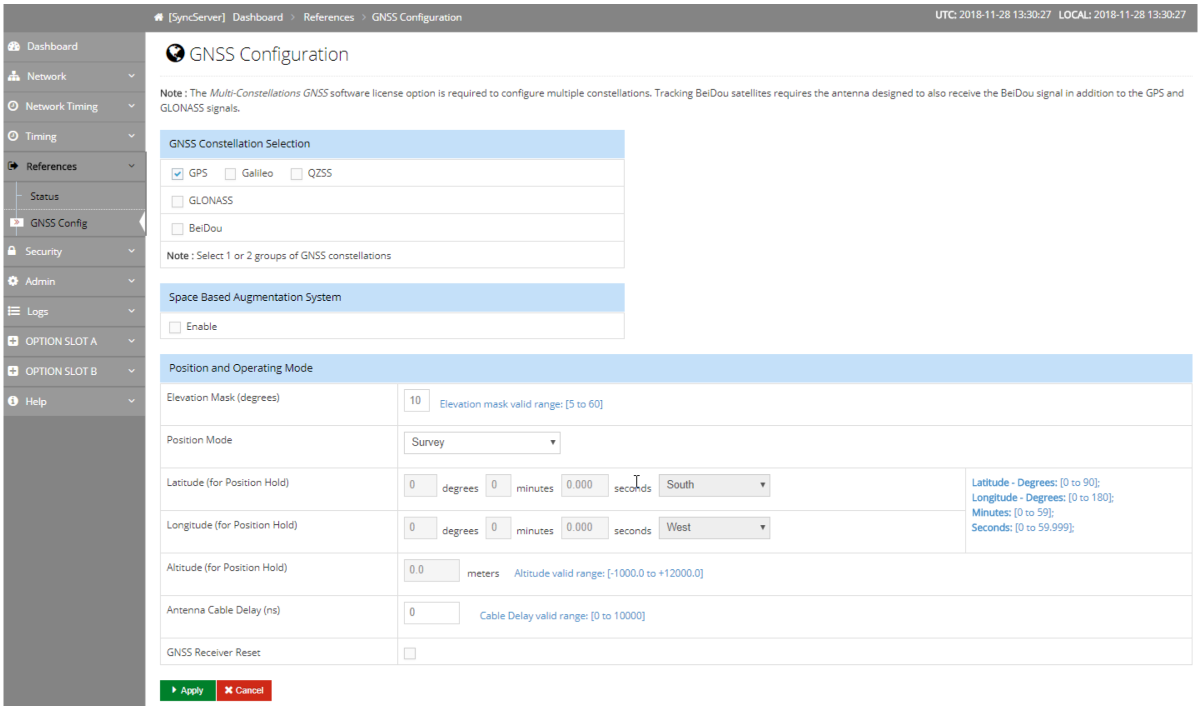
If the GNSS multi-constellation license is installed, then GPS, GLONASS, Galileo, QZSS, and BeiDou can be selected. Only one or two of the constellations groups can be selected. GPS, Galileo, and QZSS are considered part of one constellation group, and can all be selected together as one of the two available constellation groups. It is not possible to select all five constellations.

The Space Based Augmentation System (SBAS) can be enabled.

The Position Mode allows the user to set the position mode to Survey (stationary), Position Hold (stationary), or Dynamic. The default configuration for the SyncServer S6x0 is Survey mode. For stationary applications, Microchip recommends using the Survey mode to avoid timing errors introduced by manually entering an inaccurate position.

- Survey means the SyncServer S6x0 will automatically survey the position and then transition to using this position value. This is meant for stationary applications.
- Position Hold allows the user to manually enter the position for a stationary application. The user enters the Latitude, Longitude and Altitude values for the SyncServer S6x0. The position needs to be accurately determined to avoid creating timing errors.
- Dynamic means the SyncServer S6x0 will continuously determine the position for applications where the system is moving. The user can select the dynamic platform model for Automotive, Seaborne, or Airborne. For Automotive, the maximum horizontal velocity is 100 m/sec. For Seaborne, vertical velocity is assumed to be zero, and maximum horizontal velocity is 25 m/sec. For Airborne, maximum horizontal velocity is 500 m/sec and maximum vertical velocity is 100 m/sec. For unpressurized airborne applications, the maximum operational altitude for the product is 25,000 ft (7620 m).

Figure 5-38. References - GNSS Window



Note: The updated GNSS receiver included in hardware released for v3.1 and later, allows for Galileo as a choice for GNSS Constellation Selection. If v3.1 or newer software is installed in an older unit, the Web GUI screen will not display Galileo as a choice.
Check the Help > About window for the System Inventory. The GNSS Receiver line indicates if the GNSS receiver is Galileo capable.

5.3.5 Security Configuration Windows

The Security tab on the dashboard provides access to configure security for Users, Access Control, Services & System Control, HTTPS, SSH, NTPd Symmetric Key, NTPd Autokey Server, NTPd Autokey Client, RADIUS, TACACS+, and LDAP.

5.3.5.1 Security - Users Window

Use this window to add or delete users, and for Password Maintenance. See the image below. All Users and Admin have the same privileges

The top section allows configuration of the password policy. The minimum length and the types of characters (uppercase, lowercase, number, special) that must be in the password can be configured.

Password expiration can be configured -- the number of days to expire and if the expiration feature is enabled/disabled.

Notes: Only alphanumeric characters and underline are allowed for the User name. Alphabetic characters in User names must be lower case.

- abcdefghijklmnopqrstuvwxyz
- 0123456789
- _

Note: The following characters are not allowed for the password:
(', “, <, >, &,), $

> **Note**
> Number of allowed characters:
> - Username: 1-32 characters, must be lowercase.
>   Mixed-case is not supported.
> - Password: 8-64 characters, must contain uppercase, lowercase, numbers, and special characters
> - Recovery question: 1-34 characters
> - Recovery answer: 1-34 characters
> - Email address: 1-34 characters, ”-“ is not allowed in email address
> - SMTP gateway: 1-34 characters

Figure 5-39. Security - Users Configuration Window - Upper Portion

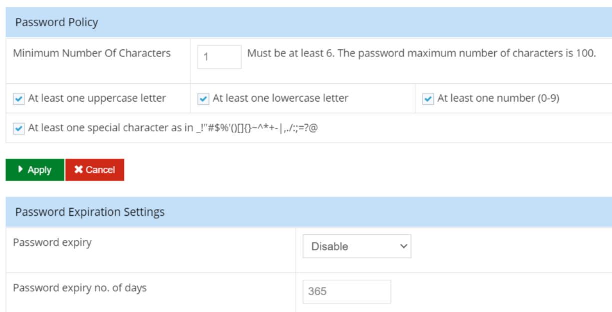
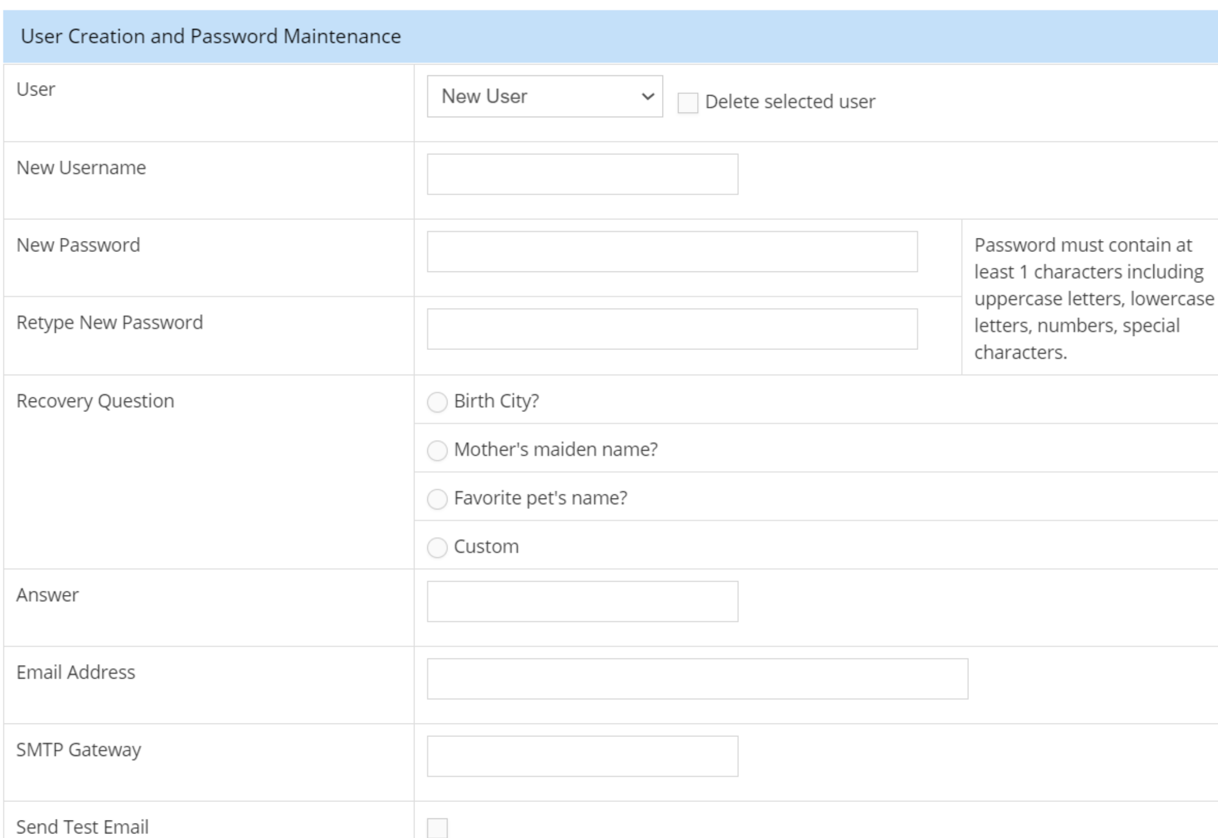


Figure 5-40. Security - Users Configuration Window - Lower Portion

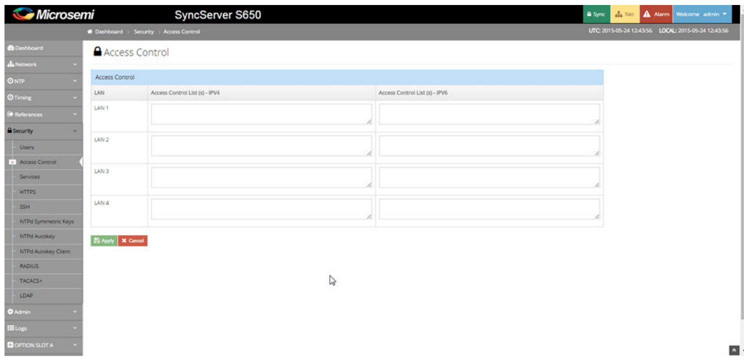


5.3.5.2 Security - Access Control Configuration Window

Use this window to configure access control for LAN1-LAN6 (whitelist). If nothing is configured, then the unit will accept data from all devices. If any addresses are configured, only packets from those devices will be accepted. Each field will support a maximum of 1000 characters. Enter IP addresses separated by a comma. See the image below.

Note: If ACL is configured, then the user must add any desired servers to the list. For example, syslog server, SNMP manager, RADIUS/TACACS+/LDAP servers.

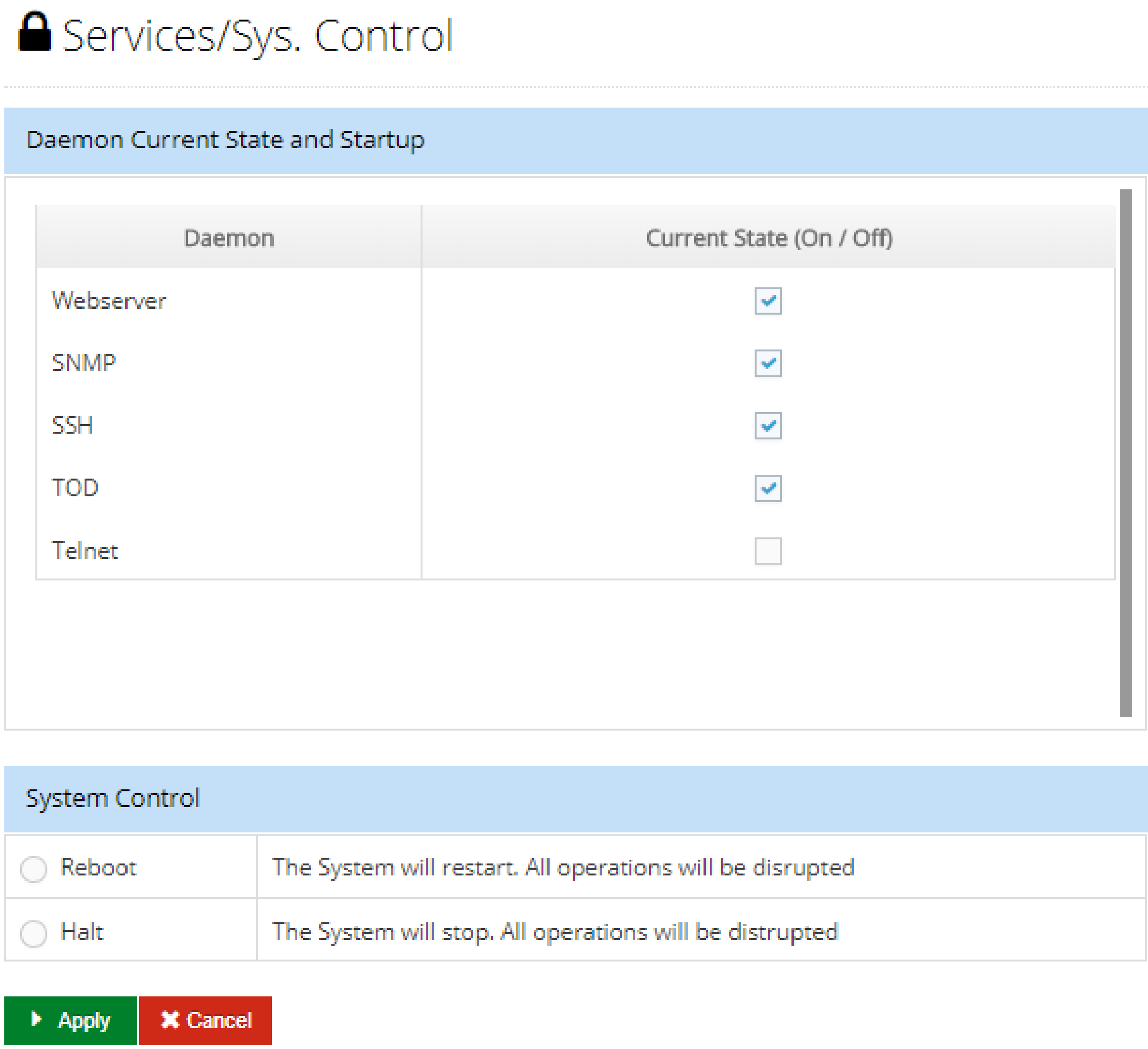
Figure 5-41. Security - Access Control Configuration Window



5.3.5.3 Security - Services & System Control Window

Use this window to configure the state for the Webserver, SNMP, SSH, TOD, and Telnet, and to reboot or halt the system. See the image below.

Figure 5-42. Security - Services & System Control Configuration Window



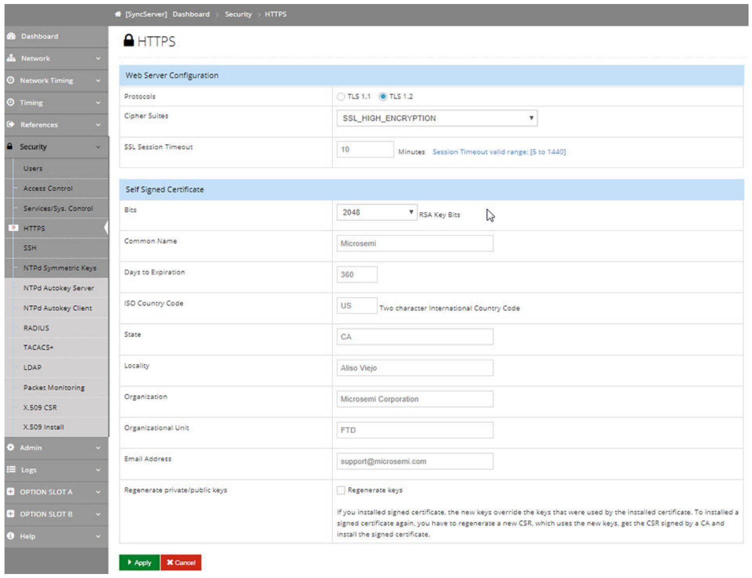
5.3.5.4 Security - HTTPS Configuration Window

Use this window to configure the web server and self-signed certificate info. See the following image.

See the following table for details about supported HTTPS protocols.

	Note Number of allowed characters: • Common name: 1-63 characters • State: 1-63 characters • Locality: 1-63 characters • Organization: 1-63 characters

Figure 5-43. Security - HTTPS Configuration Window



Note: The https certificate will revert to self-signed certificate after importing configuration.

Table 5-10. Supported HTTPS Protocols

Model	TLS 1.0	TLS 1.1	TLS 1.2
SyncServer S600		x	x
SyncServer S650		x	x

Table 5-11. HTTPS Configuration Parameters

Parameter / Column	Description
Protocols	TLS 1.1 or TLS 1.2
Cipher Suites	SSL high or SSL high and medium
Web Session Timeout	Timeout range from 5 to 1440 minutes

Note: The web browser controls which cipher is selected. The browser can be configured to not use undesired/weak ciphers. Also, at each software revision, Microchip will remove ciphers that are deemed to be less secure.

Note: The Internet Explorer 11 web browser does not support TLS 1.1 with SSL high encryption.

Table 5-12. HTTPS Self-Signed Certificate Parameters

Parameter / Column	Description
Bits	Number of bits for RSA key
Common Name	Fully qualified domain name (FQDN) of the SyncServer
Days to Expiration	Number of days before certificate expires
ISO Country Code	Two-character code for country where you are located
State	State where you are located (for example, California)
Locality	City where you are located
Organization	Name of Organization
Organizational Unit	Unit or division of organization (for example, IT Department)

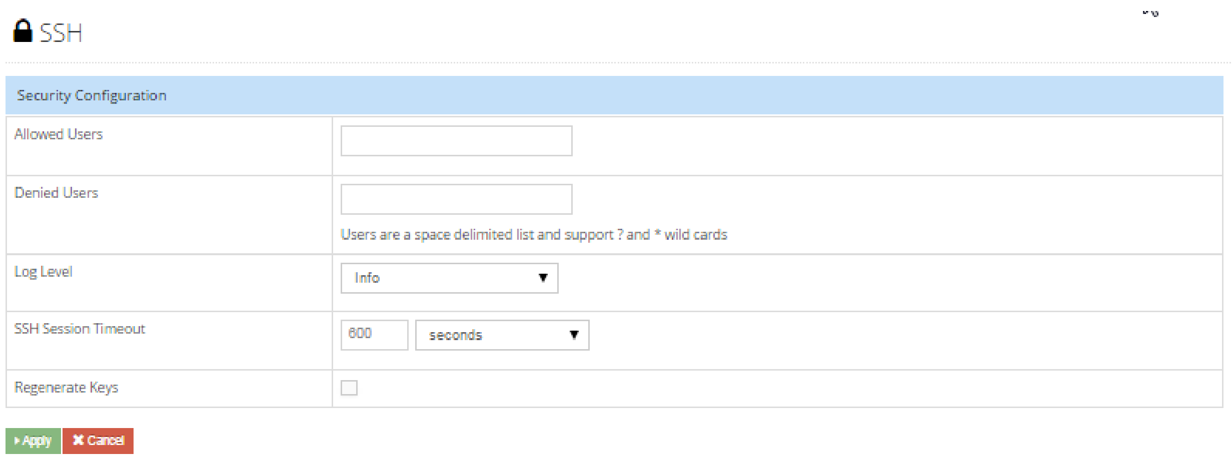
...........continued	
Parameter / Column	**Description**
Email Address	Email address associated with company

Regenerate keys -- check this box to regenerate the public/private keys. Some CSR require new keys for new certificates.
Note: Do not regenerate keys if you are using a signed certificate and you are not planning to get a new certificate.

5.3.5.5 Security - SSH Configuration Window

Use this window to configure SSH security. See the image below. Including the same username in both the allowed and denied lists is not supported.

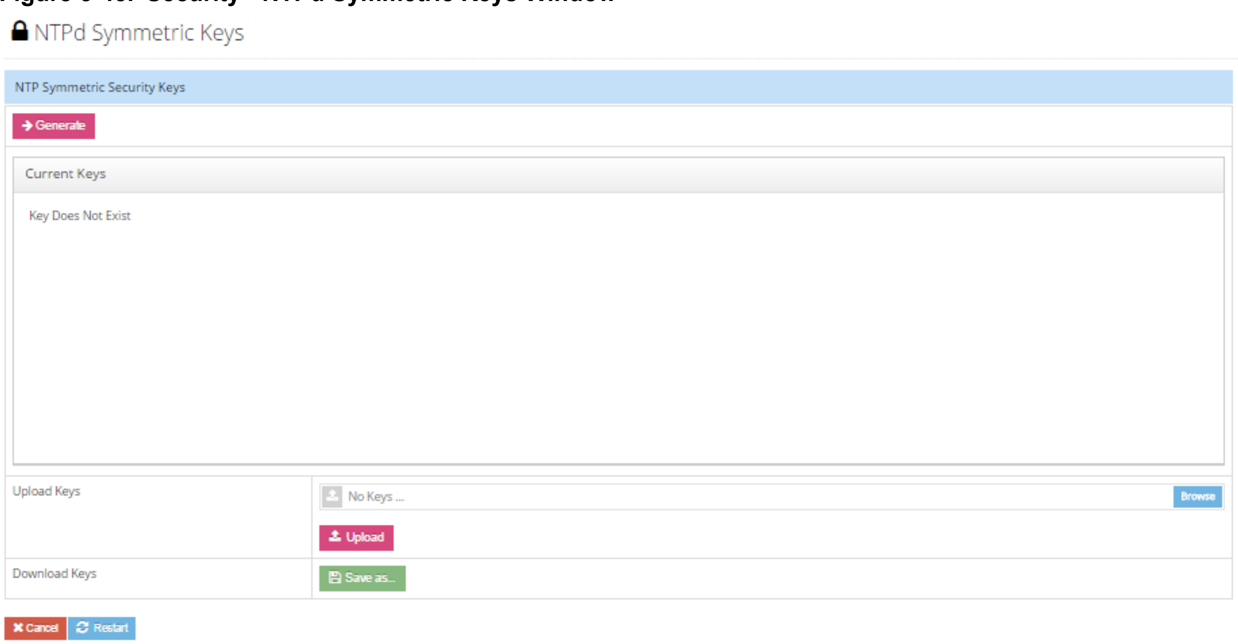
Figure 5-44. Security - SSH Configuration Window



5.3.5.6 Security - NTPd Symmetric Keys Configuration Window

Use this window to generate, upload and download NTP Symmetric Security Keys. See image below. MD5 keys should be 20 characters long. SHA keys should be 40 hex characters.

Figure 5-45. Security - NTPd Symmetric Keys Window

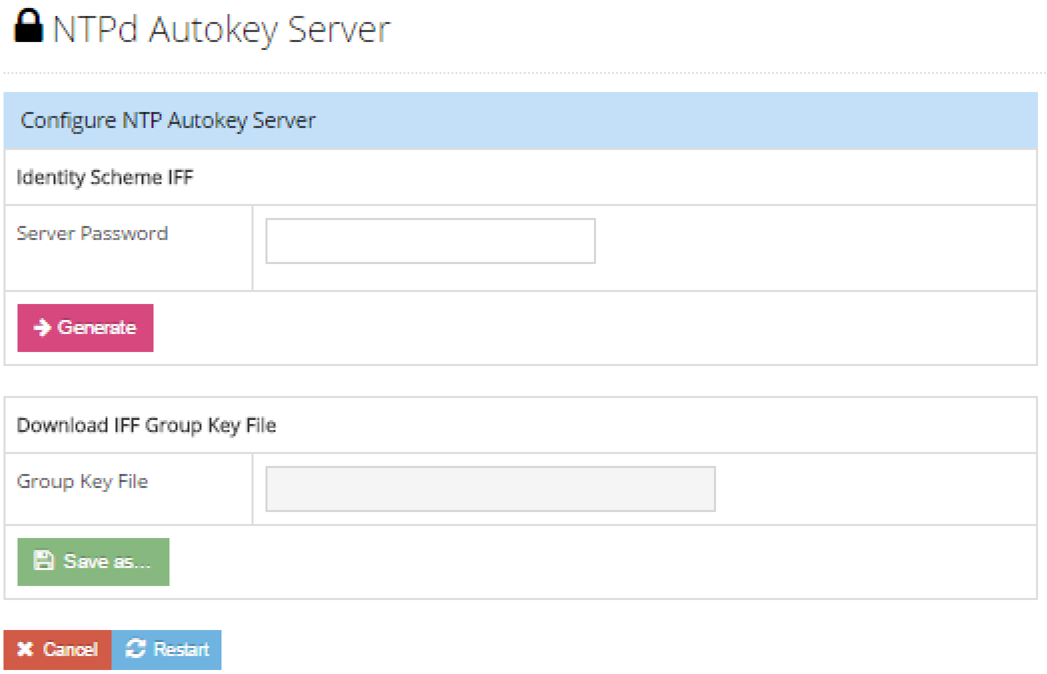


5.3.5.7 Security - NTPd Autokey Server Configuration Window

Use this window to configure the NTP Autokey Server and download the IFF Group Key file. See image below.

Note: Autokey, LDAP, RADIUS, and TACACS+ require the optional security license.

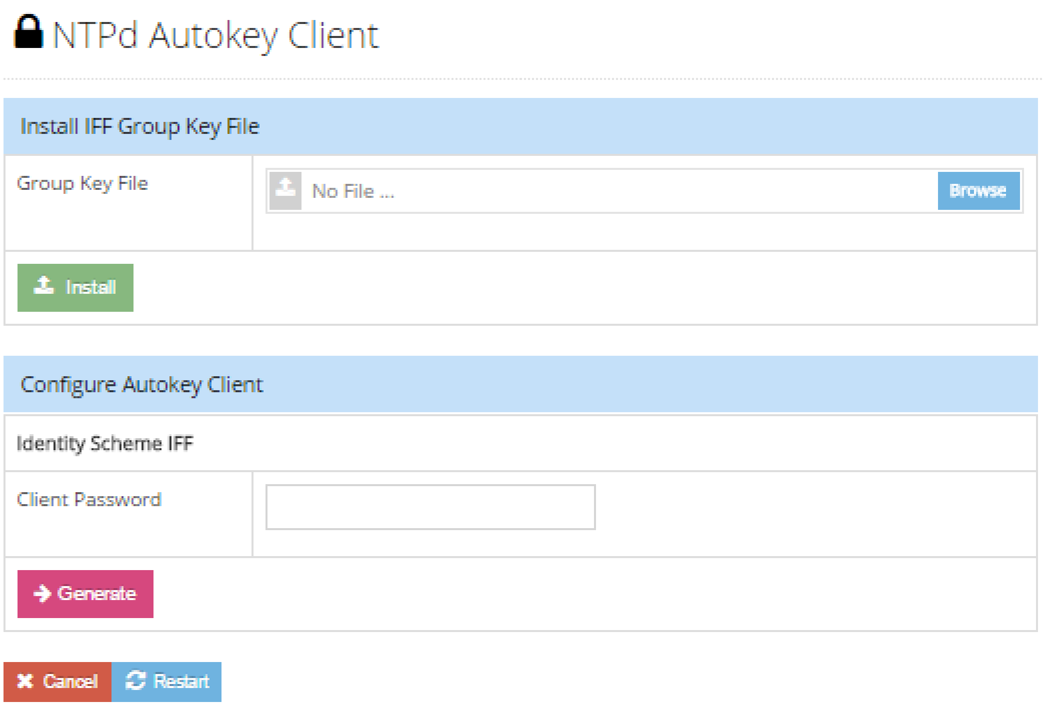
Figure 5-46. Security - NTPd Autokey Server Configuration Window



5.3.5.8 Security - NTPd Autokey Client Configuration Window

Use this window to configure the NTP Autokey Client and install the IFF Group Key file. See image below.

Figure 5-47. Security - NTPd Autokey Client Configuration Window



5.3.5.9 Security - RADIUS Configuration Window

Use this window to enable and configure RADIUS authentication. Up to 5 RADIUS servers can be configured. See image below. After entering the RADIUS information, click the green “+” icon to add the row. Then click the “save” icon to save the information.

The SyncServer S6xx software supports remote authentication using RADIUS, TACACS+ and LDAP servers. The authentication process with multiple remote authentication servers is different among the RADIUS, TACACS+ and LADP servers.

For RADIUS and LDAP, the additional servers are used for “fail over” purpose. They are used only when the prior server in the list is not reachable. The first reachable server is going to authenticate the username and password. The result of the authentication is the result for the entire remote authentication, meaning that it is not going to use the additional servers to authenticate further. If the authentication succeeds, the user is allowed to login to the SyncServer. If the authentication fails, the SyncServer continues its local authentication using the local users list.

Notes:

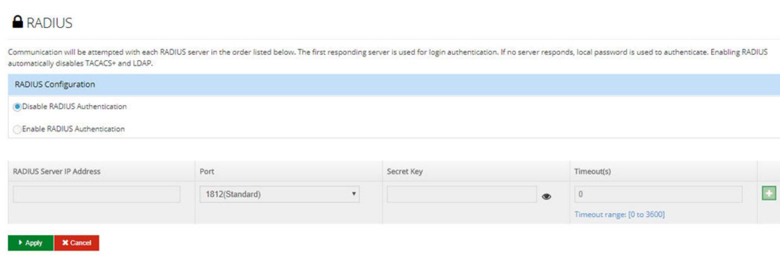
- RADIUS key: 1-16 characters
- Most RADIUS servers do not accept the # and ' characters for the key.

Note: The SyncServer S600/S650 has only one level of management access of Authentication/Authorization and that is full control. There is no read-only management access. Therefore
Authentication = Authorization when there is only one level of management access.

Note: In order to use RADIUS authentication with the SSH login, a local user must be created with the same username as used with RADIUS. This is not necessary for the web login.

Note: RADIUS is designed to be used with LAN1. Do not configure a RADIUS server address in a subnet used by the other LAN ports (LAN2 - LAN6).

Figure 5-48. Security - RADIUS Configuration Window



5.3.5.10 Security - TACACS+ Configuration Window

Use this window to enable and configure TACACS+ authentication. Up to 5 TACACS+ servers can be configured. See image below. After entering the TACACS+ information, click the green “+” icon to add the row. Then click the “save” icon to save the information.

The SyncServer S6xx software supports remote authentication using RADIUS, TACACS+ and LDAP servers. The authentication process with multiple remote authentication servers is different among the RADIUS, TACACS+ and LADP servers.

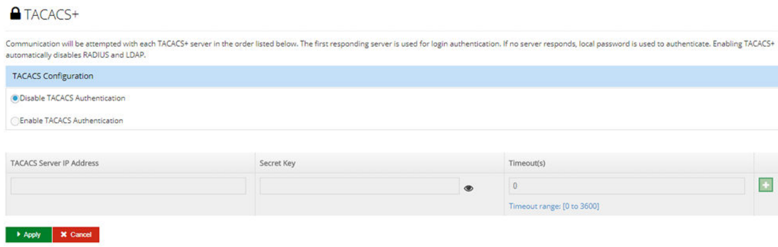
For TACACS+, the additional servers are used for “iterative” purpose. Whenever a server successful authenticates the username and password, it completes the entire remote authentication. Otherwise, the authentication continues with the next configured server. This process goes on until it uses all the authentication servers. The SyncServer local authentication happens last.

Notes:

- TACACS+ key: 1-16 characters
- Most TACACS+ servers do not accept the # and ' characters for the key.

Note: TACACS+ is designed to be used with LAN1. Do not configure a TACACS+ server address in a subnet used by the other LAN ports (LAN2 - LAN6).

Figure 5-49. Security - TACACS+ Configuration Window



Note: The SyncServer S600/S650 has only one level of management access of Authentication/Authorization and that is full control. There is no read-only management access. Therefore Authentication = Authorization when there is only one level of management access.

Note: In order to use TACACS+ authentication with the SSH login, a local user must be created with the same username as used with TACACS+. This is not necessary for the web login.

5.3.5.11 Security - LDAP Configuration Window

Use this window to enable LDAP, and configure LDAP settings and servers. Up to 5 LDAP servers can be configured. See the image below.

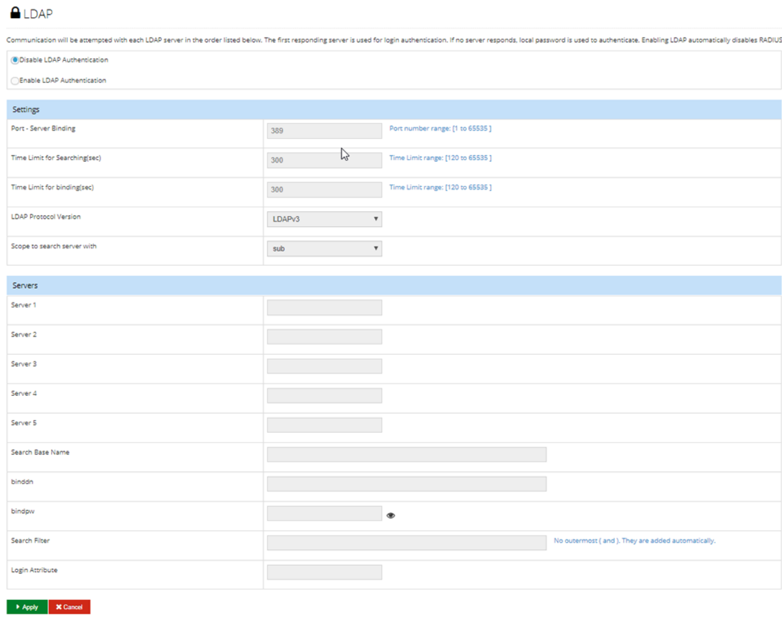
The SyncServer S6xx software supports remote authentication using RADIUS, TACACS+ and LDAP servers. The authentication process with multiple remote authentication servers is different among the RADIUS, TACACS+ and LADP servers.

For RADIUS and LDAP, the additional servers are used for “fail over” purpose. They are used only when the prior server in the list is not reachable. The first reachable server is going to authenticate the username and password. The result of the authentication is the result for the entire remote authentication, meaning that it is not going to use the additional servers to authenticate further. If the authentication succeeds, the user is allowed to login to the SyncServer. If the authentication fails, the SyncServer continues its local authentication using the local users list.

Notes:
- Search base name: 1-199 characters
- binddn: 1-63 characters
- bindpw: 1-63 characters
- Search filter: 1-199 characters
- Login attribute: 1-63 characters
- Most LDAP servers do not accept the # and ' characters for the password.

Note: LDAP is designed to be used with LAN1. Do not configure a LDAP server address in a subnet used by the other LAN ports (LAN2 - LAN6).

Figure 5-50. Security - LDAP Configuration Window



Note: The SyncServer S600/S650 has only one level of management access of Authentication/Authorization and that is full control. There is no read-only management access. Therefore
Authentication = Authorization when there is only one level of management access.

Note: In order to use LDAP authentication with the SSH login, a local user must be created with the same username as used with LDAP. This is not necessary for the web login.

Table 5-13. LDAP Configuration Parameters

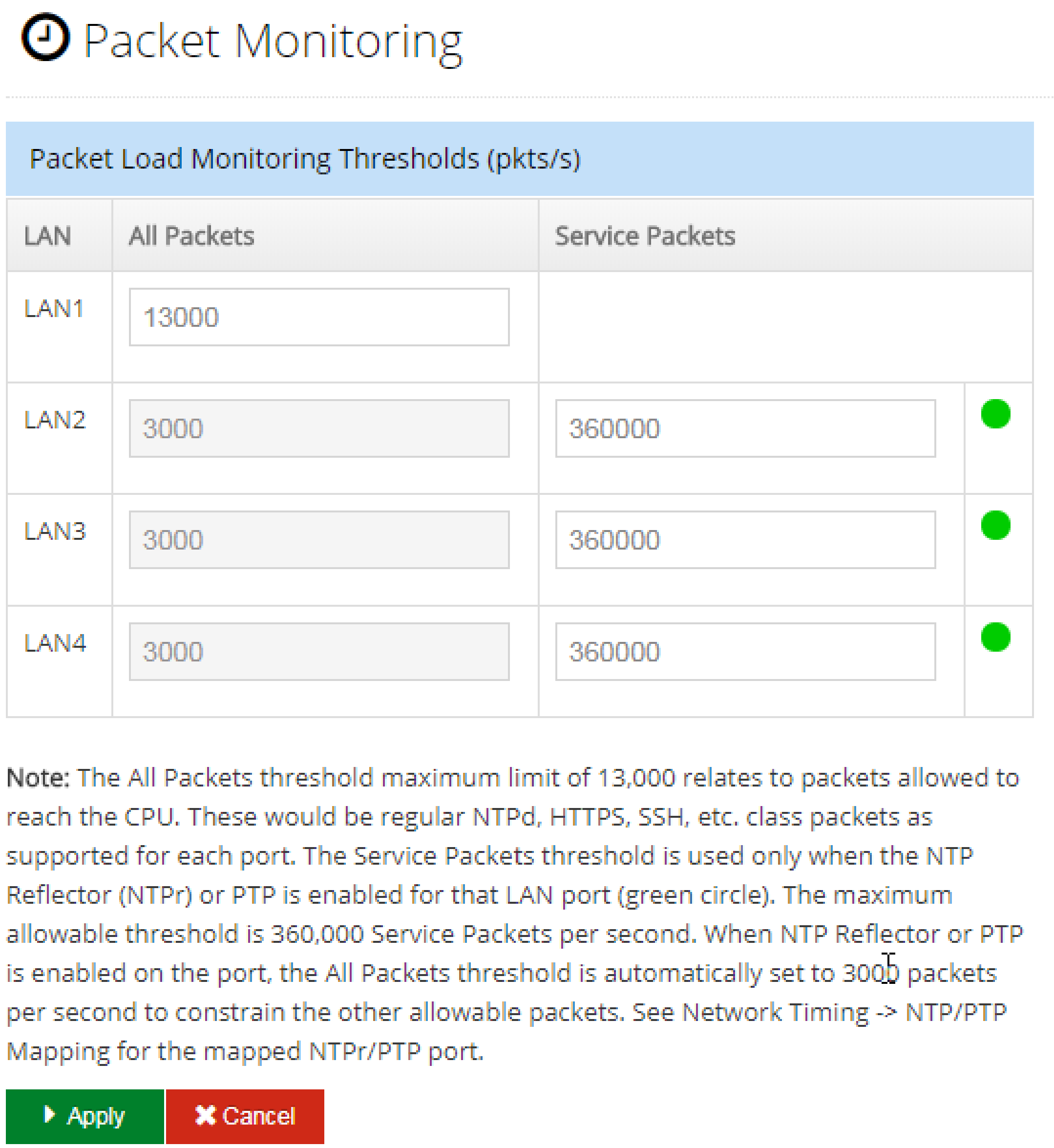
Parameter / Column	Description
Port - Server Binding	IP port for server
Time Limit for Searching	Timeout for searches
Time Limit for binding (sec)	Timeout for binding
LDAP Protocol Version	LDAPv2 or LDAPv3
Scope to search with	• base - limits search to base object • one - limits search to immediate children of base object, but not base object • sub - search base objects and all child objects
Server 1 - 5	Enter up to 5 servers
Search Base Name	Search base
binddn	bind dn
bindpw	bind password
Search Filter	Search filter
Login Attribute	Login attribute
Apply	Use this to apply the LDAP settings configured on this page This also saves the settings that are associated with Configure for this page.
Cancel	Cancel and clear the settings on this page.

5.3.5.12 Security - Packet Monitoring (security license required)

Use this window to configure packet load monitoring thresholds. The All Packets threshold is used to limit the number of packets from each port that are sent to the processor. It will also generate the “Excessive traffic on port” alarm if the threshold is exceeded, and identify the impacted port. Packets that are handled by the NTP reflector or PTP master are not counted toward this limit. The Service Packets limit sets a threshold to create an alarm when the packet rate exceeds the limit when using the NTP reflector or PTP master. The service packets threshold does not limit the number of packets handled. When the service packet threshold is exceeded the “service load limit exceeded” alarm will set. If a timing service (NTP reflector or PTP) is mapped to an Ethernet port, then the all packets threshold is set to a fixed value of 3000 packets/second.

See the image below. If a timing service is enabled on a port it is identified by the green indicator on this form.

Figure 5-51. Security - Packet Monitoring Window



5.3.5.13 Security - X.509 Certificate Signing Request (CSR)

Use this window to generate and download a Certificate Signing Request (CSR). See the image below. CSRs are created in the Base-64 encoded PEM format. This format includes the “-----BEGIN CERTIFICATE REQUEST-----” and “-----END CERTIFICATE REQUEST-----” lines at the begining and end of the CSR.

Note: Some certificate authorities require the user to change the public/private keys before requesting a new certificate. To change the keys, go to the Security->HTTPS web page, fill out the self-signed certificate with the “Regenerate keys” box checked. Then click “Apply”.
Then you will be ready to create a CSR with new keys.

However, changing the keys will invalidate any existing X.509 certificate, and the system will use a new self-signed certificate until a new certificate is installed.

The SyncServer is typically deployed within an enterprise that manages it's own root and/or intermediate Certification Authorities. The Certificate Signing Requests generated by the SyncServer will be signed by these internal Certification Authorities to generate X.509 Certificates that will be installed on the SyncServer.

The CSR page accepts the following information from the user:

Figure 5-52. Security - X.509 CSR Window

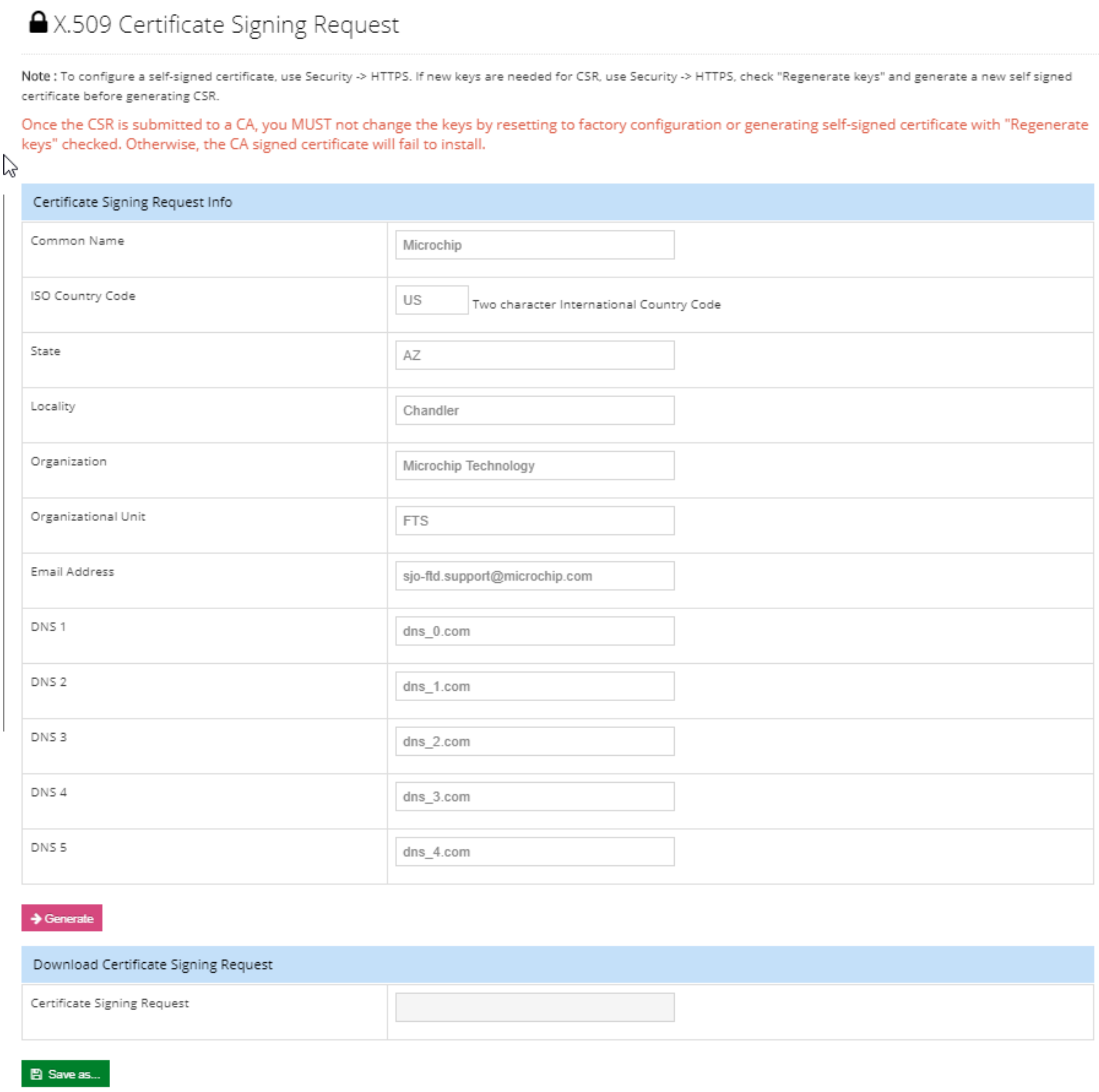


Table 5-14. X.509 Configuration Parameters

Parameter / Column	Description
Common Name	Fully qualified domain name (FQDN) of the SyncServer
ISO Country Code	Two-character code for country where you are located
State	State where you are located (for example, California)
Locality	City where you are located
Organization	Name of organization
Organizational Unit (optional)	Unit or division of organization (for example, IT Department)
Email Address	Optional email address
DNS 1	FQDN for optional SAN (subject alternative name). Leave blank if not required.
DNS 2	FQDN for optional SAN (subject alternative name). Leave blank if not required.
DNS 3	FQDN for optional SAN (subject alternative name). Leave blank if not required.
DNS 4	FQDN for optional SAN (subject alternative name). Leave blank if not required.
DNS 5	FQDN for optional SAN (subject alternative name). Leave blank if not required.
Generate	The CSR is generated when the “Generate” button is pressed.
Download Certificate Signing Request	The “Download Certificate Signing Request” section on the page allows the user to download the CSR as a file.
Save As	This button allows the user to save the CSR on the user’s machine

To learn more, perform an internet search on the terms “SSL Certificate Formats”, “PEM Files” and/or “Converting SSL certificate formats”

5.3.5.13.1 Security - X.509 Install

Use this window to install on the SyncServer the Certificate or Certificate/Chain that was generated using the CSR. See the image below. Installation can be done with certificate/chain files in PEM or PKCS7 format. The PEM format is the most common format that Certification Authorities issue certificates in. PEM certificates usually have extentions such as .pem, .crt, .cer, and .key. They are Base64 encoded ASCII files and contain “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----” statements. Server certificates, intermediate certificates, and private keys can all be put into the PEM format. Apache and other similar servers use PEM format certificates. Several PEM certificates, and even the private key, can be included in one file, one below the other, but most platforms, such as Apache, expect the certificates and private key to be in separate files. The PKCS#7 or P7B format is usually stored in Base64 ASCII format and has a file extension of .p7b or .p7c. P7B certificates contain “-----BEGIN PKCS7-----” and “-----END PKCS7-----” statements. A P7B file only contains certificates and chain certificates, not the private key. Several platforms support P7B files including Microsoft Windows and Java Tomcat.

Depending on the CA signing setup, installation can be done in either one of the following two ways:

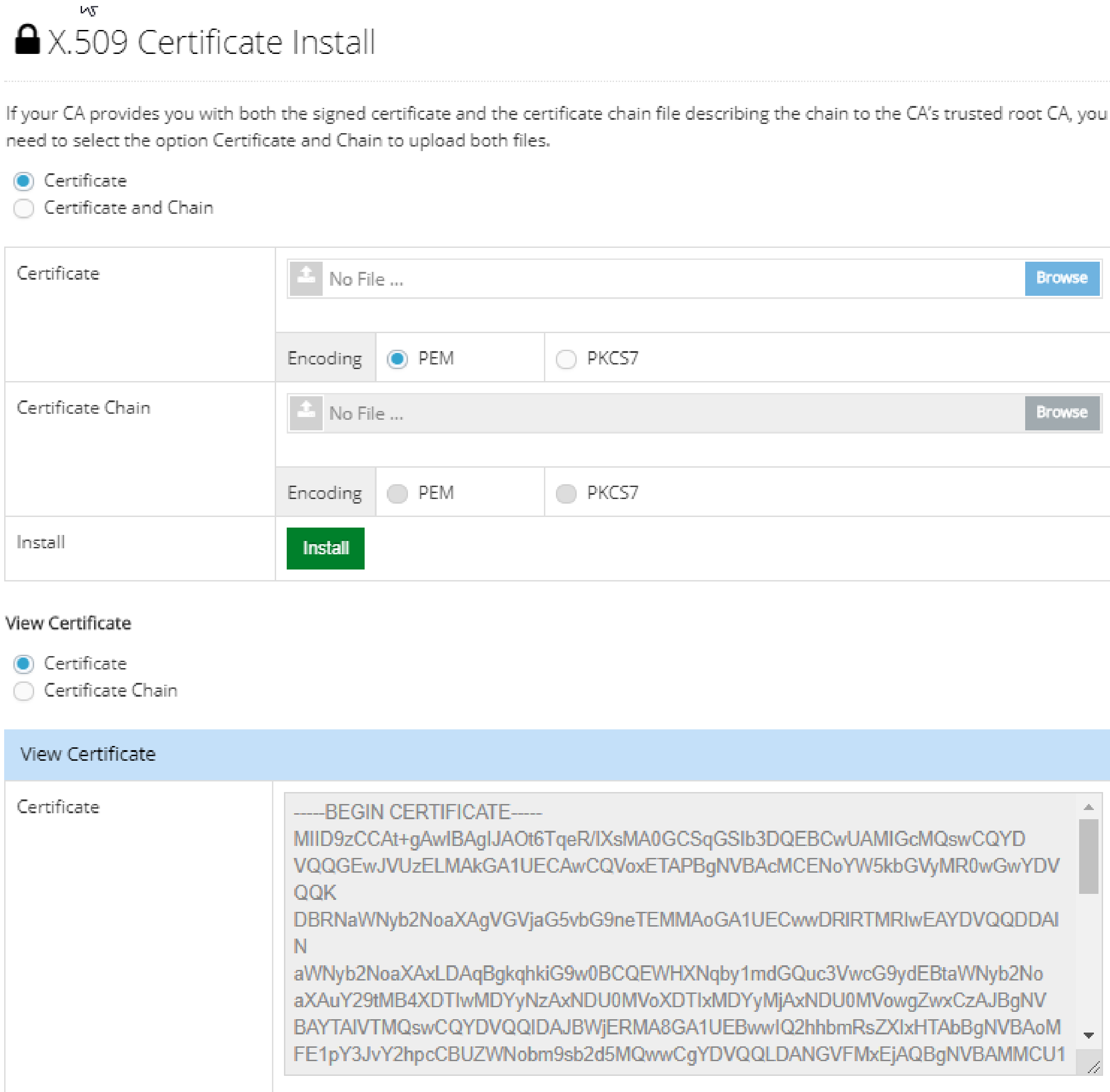
1. A single certificate file, which includes the signed end user (SyncServer) certificate and the certificate chain (intermediate CAs if any and root CA).
2. Two files, with the first one being the signed end user (SyncServer) certificate and the second being the certificate chain.

The user can upload the signed certificate/chain files and then click the “Install” button to install the certificate on the SyncServer.

The “View Certificate” section allows the user to view the certificate currently being used in the system. The root/intermediate CA's certificate(s) are also installed in client web browsers that will access the SyncServer. The browser being used needs to be able to identify the Certification Authority as a known or trusted CA. This will allow the browser to show the connection to the SyncServer as being secure (https).

Note: If an HTTPS certificate was installed, the system will return to using the self-signed HTTPS certificate after a configuration default.

Figure 5-53. Security - X.509 Install Window



5.3.6 Jamming / Spoofing Windows

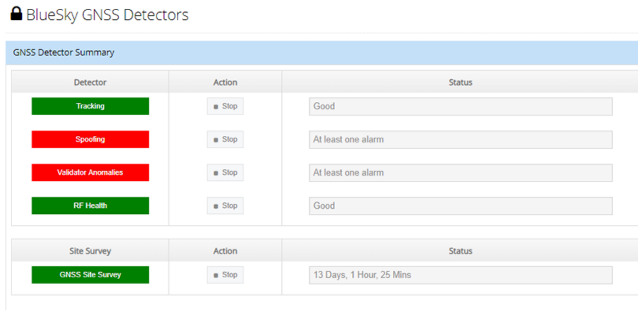
The Jamming / Spoofing tab on the dashboard provides access to view BlueSky GNSS detectors, configure BlueSky GNSS, view BlueSky GNSS Integrity status, and display GNSS satellite information in a variety of chart formats.

5.3.6.1 Jamming / Spoofing - Detectors

Use this window to start and stop GNSS detectors, as well as to view status of these detectors.

Note: Maximum NTP load is reduced to 6000 requests/second if the validator detector is running.

Figure 5-54. Jamming / Spoofing - Detectors Window

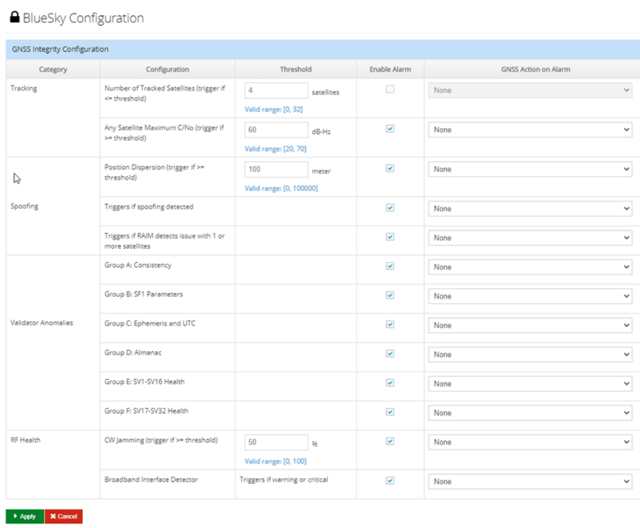


5.3.6.2 Jamming / Spoofing - Configuration

Use this window to configure GNSS integrity settings for jamming / spoofing.

Note: If a satellite is unhealthy, especially for maintenance or commissioning, then the use may want to not configure validator rules to disqualify GNSS since validator rules may be violated during maintenance.

Figure 5-55. Jamming / Spoofing - Configuration Window

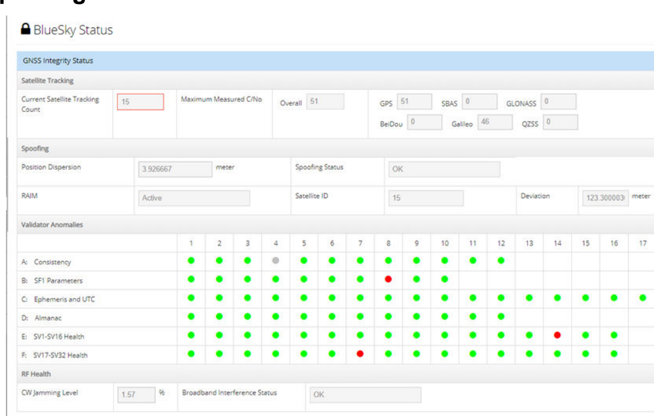


5.3.6.3 Jamming / Spoofing - Status

Use this window to view the status of GNSS integrity.

Note: You can get the GPS constellation status, including planned outages, at:www.navcen.uscg.gov/?Do=constellationStatus

Figure 5-56. Jamming / Spoofing - Status Window



5.3.6.4 Jamming / Spoofing - Charts

Use this window to view GNSS satellite information charts.

Figure 5-57. Jamming / Spoofing - Charts Window - Current Sky View

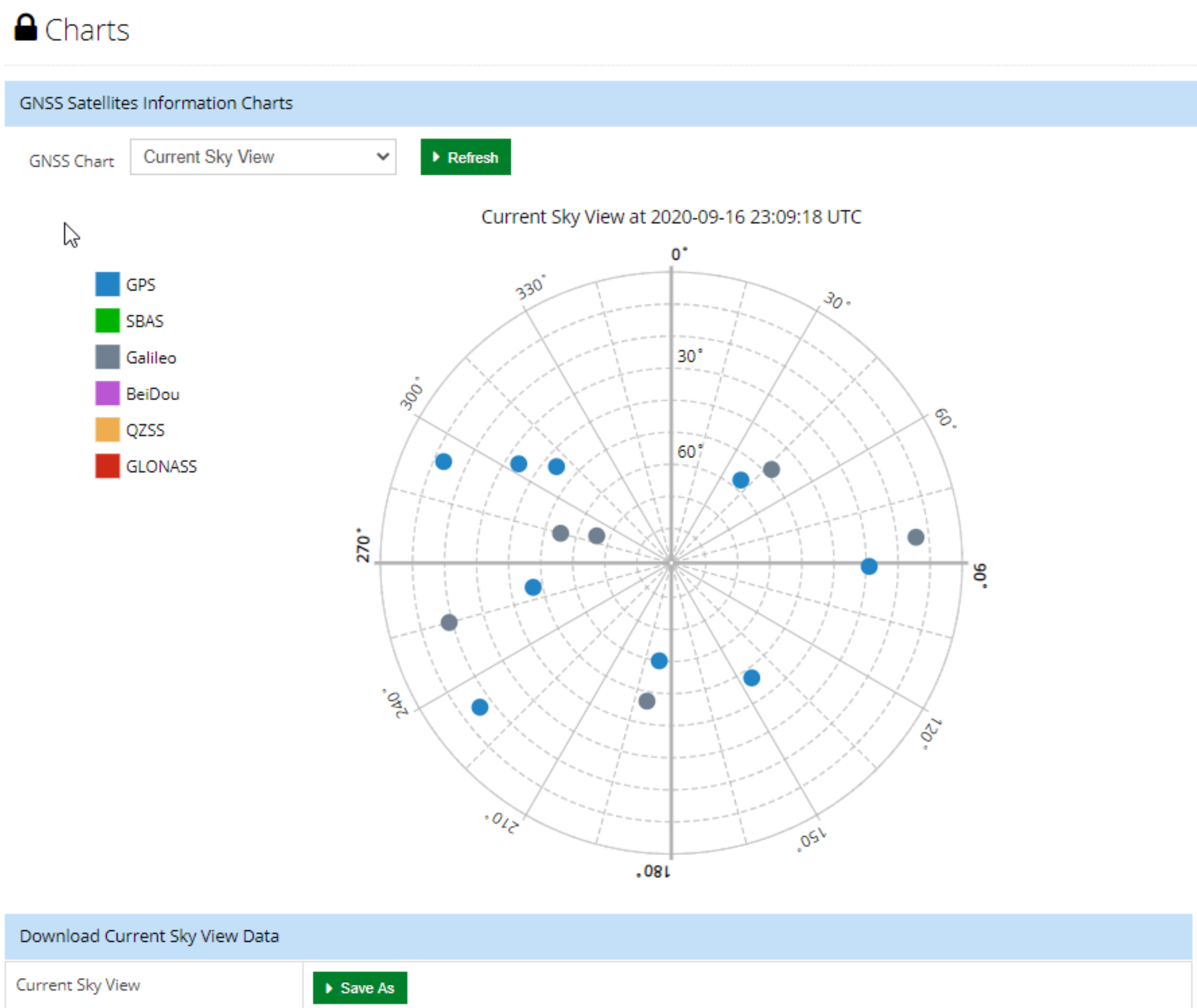


Figure 5-58. Jamming / Spoofing - Charts Window - Tracked Satellites

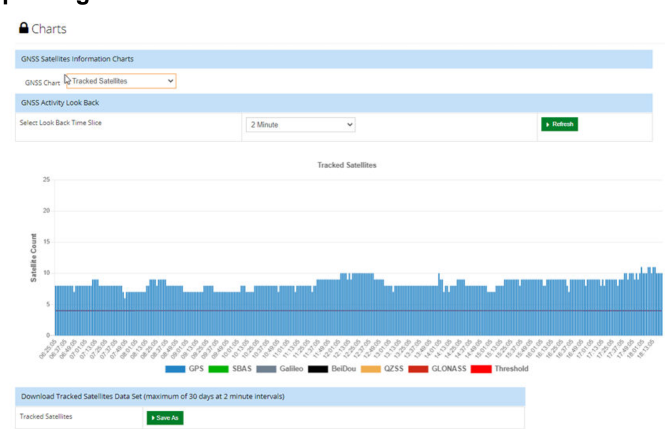


Figure 5-59. Jamming / Spoofing - Charts Window - Cumulative Site Survey

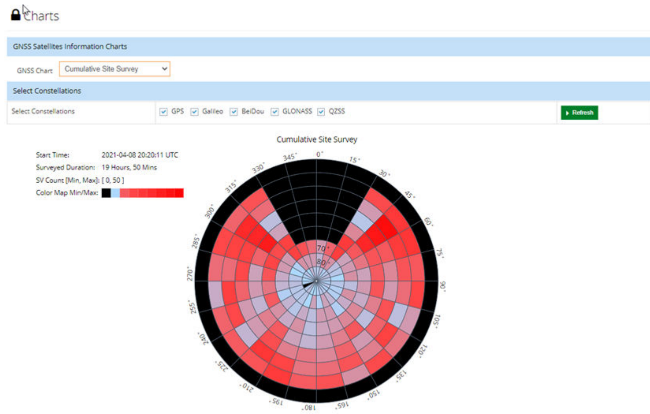


Figure 5-60. Jamming / Spoofing - Charts Window - Position Dispersion

Figure 5-61. Jamming / Spoofing - Charts Window - Maximum C/No

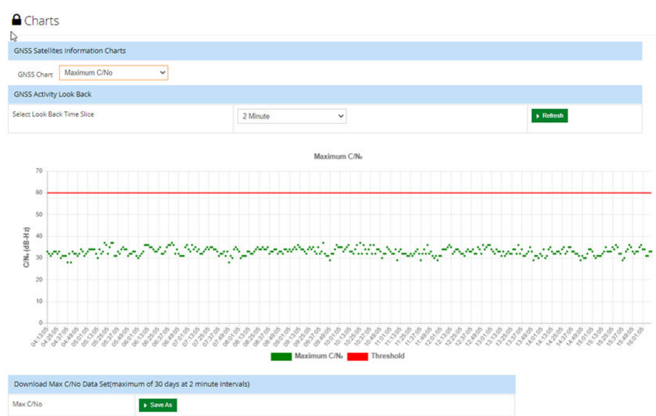


Figure 5-62. Jamming / Spoofing - Charts Window - CW Jamming

5.4 Admin Configuration Windows

5.4.1 Admin - General Configuration Window

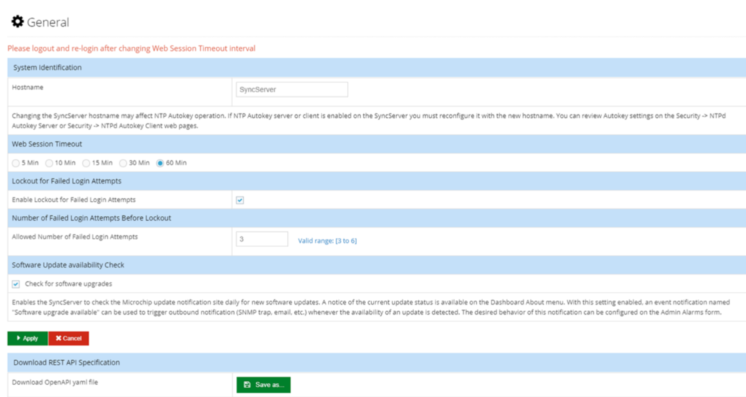
Use this window to configure system identification and to check for software updates. See the image below. Enables the SyncServer to check the Microchip upgrade notification site at http://update.microsemi.com every day at noon local time for new software updates. Displays a notice on the Status page and can send and SNMP trap when an upgrade is available. Requires that the SyncServer management port have firewall access to the internet.

This page also provides control for the user lockout due to failed login attempts. This feature can be enabled/disabled and the number of attempts can be configured.

Notes: Only alphanumeric characters, hyphen, and underline are allowed for the hostname. The hostname can be from 1 to 63 characters long.

- abcdefghijklmnopqrstuvwxyz
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 0123456789
- -_

Figure 5-63. Admin - General Configuration Window

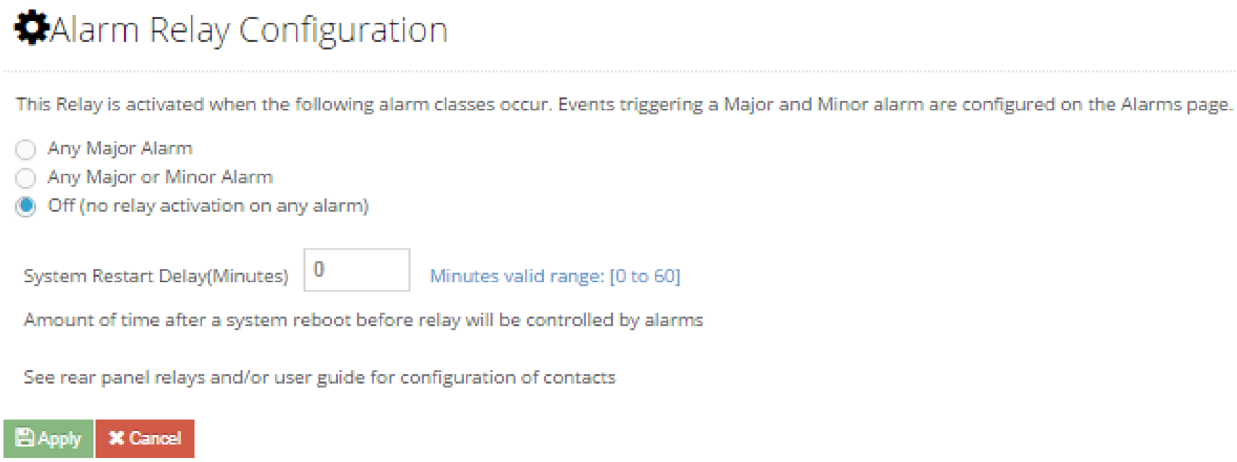


Note: The software update availability feature uses IPv4. An IPv4 address and DNS server must be configured on the Network->Ethernet page in order to use this feature.

5.4.2 Admin - Alarm Relay Configuration Window

Use this window to configure system alarm relay details. See the image below.

Figure 5-64. Admin - Alarm Relay Configuration Window



5.4.3 Admin - Alarm Configuration Window

Use this window to configure system alarms. Users can also see the current status of each alarm and clear individual alarms. Use the scroll control on this form to access additional alarms. See the image below. See the following table for descriptions of Alarm Configuration parameters.

Figure 5-65. Admin - Alarm Configuration Window

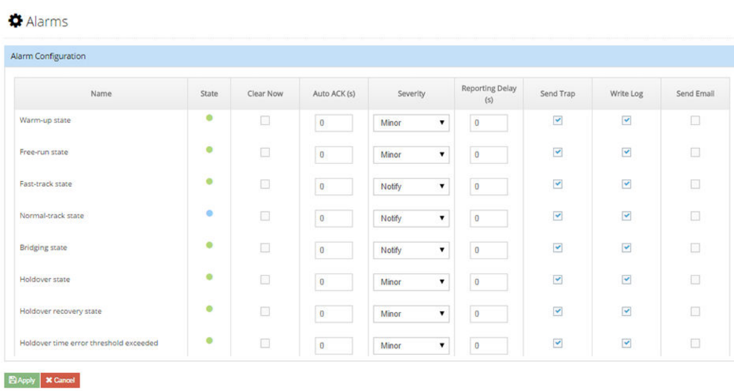


Table 5-15. Alarm Configuration Parameter Descriptions

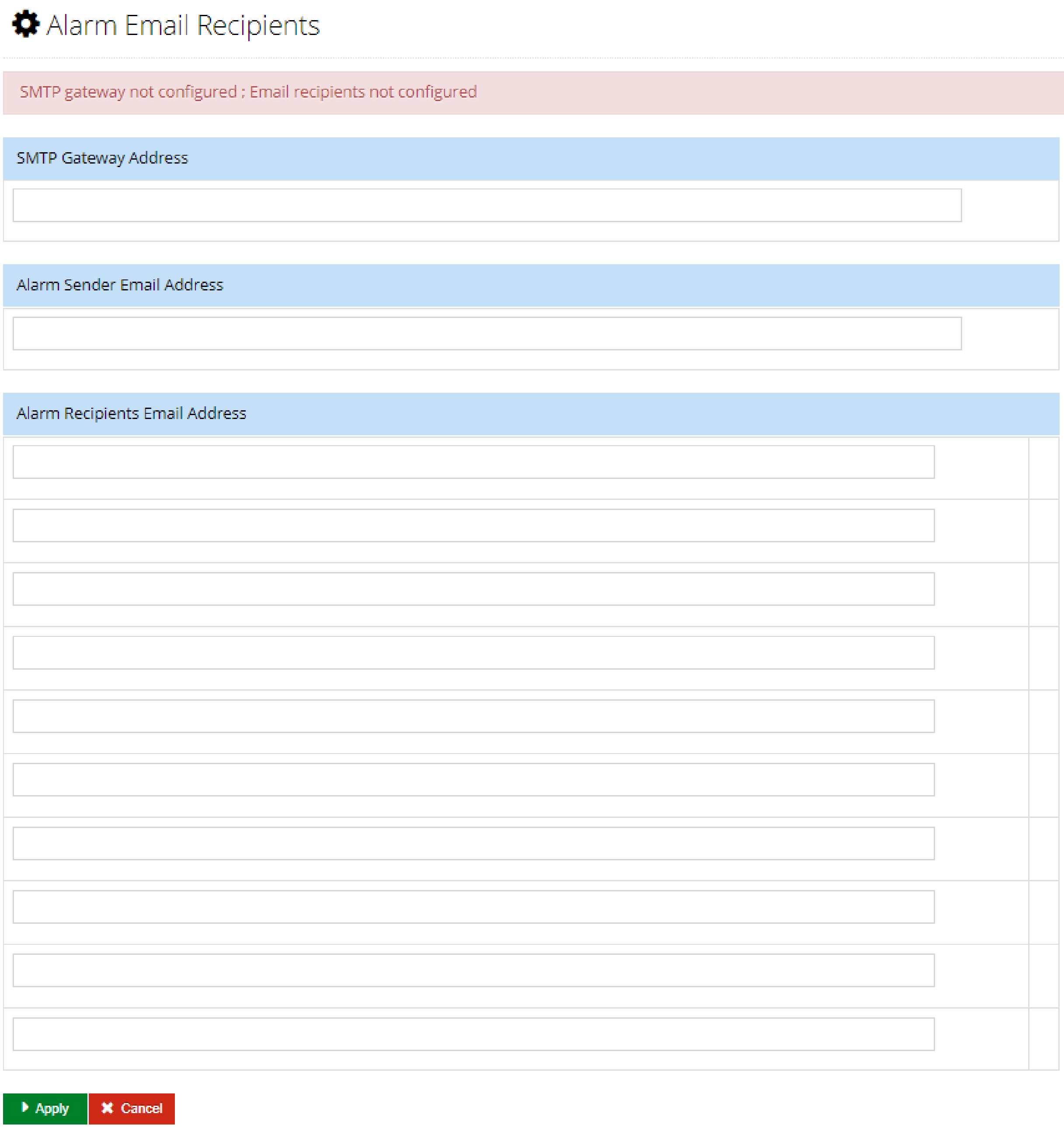
Parameter	Description
Name	Name of the alarm. If there is an asterisk as first character it means it is a transient alarm. For alarms that have multiple secondary info (e.g. Excessive Traffic on Ethernet port has a secondary field that identifies which port), these settings are global to all of the secondary cases.
State	Indicates the current status of the alarm based on color • Always grey (unlit) if the event is transient. • Green if severity is Minor, Major, or Notify and the condition is not SET or if the user has cleared (acknowledged it) even if it is SET. • Blue if severity is Notify and the condition is SET and not user-cleared • Amber if severity is Minor and the condition is SET and not user-cleared • Red if severity is Major and the condition is SET and not user-cleared

...........continued	
Parameter	**Description**
Clear Now	This is a user-control to cause some of the alarm report mechanisms to extinguish that particular alarm indication. These include Dashboard > Alarms, Alarm summary at top of Web GUI, Physical alarm connector, front panel Alarm LED, and Alarm information on front-panel display.This is really just an acknowledgement of the alarm, but of course has no ability to impact the underlying condition.
Auto ACK	This is the same as Clear Now except it provides an automatic clearing action after a user-defined time period following SET of the alarm. Zero (default) means to never auto-clear it.
Severity	Controls the reported severity level of the alarm. Notify | Minor | Major The severity level “Notify” is not reported on Dashboard > Alarms, Alarm summary at top of Web GUI, Physical alarm connector, front panel Alarm LED, Alarm information on front-panel display. This also applies to transient alarms.
Reporting Delay	This value can be used to defer the time from when the condition becomes SET until it is actually reported. If the condition has cleared by the time the delay has elapsed then the alarm is never reported. Main purpose would be to avoid “chatter”.
Send Trap	Provides “per alarm” user control of reporting the alarm via SNMP Trap. All severities are reported with Traps.
Write Log	Provides “per alarm” user control of reporting the alarm by writing an event entry in the Log. All severities and transients are reported into the message log.
Send Email	Provides “per alarm” user control of reporting the alarm by sending an Email. All severities and transients are reported with email.

5.4.4 Admin - Email Configuration Window

Use this window to set, modify or delete email addresses for alarm email recipients. See the image below.

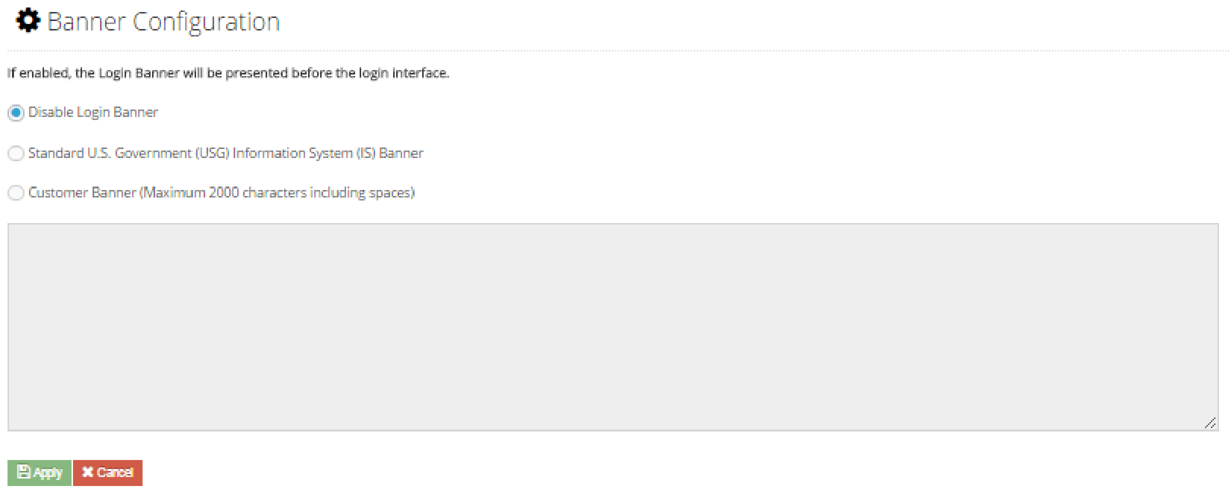
Figure 5-66. Admin - Email Configuration Window



5.4.5 Admin - Banner Configuration Window

Use this window to enable whether the login banner is displayed before the login interface. Users can create a custom banner or use a standard U.S. government banner. See the image below.

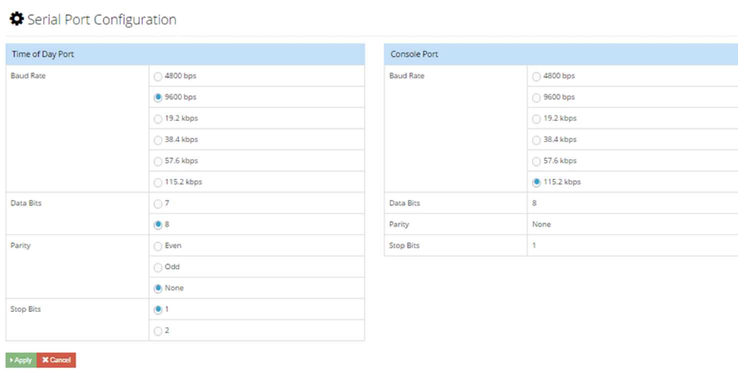
Figure 5-67. Admin - Banner Configuration Window



5.4.6 Admin - Serial Port Configuration Window

Use this window to configure the parameters for the Time of Day port and for the console Serial port. See the image below.

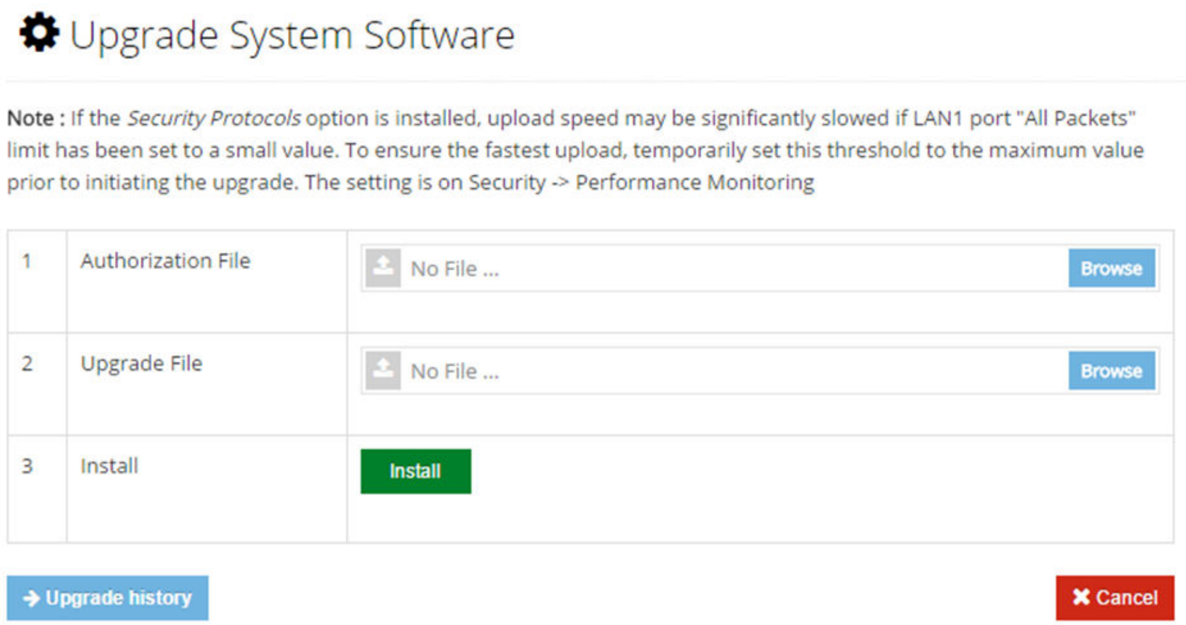
Figure 5-68. Admin - Serial Port Configuration Window



5.4.7 Admin - Upgrade System Software Window

Use this window to upgrade system software. Note that the system will reboot after the software is upgraded. See the image below.

Figure 5-69. Admin - Upgrade System Software Window



The authentication file is provided with the upgrade file and verifies that this SyncServer unit is authorized to upgrade with the specified upgrade file.

Note: You can check for the latest version number of SyncServer S600 and S650 software at these URLs: http://update.microsemi.com/SyncServer_S600

http://update.microsemi.com/SyncServer_S650

The number of the most current version of the software will appear. You can compare this to the version number installed in the SyncServer by proceeding to the web GUI Dashboard and finding the version number in the About drop down on the right side. If you do not have the latest version installed consider contacting Technical Support.

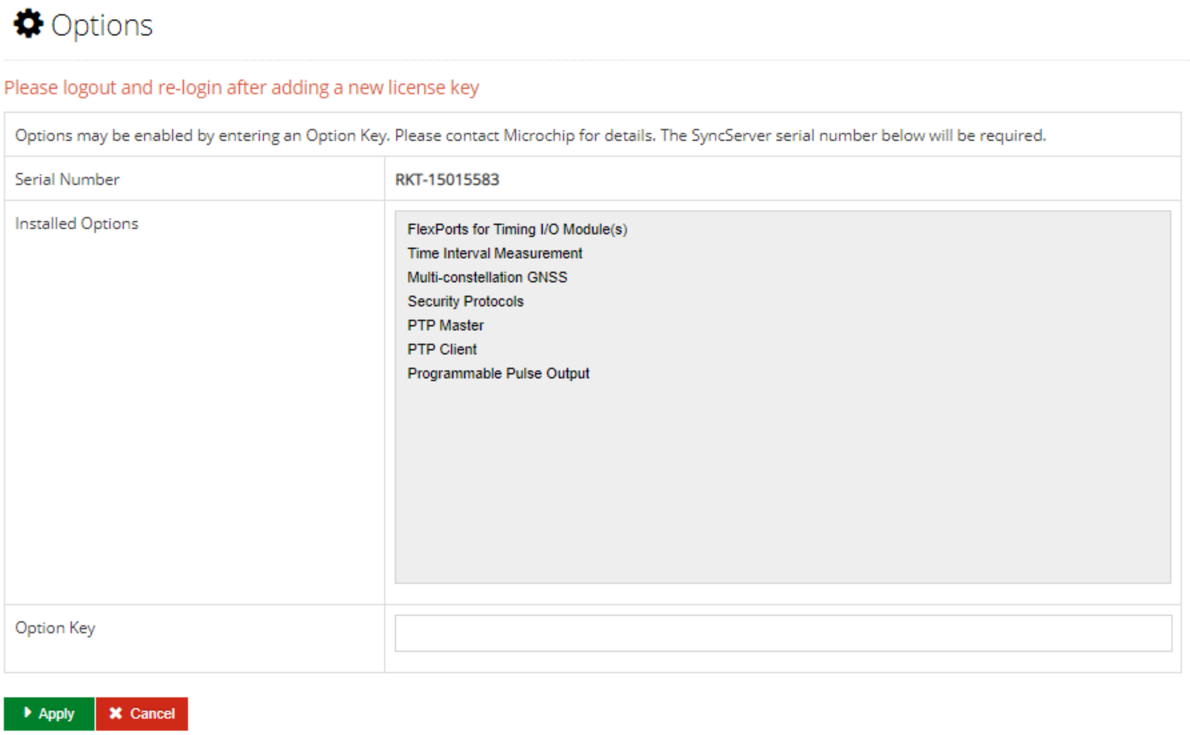
Note: For releases after 1.1, if the upgrade process is used to load a previous (older) version of the software, then the unit will reset the configuration to factory default values.

Note: If the all-packets limit on LAN1 has been reduced on the Security->Packet Monitoring page, then it is recommended that the limit be temporarily increased back to the default value of 13000 packets/second. Otherwise, the file upload will be very slow and may timeout.

5.4.8 Admin - Options Configuration Window

Use this window to view installed options and to enter option keys to enable SyncServer options. See the image below.

Figure 5-70. Admin - Options Configuration Window



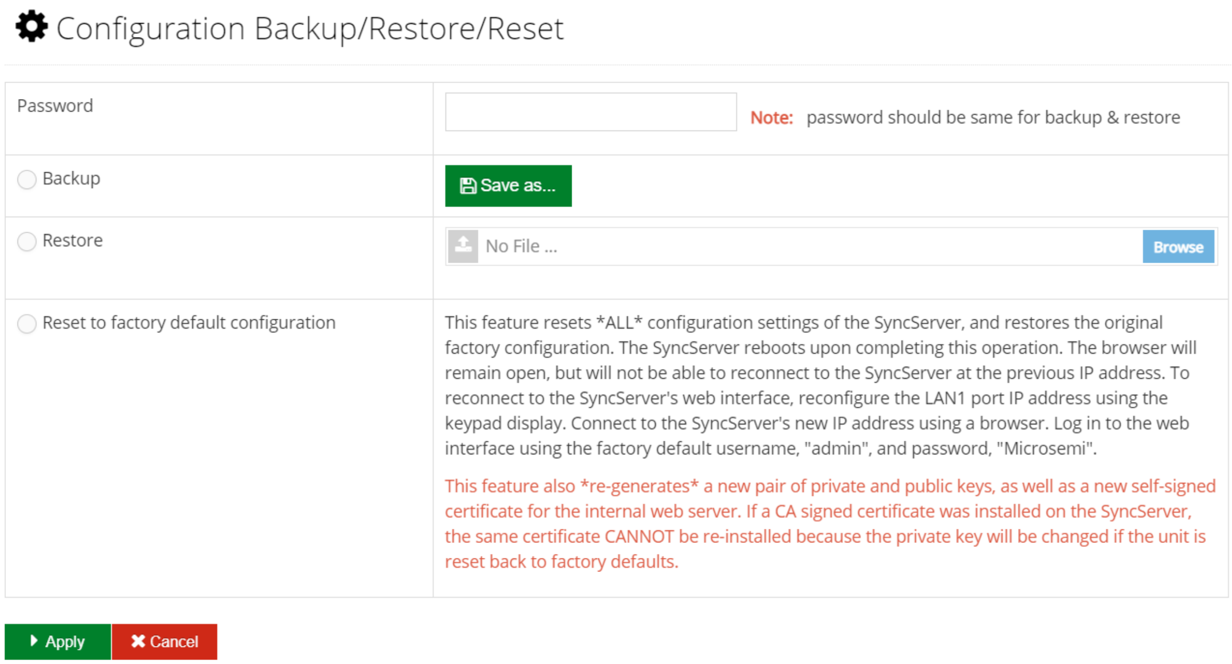
5.4.9 Admin - Configuration Backup / Restore / Reset

Use this window to back up, restore, or reset the SyncServer S6x0 to factory configuration. See the image below.

Note: For a configuration restore, the system will reject a configuration file that was generated from a unit running system software that is newer than the software currently running in the unit.

Note: If an HTTPS certificate was installed, the system will return to using the self-signed HTTPS certificate after a configuration reset to factory default.

Figure 5-71. Admin - Factory Reset Window



5.5 Logs Configuration Windows

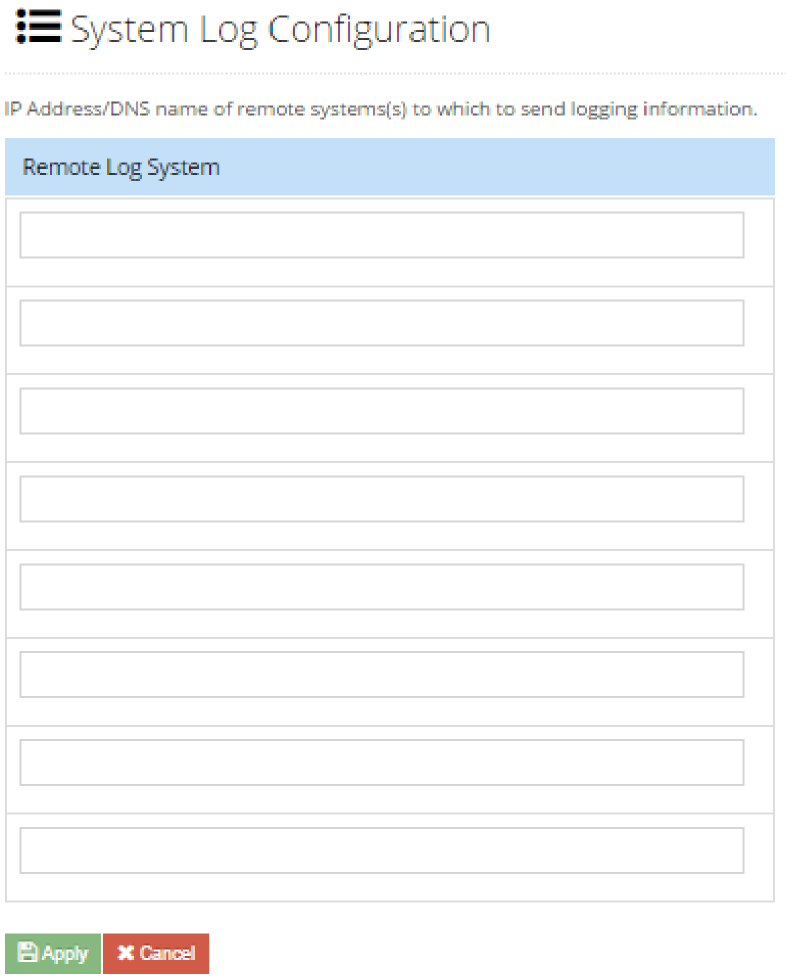
The logs rotate, and up to 7 logs are kept. In release 2.0 or later, individual rotated log files can be selected. When 7 have been created, the oldest will be overwritten. The log rotate depends on size of 100k, but this is subject to change without notice.

5.5.1 Logs - System Log Configuration Window

Use this window to set, modify, or delete IP addresses / DNS names of remote systems to which to send log information. See the image below.

Note: Syslog is designed to be used with LAN1. Do not configure a system log server address in a subnet used by the other LAN ports (LAN2 - LAN6).

Figure 5-72. Logs - System Log Configuration Window



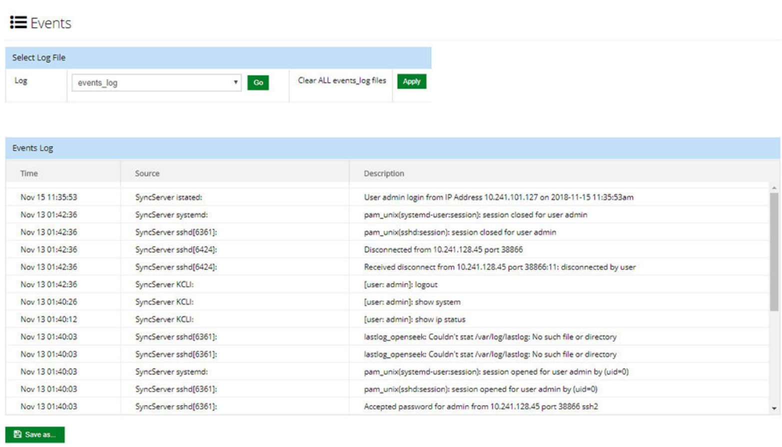
A remote syslog server can be configured with this window and all logs can then be stored on the remote server.

5.5.2 Logs - Events Log Configuration Window

Use this window to view and save the events log. See the image below.

Note: When an item is logged, the system will use the currently configured local timezone to calculate the time.

Figure 5-73. Logs - Events Window

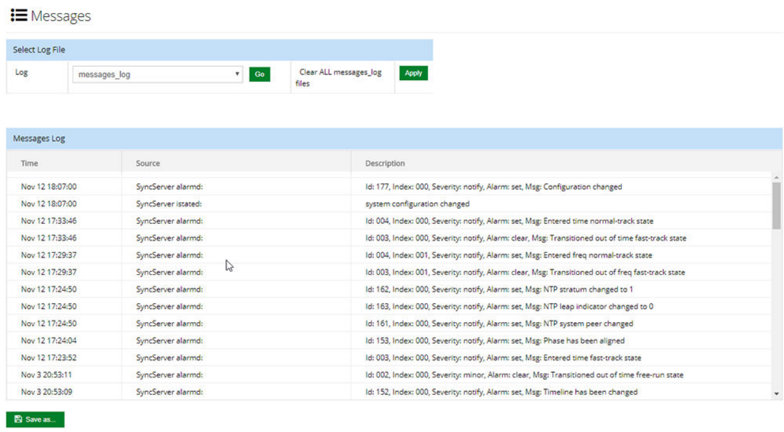


5.5.3 Logs - Messages Window

Use this window to view and save the message log. See the image below.

Note: When an item is logged, the system will use the currently configured local timezone to calculate the time.

Figure 5-74. Logs - Messages Window



5.6 Option Slot A/ Slot B Configuration Windows

5.6.1 Options Slot A and B Configuration Window - Timing I/O Module

Use this window to configure the module in Options Slot A and B.. See Provisioning IRIG Inputs on Timing I/O Module . See Provisioning Sine Wave Inputs on Timing I/O Module . See Provisioning Outputs on Timing I/O Module.

Note: Option Slot A and B are only available with the SyncServer S650.
The configurations on the Timing I/O Module configuration page are fixed unless the optional flex timing license is installed.

Note: For LPN and ULPN modules, even if the SyncServer has been locked for an extended time, the PPS coherency feature may require multiple hours to settle after being enabled. During initial lock and holdover recovery, the system 1PPS may have phase adjustments. This will impact the coherency between the 1PPS and the LPN/ ULPN 10 MHz outputs. The LPN/ULPN outputs will phase-jam and/or slew to the new 1PPS phase.

Note: If the programmable pulse license is installed, this feature is available on J7.

Figure 5-75. Options Slot A Configuration Window Showing Timing I/O Module

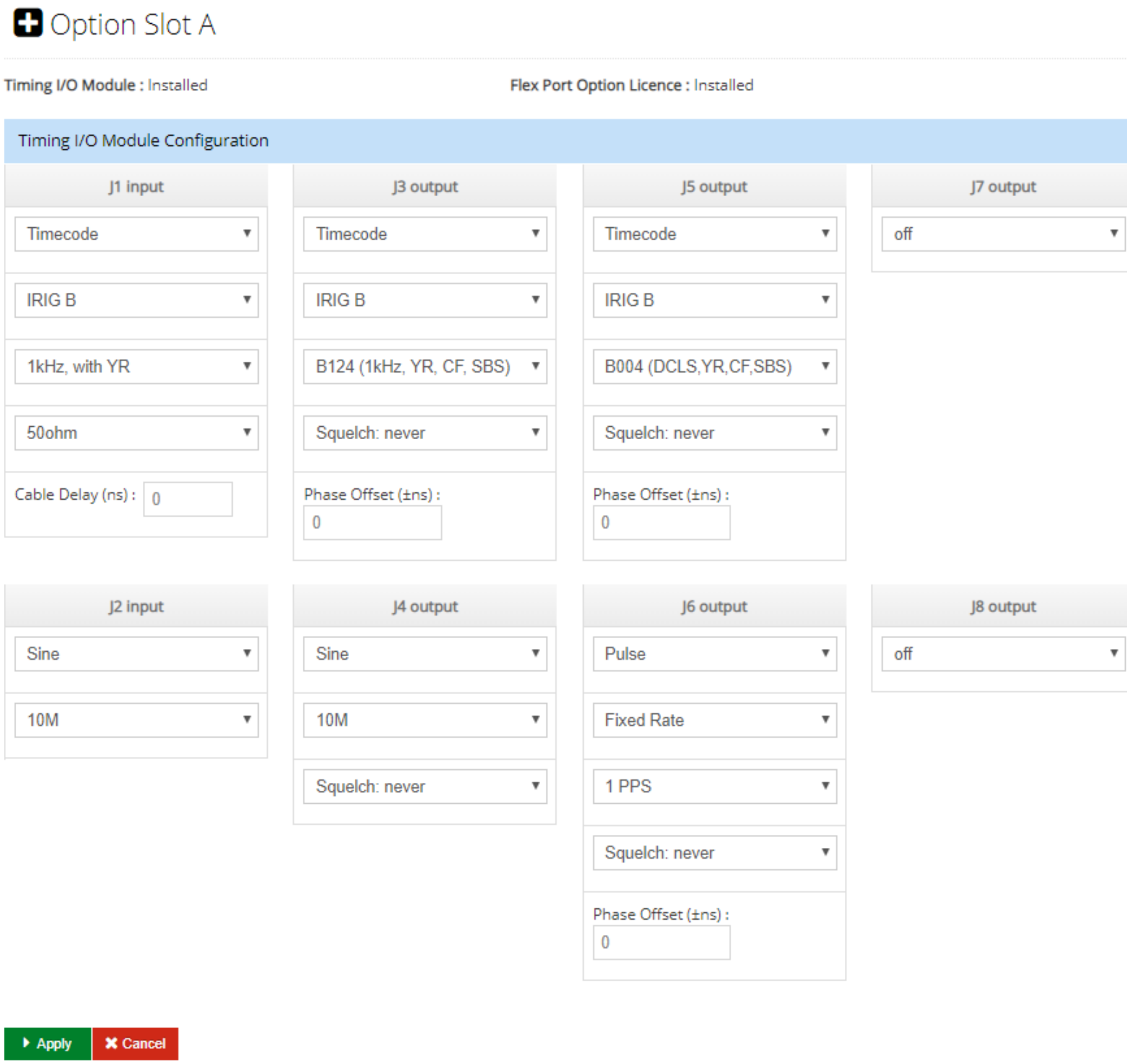


Figure 5-76. Options Slot A Configuration Window - Telecom Module Installed

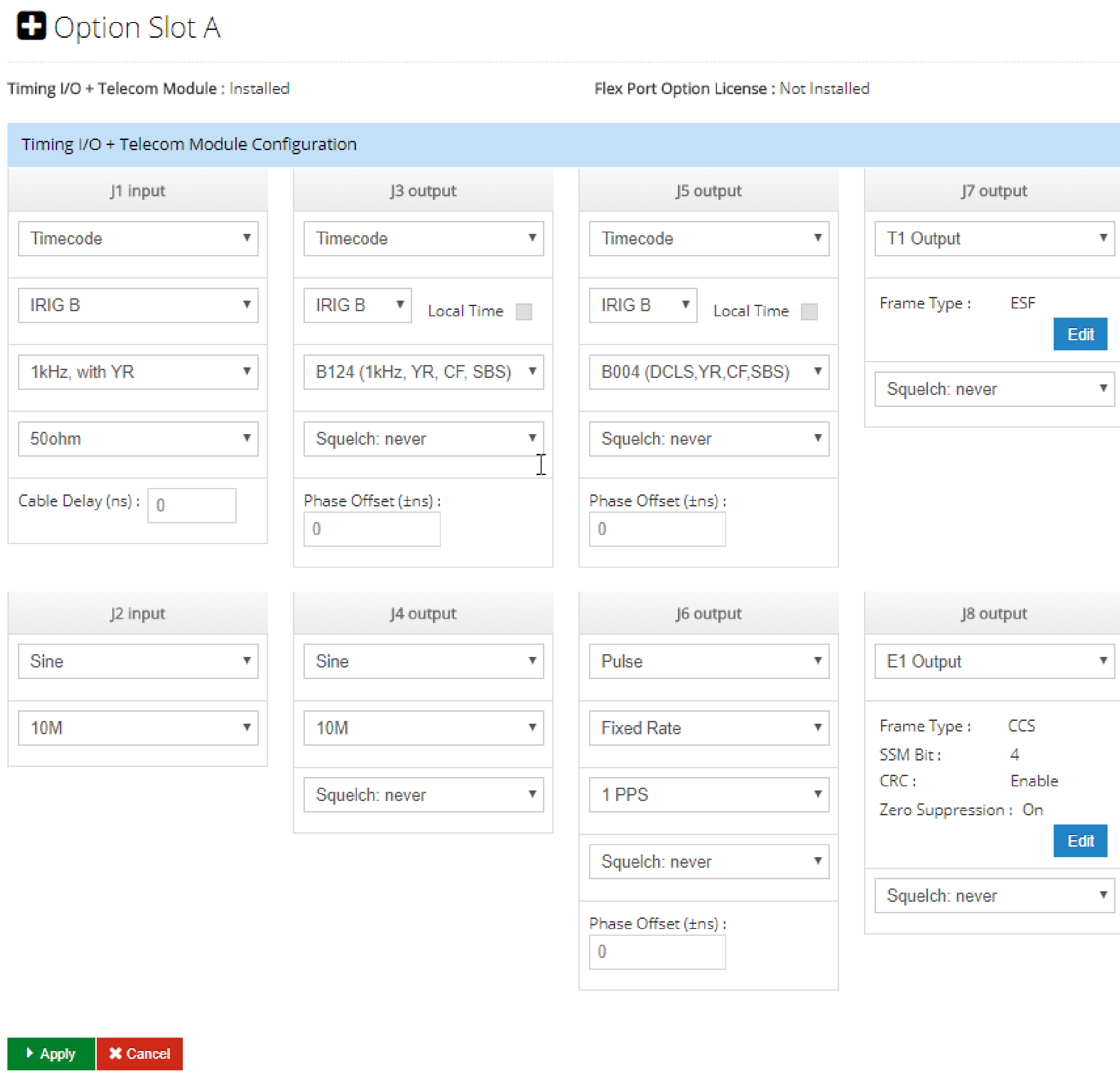


Figure 5-77. Options Slot A Configuration Window - Telecom Module - T1 Input Choices

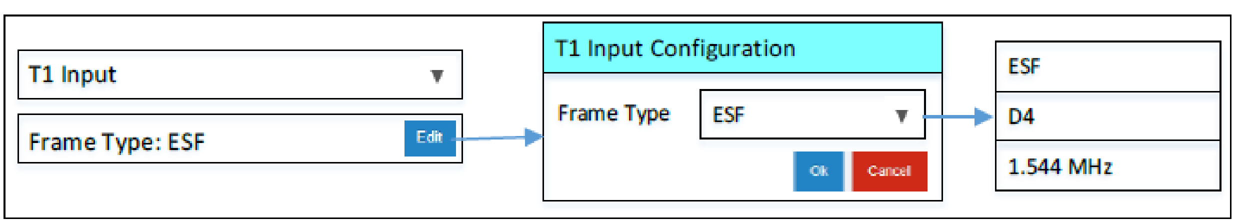


Figure 5-78. Options Slot A Configuration Window - Telecom Module - E1 Input Choices

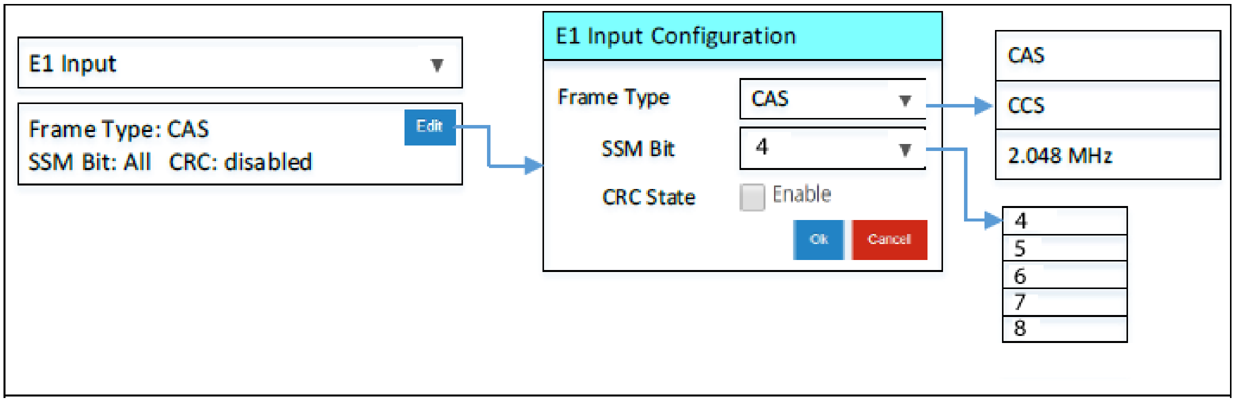


Figure 5-79. Options Slot A Configuration Window - Telecom Module T1 Output Choices

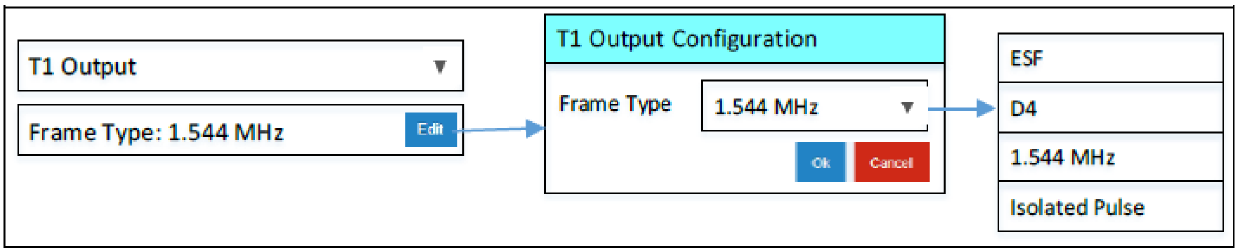


Figure 5-80. Options Slot A Configuration Window - Telecom Module E1 Output Choices

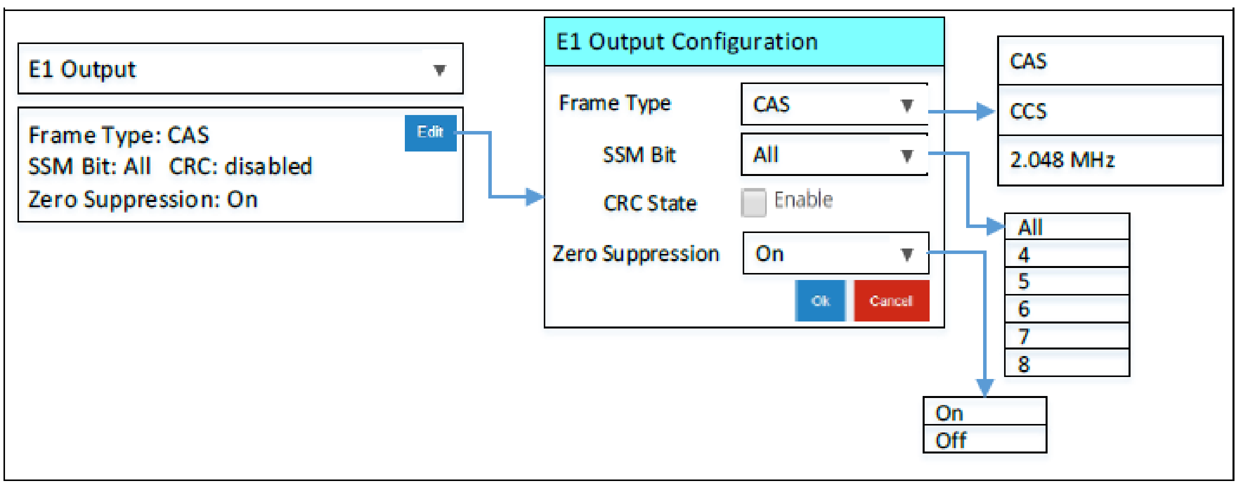


Figure 5-81. Telecom Module - J7 and J8 Examples - Flex Port License

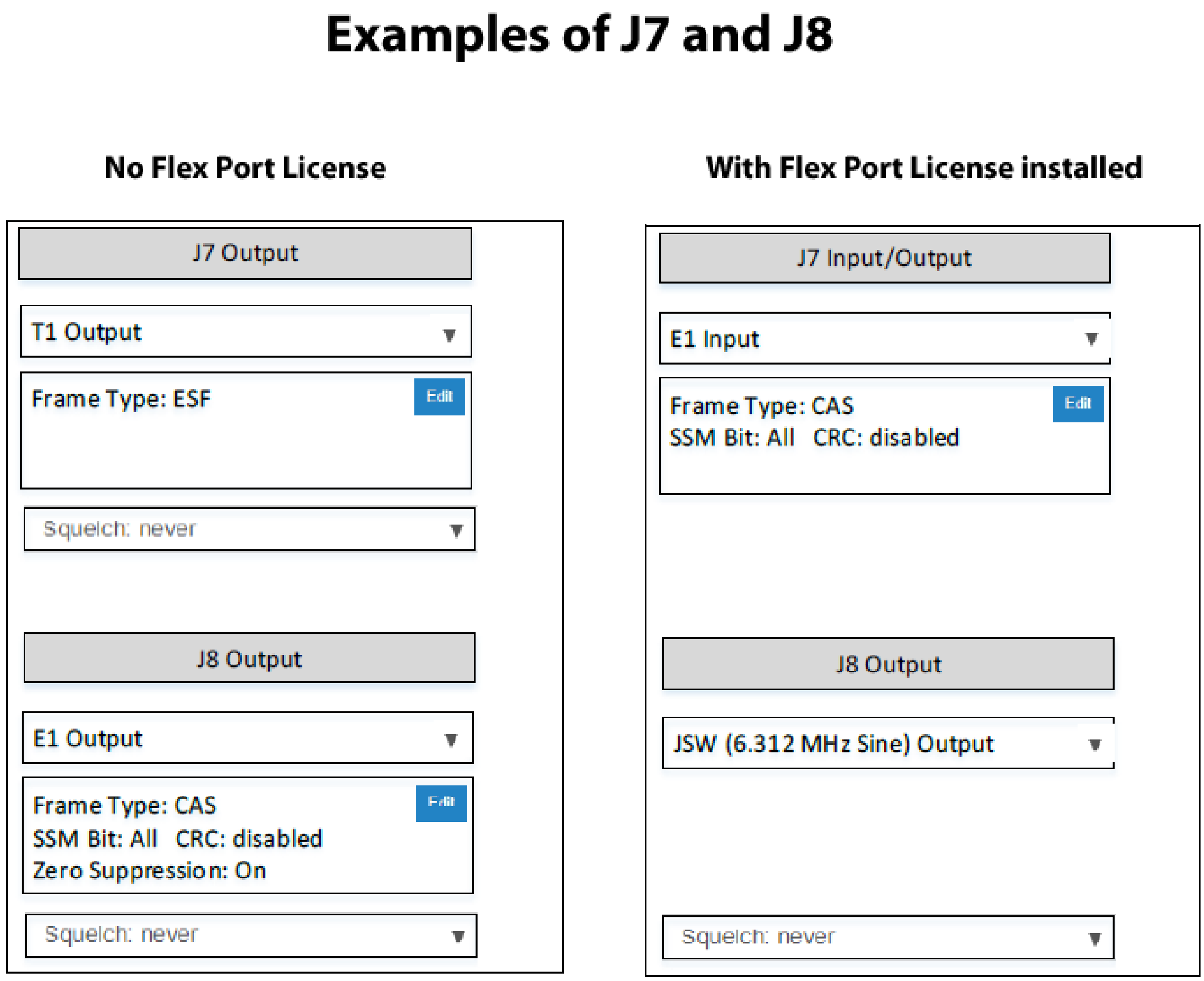
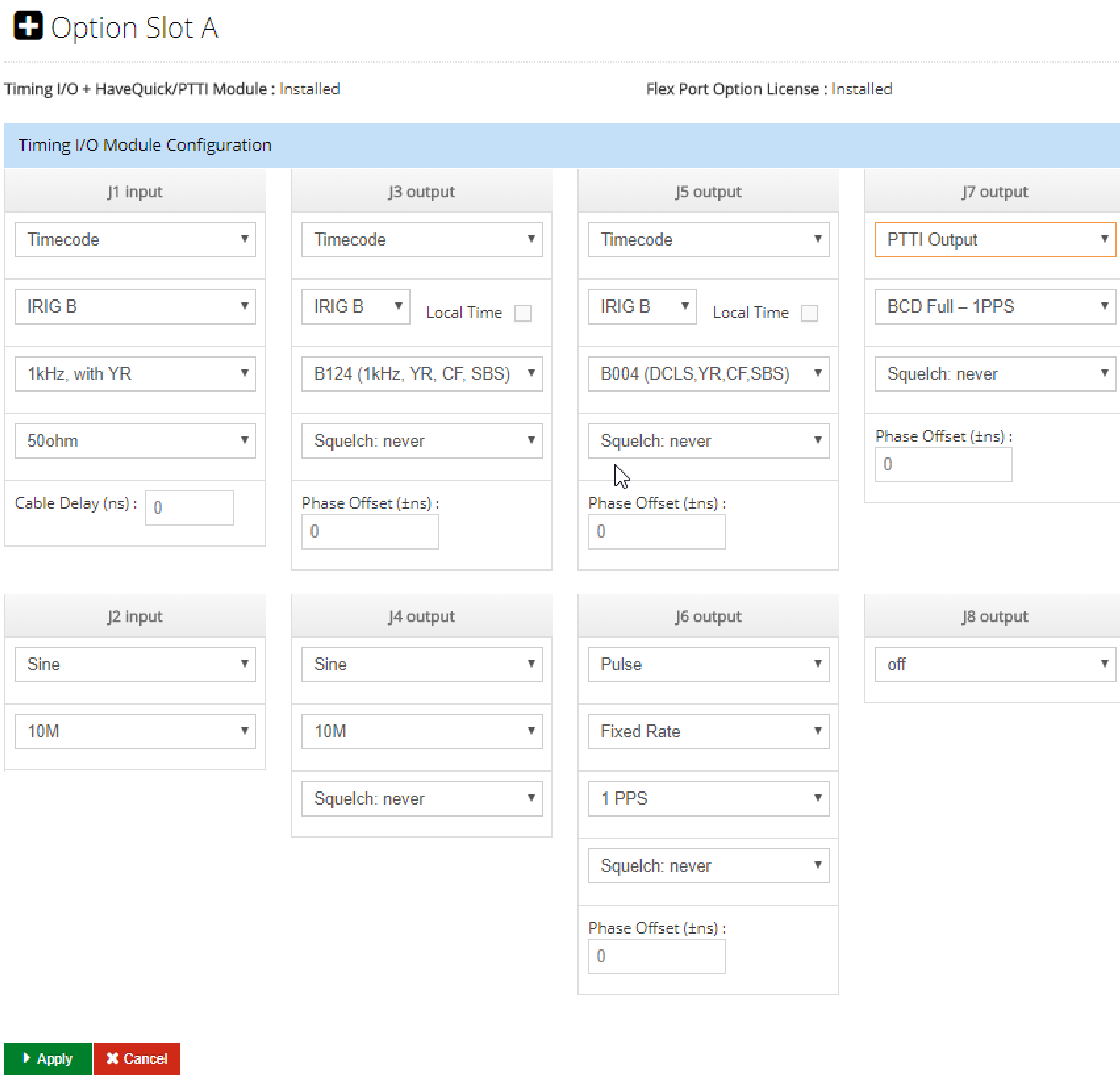


Figure 5-82. Options Slot A Configuration Window - HaveQuick/PTTI Module Installed



The SyncServer S600/S650 has separate timing and frequency clock controls.

The squelch feature uses the time clock state for timecode and fixed-rate pulse modes. The squelch feature uses the frequency clock state for programmable-period pulse and sine modes.

The time clock state can be viewed on the “Time of Day Status” line on the Dashboard >Timing display. Normally frequency and clock states are the same. If they are different, then the frequency clock state is displayed next to the icon on the “Current Reference” line.

Table 5-16. Squelch Settings

Squelch Setting	Function	Notes
Never	Clock state will not cause squelch.	
If not locked	Output will only occur when appropriate clock state is “Locked” or “Bridging” (internal state = Normal or Bridging)	

...........continued		
Squelch Setting	**Function**	**Notes**
In warmup / freerun / locking / holdover exceeded	Output will only occur when appropriate clock state is “Locked”, “Bridging”, or “Holdover”	
In warmup	Squelch output from powerup until unit comes out of warmup. It will not be squelched after that.	Output will first turn on when “freerun” is entered.
In warmup / freerun	Prevent output from powerup until the unit comes out of freerun. Once (if) it does it will stay on since these states can never be re-entered.	Output will be turned on when “Locking” is entered.
In warmup / freerun/ locking	Prevent output from powerup until unit comes out of “Locking” (internal state = “fast”). Another way of saying this is don't output until first lock from powerup, but thereafter always output.	These 3 states are only encountered following powerup or reboot. Once Locked state is attained none of these states will ever occur again.

Table 5-17. Clock Status

SyncServer Clock Status	Description	Possible Next State	Conditions Required for Next Transition State
Warmup	The unit is warming up. This is the first clock state following power-up or reboot. Typical Warm-up time is: Quartz: 6 minutes Rubidium: 9 minutes **Note:** Warm-up times may vary based on environmental conditions and other factors.	Freerun	Warm-up complete
Freerun	The unit is operating without an input reference, but is ready to use one. This state will persist if no qualifiable input reference is provided. While in this state, the stability of the clock output is tied to the internal reference oscillator.	Fast-track	Input becomes qualified
Fast-track	The selected input has been qualified and the firmware clock servo begins to actively converge the output to the selected input. This is the transitional phase that leads to the Locked clock state. Typical duration for Quartz and Rubidium: 20 minutes	Freerun	The unit no longer has a qualified input.
		Normal	Clock stabilized
Locked	The unit has a qualified input and is locked to the reference.	Recovery	Clock not stabilized adequately
		Bridging	The unit no longer has a qualified input.

...........continued

SyncServer Clock Status	Description	Possible Next State	Conditions Required for Next Transition State
Bridging	The unit no longer has a qualified reference, but remains operating within performance associated with Locked operation.	Holdover	Bridging time exceeded
		Normal	Input reference re-qualified in less than bridging time.
Holdover	The unit no longer has a qualified reference.	Recovery	Input becomes qualified
Recovery	The selected input has been qualified and the firmware clock servo begins to actively converge the output to the selected input.	Holdover	The unit no longer has a qualified input.
		Locked	Clock stabilized

5.6.2 Options Slot B Configuration Window

Use this window to configure the module in Options Slot B.

Note: Option Slot B is only available with the SyncServer S650.

Figure 5-83. Slot B - Fiber Input Module, Flex Port and Pulse Output Options Installed

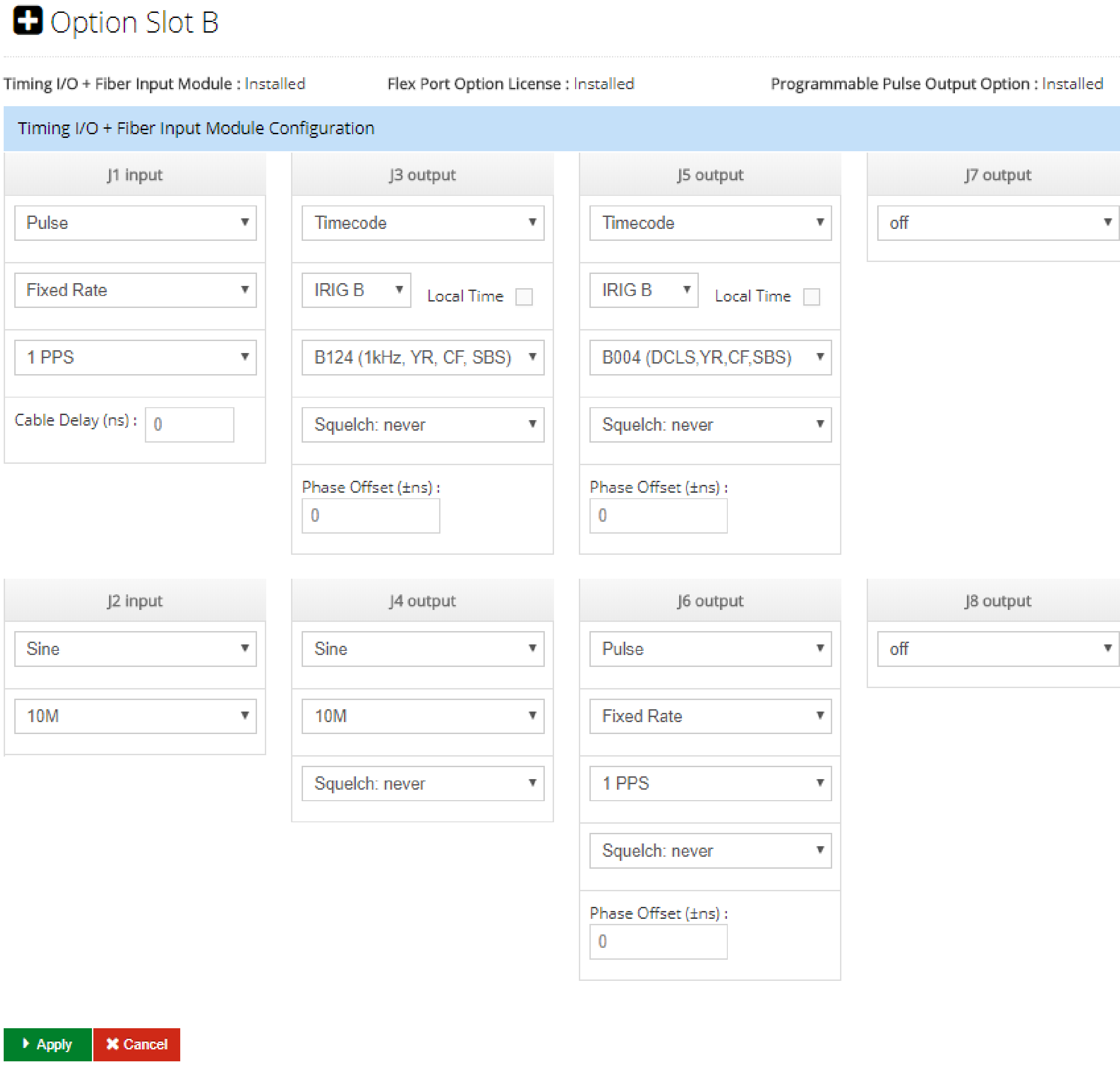


Figure 5-84. Slot B - Fiber Output Module, Flex Port and Pulse Output Options Installed

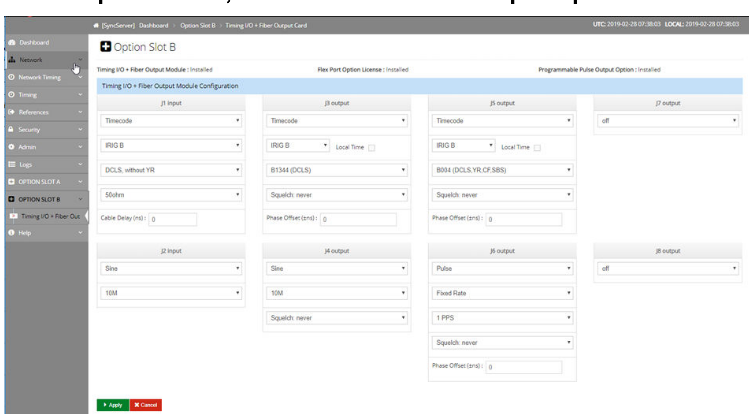
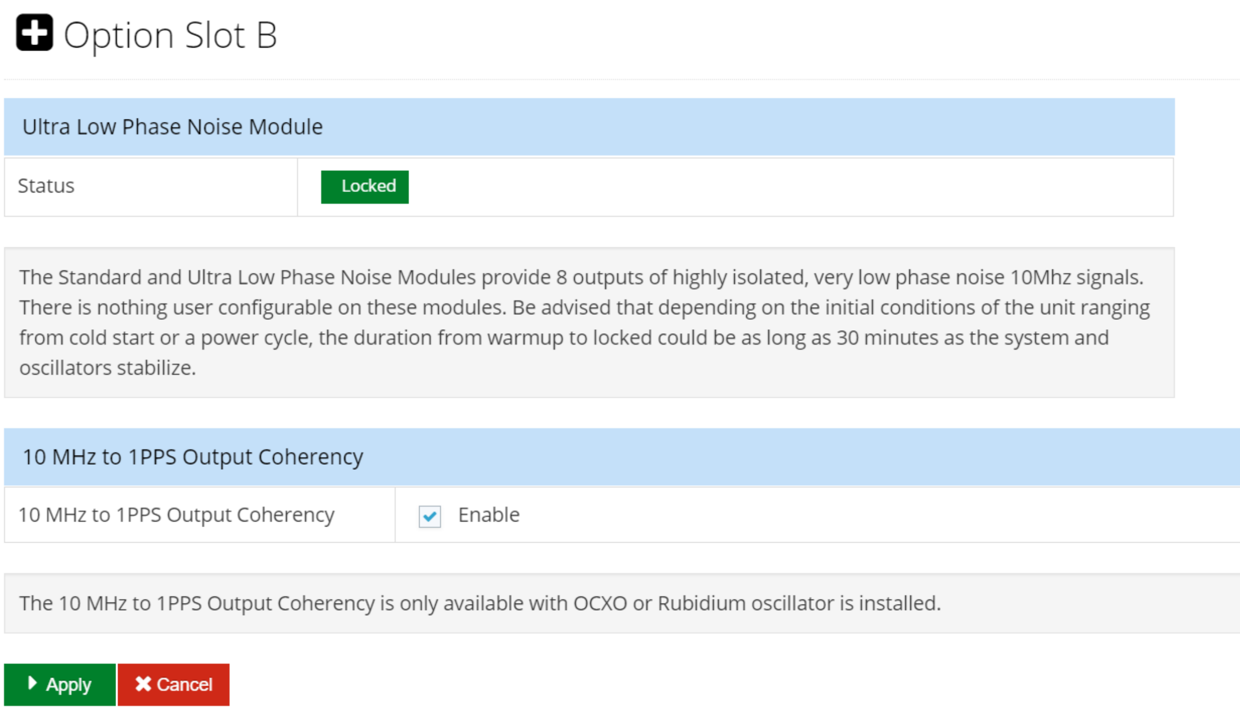


Figure 5-85. Slot B - LPN



Note: During initial lock and holdover recovery, there may be phase adjustments to the system 1PPS. The 1PPS to 10 MHz coherency will be affected while the LPN/ULPN outputs slew to the new 1PPS phase.

5.7 Help Windows

5.7.1 About Window

Use this window to view information about the unit. See the image below.

Figure 5-86. Help - About Window

About

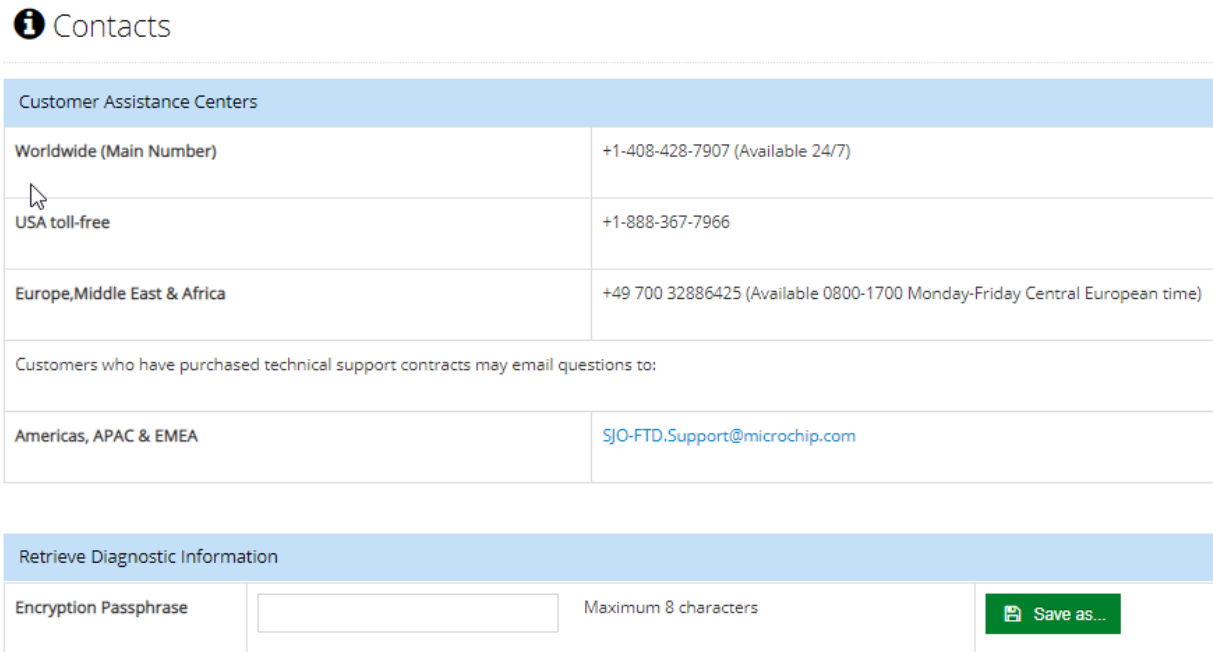
System Inventory		
Model	SyncServer S650	
Product Number	090-15200-650	
Configuration Code	650-02-00-00-06-07-0000000000FD	
Serial Number	RKT-15015583	
Hardware Version	A02	
IO Module Slot A	Timing I/O + Fiber Input	
IO Module Slot B	Timing I/O + Fiber Output	
GNSS Receiver	GPS, GLONASS, BeiDou, QZSS capable	
Oscillator	Standard	
Oscillator Additional Info		
Power Supply	Dual AC	
10G Card	Not Installed	
Ethernet MAC	LAN1	00:B0:AE:00:34:D1
	LAN2	00:B0:AE:00:34:D2
	LAN3	00:B0:AE:00:34:D3
	LAN4	00:B0:AE:00:34:D4

System Information		
Hostname	SyncServer	
Software Version	4.0.6	
GNSS Receiver Firmware	2.20 (81289)	
FPGA	Mainboard	67
	IO Module	Slot A: 51, Slot B: 51

5.7.2 Contact Window

Use this window to view information about how to contact Customer Assistance Centers. See the following image.

Figure 5-87. Help - Contacts Window



6. Provisioning

This chapter describes the procedures for provisioning the SyncServer S6x0. Use these procedures after you have installed and powered up the SyncServer S6x0 (see Chapter 2: Installing).

6.1 Establishing a Connection to the SyncServer S6x0

There are four ways to bring the SyncServer S6x0 on line:

1. The SyncServer S6x0 default IPv4 address for port LAN1 is 192.168.1.100, the subnet mask is 255.255.255.0, and the gateway address is 192.168.1.1. These may be suitable.
2. Use the front panel to input the IP address, subnet mask and gateway.
3. Use the front panel to turn on DHCP and review the assigned address.
4. Use the serial port

6.1.1 Communicating Through LAN1 Ethernet Port

The LAN1 Ethernet port must be set to an IP address that is compatible with your network to allow communication. If the default IPv4 address (indicated above) is not acceptable, you must first configure Ethernet LAN1 port through the EIA-232 serial port with CLI commands or with the front panel.

Once the LAN1 port has been configured, it can be used to access the SyncServer S6x0 web interface. Connect the LAN1 port to your network with a CAT5 Ethernet cable. Enter the LAN1 port IP address into a web browser. Enter your user name and password for the SyncServer S6x0 when prompted.

Note: The default user name is “admin”. The default password is:
Microsemi.

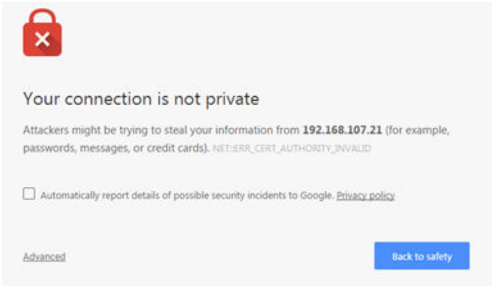
To avoid unauthorized access, you should change the default password. When logging in for the first time, or after a factory default, the system will force you to change the password.

6.1.1.1 HTTPS

A certificate is required with HTTPS. The SyncServer S6xx uses a self-signed certificate rather than a certificate generated by a known certificate authority. Browsers will therefore give warnings when attempting to connect to the SyncServer S6x0. Users will need to allow the browser to continue. The actual messages and screens will be different for different browsers. Certificates have an expiration date. After the built-in certificate expires, a new certificate can be generated on the Security->https page.

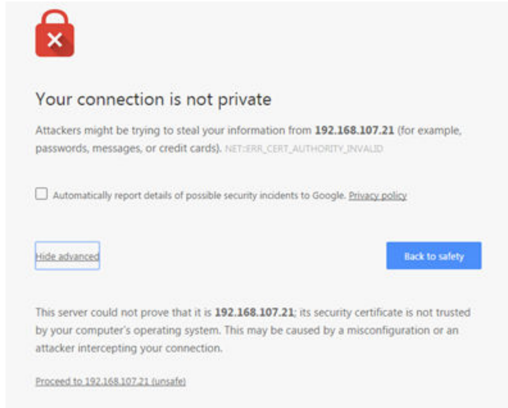
The following image shows an example HTTPS message from the Google Chrome browser.

Figure 6-1. Example - Chrome Browser HTTPS Warning



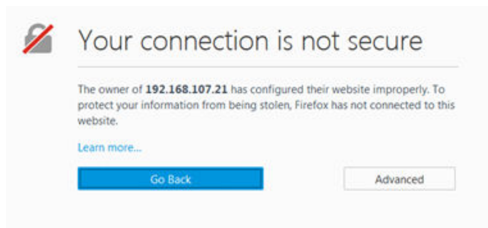
Clicking the Advanced button brings up the message shown in the following image.

Figure 6-2. Example - Chrome Browser HTTPS Warning, Advanced



The following image shows an example HTTPS message from the Mozilla Firefox browser.

Figure 6-3. Example - Firefox Browser HTTPS Warning



Clicking the Advanced button brings up the message shown in the following image.

Figure 6-4. Example - Firefox Browser HTTPS Warning, Advanced

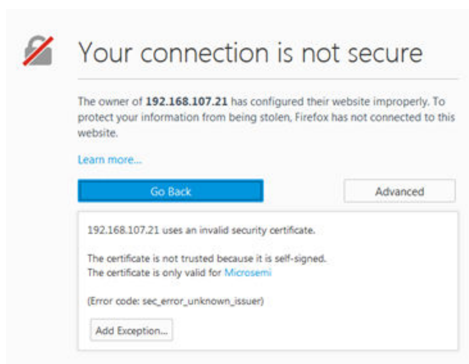


Table 6-1. Configuring the LAN1 Port

Method	Steps	Notes
Web Interface Path	Network > Ethernet	
CLI Command	`set ip ip-address lan1 ipv4 address <addrv4_value> netmask <maskv4_value> gateway <gatewayv4_value>` set ip address-mode lan1 {ipv4|ipv6} dhcp	

...........continued		
Method	**Steps**	**Notes**
Front Panel	Menu button Select “1) LAN1” Select “1. Configure” Select “1) IPv4” or “2) IPv6 (DHCPv6) If IPv4, select Addressing Type “1) Static Addr” or “2) DHCP” If IPv4 Static Addr, • enter IPv4 address and press Enter button • enter netmask and press Enter button • enter gateway and press Enter button	This method can only be used to configure LAN1.

6.1.2 Communicating Through the Serial Port

An EIA-232 serial port is available on the rear panel for a direct serial connection to a terminal or a computer with terminal emulation. Use the following procedure to connect the SyncServer S6x0 to a terminal or a computer with terminal emulation via a straight through serial cable:

Note: For information on restricting user access, see the following topic, Managing the User Access List..

1. Connect one end of a straight through serial cable to the serial port on the computer or terminal and the other end to the EIA-232 connector labeled “Console” on the rear panel of the SyncServer S6x0.
2. Configure the emulation software for 8 data bits, 1 stop bit, no parity, 115.2 kbps baud rate, and no flow control.
3. Start the terminal emulation software and press **Enter**. The system prompt should appear. If it does not, recheck each step in this procedure.
4. Type your user name and press **Enter**. The system prompts for a password.
5. Type your password and press **Enter**. The system prompt appears.
   Note: The default user name is “admin”. The default password is:
   Microsemi.

   *To avoid unauthorized access, you should change the default password.

6.2 Managing the User Access List

When you are logged in with the Web GUI, you can add, edit, or delete user names in the user access list. The user list can contain up to 15 names (in addition to “admin”). Users are required to enter a user name and password to log in to the system. All Users and Admin have the same privileges.

Use the procedures in this section to manage user access to the SyncServer S6x0.

6.2.1 Logging In

Use the following procedure to log in to the system at the admin level.

Note: The default user name is “admin” and the default password is: Microsemi .

To avoid unauthorized access, you should change the default password. When logging in for the first time, or after a factory default, the system will force you to change the password.

6.2.2 Adding a User

Use the following methods to add a user to the system access list.

Table 6-2. Adding a New User

Method	Steps	Notes
Web Interface	Security > Users 1. Enter New Username 2. Enter New Password 3. Retype New Password 4. Use radio buttons to select the desired type of password recovery question 5. Enter Answer to password recovery question 6. Enter email address of user for password recovery communication 7. Enter SMTP gateway IPv4 address for SyncServer 8. Send Test Email. 9. Click the **Apply** button	
CLI	n/a	
Front Panel	n/a	

Notes: The User name can only have alphanumeric characters, hyphen, and underline, with a maximum of 32 characters. Alphabetic characters in User names must be lowercase.

- abcdefghijklmnopqrstuvwxyz
- 0123456789
- -_

There is a maximum of 16 users, including admin user.

Notes:

- Passwords must be at least 8 characters (maximum of 64 characters), and need to include at least 1 upper-case, 1 lower-case, 1 number, and 1 special character.
- The following characters are not allowed: (', “, <, >, &,), $

6.2.3 Deleting A User

Use the following methods to delete a user from the system access list. Do not delete the default username and password.

Table 6-3. Deleting a User

Method	Steps	Notes
Web Interface	Security > Users 1. Select the user to be deleted with User dropdown box 2. Click the Delete Selected User box. 3. Click the **Apply** button.	
CLI	n/a	
Front Panel	n/a	

6.2.4 Changing a User’s Password

Use the following procedure to change a user’s password.

Notes:
- Passwords must be at least 8 characters (maximum of 64 characters), and need to include at least 1 upper-case, 1 lower-case, 1 number, and 1 special character.
- The following characters are not allowed: & < > ' “

Table 6-4. Changing a User’s Password

Method	Steps	Notes
Web Interface	Security > Users 1. Select the user with User dropdown box 2. Enter the new password in the New Password box 3. Enter the new password in the Retype New Password box 4. Click the **Apply** button.	
CLI	n/a	
Front Panel	n/a	

6.3 Provisioning the Ethernet Ports

6.3.1 Ethernet Auto-Negotiation

The Ethernet ports LAN1-LAN6 ports can be configured to allow automatic negotiation of their connection speeds. When the Speed setting for a port is set to “Auto” (default), auto-negotiation is enabled and the SyncServer S6x0 will advertise connection speeds of 100/1000M. The user can also select a connection speed for a port of 100M or 1000M to configure the speed used by auto-negotiation.

6.3.2 IP Version

The Ethernet ports LAN1-LAN6 ports can be individually configured for an IPv4 and/or IPv6 address. Use the dot-decimal notation format xxx.xxx.xxx.xxx to enter the IPv4 address parameter.

6.3.3 Configuration - DHCP or Static

The SyncServer S6x0 supports static as well as dynamically allocated IP addresses on the Ethernet ports LAN1 - LAN6. For a dynamically allocated address with the DHCP setting, a connection to a DHCP server is required. In Static mode, the user must configure the IP parameters (Host Address, Subnet Mask, and Gateway Address) for the Ethernet port.

Note: The LAN1 interface should not be configured with the same address as any of the other Ethernet ports. If this is done, then network access could be lost to the LAN1 management interface.

All Ethernet Interfaces (LAN1, LAN2, LAN3, LAN4, LAN5, LAN6) must be configured to be in different subnets/ networks. If any two or more IP interfaces have the same subnet, those interfaces will not function properly.

Note: If using a gateway, then all IP interfaces should be configured with the proper gateway IP address and subnet mask. If not using a gateway, then configure the SyncServer S6x0 to not use a gateway by leaving the gateway address blank on the GUI. If a gateway address is programmed on LAN1, then the gateway/router must be present and reachable for the port to operate normally.

Note: The SyncServer will not use a new DHCP server until the current DHCP lease expires. To force the SyncServer to acquire a new DHCP address from a new DHCP server, temporarily configure the LAN port to a static IP address, and then reconfigure the port to DHCP.

Table 6-5. Setting Ethernet Port Parameters

Method	Steps	Notes
Web Interface	Network > Ethernet 1. Select the speed with Speed dropdown box for the desired port 2. Select the IP address type by clicking on the IPv4 check box 3. Enter the IP address using the dot-decimal notation format xxx.xxx.xxx.xxx 4. Enter the Subnet mask using the dot-decimal notation format xxx.xxx.xxx.xxx. For IPv6, enter the prefix length. 5. Enter the Gateway address using the dot-decimal notation format xxx.xxx.xxx.xxx. 6. Click the **Apply** button.	
CLI	`set ip ip-address lan {1|2|3|4|5|6} ipv4 address <addrv4_value> netmask <maskv4_value> gateway <gatewayv4_value>` `set ip address-mode lan{1|2|3|4} {ipv4|ipv6} dhcp`	
Front Panel	Menu button Select “1) LAN1” Select “1. Configure” Select “1) IPv4” or “2) IPv6 (DHCPv6) If IPv4, select Addressing Type “1) Static Addr” or “2) DHCP” If IPv4 Static Addr, • enter IPv4 address and press Enter button • enter netmask and press Enter button enter gateway and press Enter button	Can only be used to set parameters for LAN1.

6.4 Provisioning Input References

When operating in normal (locked) mode, the SyncServer S6x0 uses an external reference, such as GNSS, to acquire the frequency and/or TOD alignment. Selection among multiple references inputs is based on priority.

The SyncServer 6x0 does not contain a battery-backed real time clock. Therefore, it will always boot up with a default value for the system time. This time will be updated when it obtains time from a time reference such as GNSS, IRIG, or NTP. The default value for the date is the software build date. This date will be used for the first log entries when booting up the unit. The time will change to local time during the boot-up process if a time zone has been configured.

The system will monitor all inputs and determine if there is a valid signal on each input. The system only uses one reference at a time. The highest priority valid input will be used. This is specified in the . Each reference has a different priority - the slot A and slot B references will have different priorities. With release 2.1, the priorities can be changed. All releases allow individual input references to be enabled/disabled. A frequency reference is only used if there are no valid timing references.

6.4.1 Setting GNSS Parameters

When the GNSS reference is enabled, you can set the satellite position parameters either automatically with Survey mode, or manually with Position Hold mode. The GNSS reference input is enabled by default.

In Position Hold mode, you must specify the latitude, longitude, and height. Position Hold mode should not be used unless antenna location has been accurately surveyed.

You can specify the elevation mask which provides a method to filter out satellites used in the timing solution based on elevation (0 = horizon, 90 = direct overhead). The mask selection eliminates satellites smaller than the selected mask value.

You can also specify the cable delay.The effect of the entered value is to move the positioning of the rollover of the second (e.g. PPS) earlier by the value entered, thereby accounting for the delay associated with antenna and cable. See Table 10-1 for cable-delay values for Microchip GNSS antenna kits and accessories.

Note: It is important the cable delay be configured with the proper value. This can be determined from the cable length and the delay of the antenna.

Use the following methods to provision the GNSS port state and GNSS parameters for the SyncServer S6x0.

Table 6-6. Enable GNSS Port and Set GNSS Parameters

Method	Steps	Notes
Web Interface	Timing >Input Control 1. Select radio button for External Input Sources. 2. Click the GNSS check box. 3. Click the **Apply** button.	Enable GNSS Port.
	References > GNSS Configuration 1. In the GNSS Constellation Selection section, click the check box for GPS, GALILEO, QZSS, GLONASS, or BEIDOU. 2. In the Space Based Augmentation System section, click the Enable check box to enable SBAS. 3. Click the Apply button.	Select GNSS Constellation GPS | GALILEO | GLONASS | BEIDOU | QZSS Multi-constellation license is required for BEIDOU, QZSS, GALILEO, or GLONASS access
	References > GNSS 1. Enter Elevation Mask value. 2. Use drop-down box to select Mode of “Survey” or “Position Hold”. 3. Enter Latitude value if “Position Hold” mode.Use drop-down box to select North or South. 4. Enter Longitude value if “Position Hold” mode. Use drop-down box to select East or West. 5. Enter Altitude value if “Position Hold” mode. Use drop-down box to select dimensions. 6. Enter Cable Delay value. 7. Click the **Apply** button.	Set GNSS parameters.
CLI	n/a	
Front Panel	n/a	

Note: If v3.1 or newer software is installed in an older unit, the Web GUI screen will not display Galileo as a choice. Check the Help > About window for the System Inventory. The GNSS Receiver line indicates if the GNSS receiver is Galileo capable.

6.4.2 Provisioning IRIG Inputs on Timing I/O Module

IRIG inputs are supported on Port J1 of the Timing I/O module with the SyncServer S650.

Note: A Flex Port Option license is required for full configurability of all BNC connectors on the Timing I/O module.

Note: The system will automatically detect and decode the modulation frequency of AM-modulated IRIG inputs, regardless of the configured AM modulation frequency. The clockAccuracy value will be based on the configured AM modulation frequency and not the actual input signal modulation frequency.

Note: If an IRIG input is not consistently qualified using the 50-ohm impedance, then try using the high-impedance setting.

Table 6-7. Configure IRIG or Pulse Inputs on Timing I/O Module

Method	Steps	Notes
Web Interface	Option Slot A/B > Timing I/O Card 1. In the section of the form labeled “J1 Input”, use dropdown box to select the input signal category of interest: Timecode, “Pulse”, or Off. 2. For TimeCode, use the dropdown box to select the type of IRIG input: - DCLS, without YR - DCLS, with YR - 1kHz, without YR - 10kHz, with YR - 10kHz, without YR - 1kHz, with YR - B1344, DCLS - B1344, 1kHz - 100Hz, with YR - C37.118.1 (DCLS) 3. For Pulse, use the dropdown box to select 1PPS or 10MPPS. 4. Click the **Apply** button.	Configure IRIG Input on J1 For IRIG 1344, the code performs a subtraction using control bits 14 - 19 from the supplied IRIG time with the expectation that this will produce UTC time. This aligns with the C37.118.1-2011 definition.
Web Interface	Timing > Input Control 1. In the Manual IRIG Year Input section near the bottom of the window, enter the Year. 2. Click the **Apply** button.	Manually Configure Year for IRIG Input on J1
CLI	n/a	n/a
Front Panel	n/a	n/a

6.4.3 Provisioning Sine Wave Inputs on Timing I/O Module

Sine wave inputs are available for Port J2 of the Timing I/O module with the SyncServer S650.

Note: A Flex Port Option license is required for full configurability of all BNC connectors on the Timing I/O module.

Table 6-8. Configure Sine Wave Inputs on Timing I/O Module

Method	Steps	Notes
Web Interface	Option Slot A > Timing I/O Card 1. For input J2, use dropdown box to select "Sine" or Off. 2. If sine is selected, use the dropdown box to select the frequency of the sine wave input: - 10 MHz - 5 MHz - 1 MHz 3. Click the **Apply** button.	
CLI	n/a	n/a
Front Panel	n/a	n/a

6.4.4 Provisioning T1/E1 Input on Timing I/O Telecom Module

T1 or E1 input is available for Port J7 of the Timing I/O Telecom module with the SyncServer S650.

Note: On E1 or T1 signals that support SSM, the SyncServer will decode the SSM. If the SSM corresponds to a value worse than the internal oscillator, then the signal will be disqualified. If the input signal doesn't support SSM, then the highest quality level is assumed for the input. See Chapter 13: PQL Mapping for details.
The following signals support SSM: T1 with ESF framing and E1 CAS or CCS with CRC enabled.

Note: A Flex Port Option license is required for full configurability of all BNC and RJ48c connectors on the Timing I/O Telecom module.

Table 6-9. Configure T1 or E1 Input on Timing I/O Telecom Module

Method	Steps	Notes
Web Interface	Option Slot A/B > Timing I/O Card 1. For J7 Input/Output, use dropdown box to select T1 input. 2. In the Frame Type area, click the Edit button, 3. Use the Frame Type dropdown box to select the T1 frame type: - ESF - D4 - 1.544 MHz 4. Use the SSM dropdown box to select the SSM bit. 5. Click the **Apply** button.	A Flex Port Option license is required for T1 Input on J7 connector of the Timing I/O Telecom module.

...........continued

Method	Steps	Notes
Web Interface	Option Slot A/B > Timing I/O Card 1. For J7 Input/Output, use dropdown box to select E1 input. 2. In the Frame Type area, click the Edit button, 3. Use the Frame Type dropdown box to select the E1 frame type: - CAS - CSS - 2.048 MHz 4. Use the SSM dropdown box to select the desired SSM bit. 5. To enable CRC, click the Enable box for CRC State. 6. Click the **Apply** button.	A Flex Port Option license is required for E1 Input on J7 connector of the Timing I/O Telecom module
CLI	n/a	n/a
Front Panel	n/a	n/a

6.4.5 Provisioning HaveQuick Input on Timing I/O HaveQuick/PTTI Module

Along with support for all time and frequency input capabilities (including time-interval measurement and event timestamping if Time Interval Measurement license is installed) that are associated with the standard timing I/O module (090-15201-006), additional input reference support is provided for HaveQuick timecode inputs along with an associated precise PPS input. The specifically supported HaveQuick codes are:

- ICD-GPS-060A. This is the originating Havequick code defined in document of same name. See figure 8 and associated descriptions in that document.
- HaveQuick Extended (STANAG 4430). This code adds leap second content (compared to ICD-GPS-060A).
- HaveQuick II (STANAG 4246). This code is the same as ICD-GPS-060A but removes the 8 TFOM bits at the end of the code.

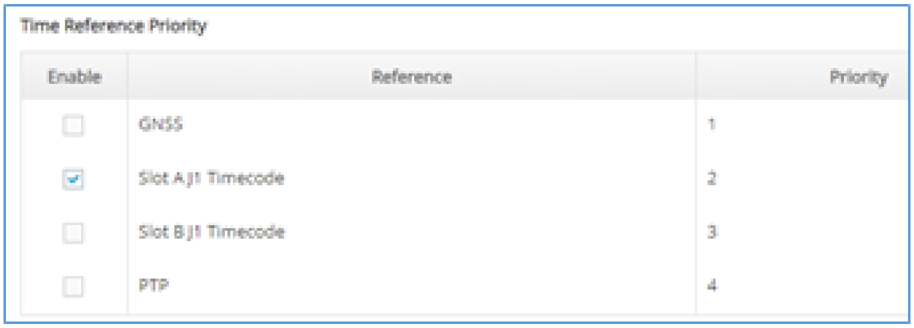
Whichever code is selected it is connected to BNC at J1. The function is to provide time-of-day information into the S6xx.

Precise alignment is provided with a PPS input on the J2 connection. The J1 and J2 inputs are used cooperatively to establish “wall clock” time (J1) with high-precision (J2).

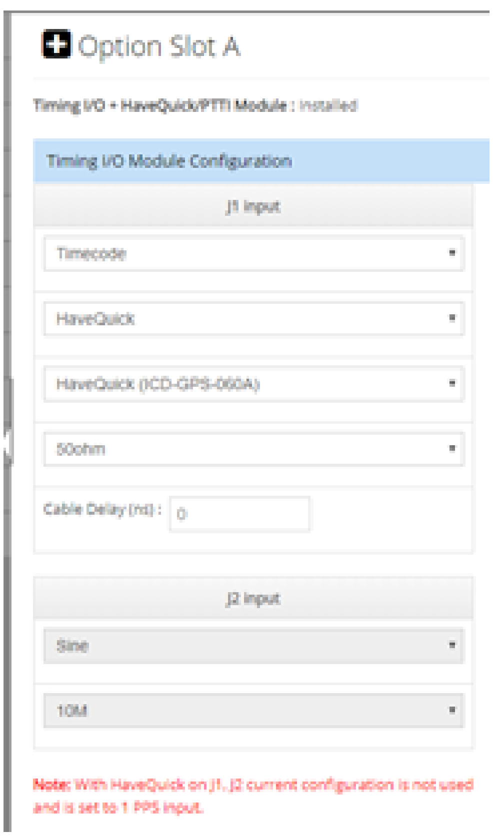
Using the Web Interface, the following steps are used to synchronize time from any of these codes:

1. As with any synchronization input to S6xx, the input must be enabled. This is always accomplished on the Timing > Input Control form. The figure below shows the relevant portion of the form. In this case since the HaveQuick/PTTI module is in slot A, only the Slot A J1 Timecode needs to be enabled.
   Select Apply to complete the configuration.

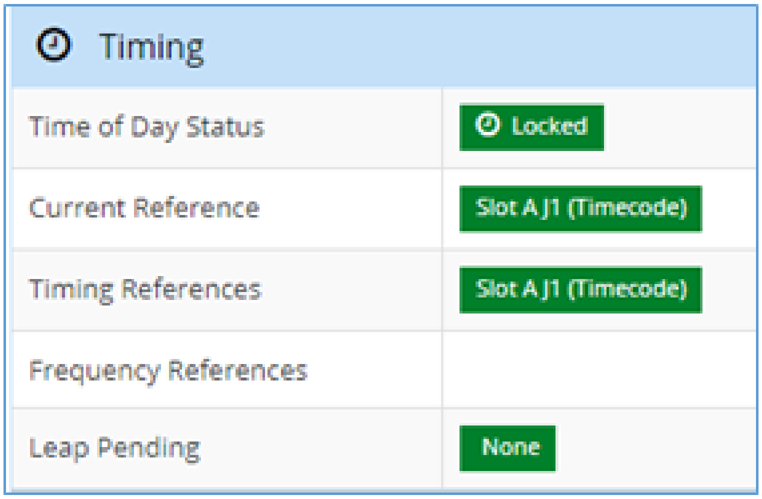
   Note: As will be seen, when J1 is configured for a HaveQuick input, J2 is automatically configured to expect an associated PPS input. There is no need to enable J2 on this form.



2. The specific input configuration is completed on the module configuration form. Since the HaveQuick/PTTI module is in slot A on this S6xx, the navigation is OPTION SLOT A > Timing I/O + HQ/PTTI. Only the relevant portion of the form is shown below.
   – The top selection for J1 is shown as Timecode. If something else is in this list box, change it to Timecode.
   – The 2nd J1 box shows HaveQuick. If something else is in this list box, change it to HaveQuick.
   – Given that the 1st and 2nd list boxes are set as shown, the 3rd box can be set to any of the supported HaveQuick codes.
   – Notice that J2 input is grayed out. No selections are possible whenever HaveQuick is selected for J1. This is because with HaveQuick on J1 a PPS input is the only allowed (and required) input for J2. Rather than force an explicit configuration, the note in red below the J2 input controls explains this situation. This approach also has the benefit that any other configured use of J2 (when relevant) remains configured when needed.
   – Since the precise alignment comes from the PPS on J2, the cable delay control on J1 (bottom control for J1) is used to compensate cable delay on the PPS connection at J2. For example, if 100 ns is entered, this will cause the synchronization of the J2 PPS to be moved earlier by 100 ns compared with the PPS rising edge arriving at J2.
   Select Apply to complete the configuration.



Assuming that appropriate inputs are being provided to J1 and J2, the S6xx will lock to this source of time. The status can be seen on the References > Status form and most comprehensively on the Dashboard > Timing form, shown below. Note that only J1 is indicated here (which is where the HaveQuick code is connected), but the J2 PPS input is also part of this combined reference and is required to obtain lock. Note that if there is no J2 PPS an LOS alarm will set.



Note that this module supports outputs that are compatible with these inputs, so it is possible to use another S6xx that has a HaveQuick/PTTI module as a source to evaluate the capability.

6.4.6 Provisioning PTP Client Input

The LAN2 - LAN6 ports can be configured as PTP Client inputs with the SyncServer S650.

Note: A PTP Input Option license is required for this feature.

Table 6-10. Configure PTP Client Inputs

Method	Steps	Notes
Web Interface	Network Timing > NTPr/PTP Config 1. In the “ADD NEW” row, enter the User-Defined Name for the service. 2. In the “ADD NEW” row, use the Service dropdown box to select “PTP Client”. 3. In the “ADD NEW” row, use the Profile dropdown box to select desired profile. 4. To configure the PTP client, click the blue Configure icon in the “ADD NEW” row, The Configurable Parameters window will open. 5. Make desired changes to the configurable parameters. Click the **OK** button when done. 6. Click the green **ADD** button. Network Timing > NTP /PTP Mapping 7. For the desired LAN port, use the Service Name dropdown box to select the desired PTP client service. 8. Click the **Apply** button for the port being mapped.	
CLI	n/a	n/a
Front Panel	n/a	n/a

GNSS must be configured, enabled, and connected if the “Auto-Asymmetry Correction” is enabled. The asymmetry correction feature allows the system to learn and correct for asymmetry in the network between the PTP master and the PTP client in the SyncServer. If asymmetry correction is enabled without GPS, then the PTP client will only be used to adjust the system frequency and won't adjust the system time. Calibration will take at least one hour and up to two hours.

6.5 Provisioning Inputs with Manual Entry Controls

The common purpose for the manual entry controls at the bottom of the Timing > Input Control window, shown in the following image, is to provide a method to enable the S6xx to become aware of time-related status information in scenarios where ther currently is no timing input capable of providing that status. The value of this may be best understood by considering that the S6xx can simultaneously support a variety of time inputs and outputs. If a particular time input does not, on its own, provide information that is needed to fully support a different type of time output then, without the method described in this section, such an output would have to report degraded status. Each of these controls exists to “fill in a gap” that otherwise would exist and lead to degraded time output capability. Table 6-12 describes the manual entry controls. Table 6-11 summarizes all available timing inputs and any gaps they might have, identifies the manual controls that can remove any gaps, and finally outputs that utilize the specific information.

Note: This section is not about the use of the “Forced Manual Time Entry” control, which has a narrow use-mode that is described in that area of the web form..

Figure 6-5. Timing - Input Control Window - Lower Portion

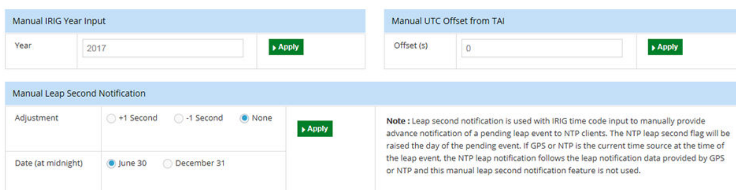


Table 6-11. Situations where use of manual time-information can allow for full capability on outputs

Input Time Reference	Information not provided by this timing reference category	Impact to outputs if not manually supplied (or provided by other qualified input)	Remedy	Notes
Any IRIG that includes current year, other than 1344 or C37.118	• No UTC offset from TAI • No pending leap	PTP: • can't set TAI timescale • can't set UTCoffsetValid flag • can't indicate pending leap NTP: • can't indicate pending leap IRIG1344/C37.118: • can't indicate pending leap	Manually set: • utc offset • pending leap	IRIG is presumed to always supply UTC timescale.

...........continued

Input Time Reference	Information not provided by this timing reference category	Impact to outputs if not manually supplied (or provided by other qualified input)	Remedy	Notes
IRIG “no year”	• No UTC offset from TAI • No Current year • No pending leap	PTP: • can't set TAI timescale • can't set UTCoffsetValid flag • can't indicate pending leap NTP: • can't provide UTC time • can't indicate pending leap IRIG1344/C37.118: • can't provide UTC time • can't indicate pending leap	Manually set: • utc offset • pending leap • current year	These IRIG codes are a subset that do not provide the current year. For standard coding of IRIGs, the codes that lack year have last digit in the range 0 - 3. If range is 4 - 7 the year is provided. For example, B000 - B003 do not provide year, B004 - B007 provide year.
IRIG 1344 or C37.118	No UTC offset from TAI	PTP: • can't set TAI timescale • can't set UTCoffsetValid flag	Manually set: • utc offset	As a practical matter, the pending leap is only for one minute, so this may not be useful for some applications - in which case manual use of pending leap can help.
NTP	• No UTC offset from TAI	PTP: • can't set TAI timescale • can't set UTCoffsetValid flag	Manually set: • utc offset	
GNSS without GPS in the constellation configuration	• No UTC offset from TAI • No Pending leap	PTP: • can't set TAI timescale • can't set UTCoffsetValid flag • can't indicated pending leap NTP: • can't indicate pending leap • IRIG1344/C37.118: • can't indicate pending leap	Manually set: • utc offset	

A simple example of this would be if the only available time input is an IRIG1344 and the S6xx is supporting a PTP (IEEE-1588) Master function. Since the IRIG input provides UTC timescale and PTP uses TAI timescale, the S6xx must convert from UTC time to get to TAI time. However, this conversion requires awareness of the current accumulated leapseconds, information the IRIG input does not supply. Without an auxiliary method for learning this value, the PTP output will encode the Announce message with the ptpTimescale flag set to false, which means that PTP clients using this S6xx PTP Master are unable to derive usable time. The remedy for this scenario is for the user to provide the current conversion value, which is easily known. By entering this in the “Manual Offset from TAI” field, the S6xx will now trust this to be the correct conversion and will apply it when it is needed to support an output. In the specific example, the time conversions are now performed (incorporating the user-supplied value), the PTP timestamps will encode TAI time, and the ptpTimescale flag is set to true.

The following table provides a summary of the function supported by each of the manual entries on this form:

Table 6-12. Manual Time Control Functions

Control	Functionality	Notes
Manual IRIG Year Input	For IRIG inputs that do not supply year, this entry supplies the missing year information. This allows time outputs that include the year to provide a user-supplied correct year.	Once supplied and accepted, the year will progress forward based on this foundation. A quick way to check if the manually entered year is being used is to look on the time in upper right of web interface or front panel of S6xx.
Manual UTC Offset from TAI	Use this control to identify the current accumulated leapsecond difference between TAI and UTC time.	TAI time is the timescale used for PTP (1EEE-1588). Unlike UTC, TAI is not affected by leapseconds, so to convert between these timescales the accumulated difference due to leapseconds must be known.
Manual Leap Second Notification	Use this control to identify that a leapsecond is pending, the direction of the leapsecond, and the date of its occurrence.	• Once supplied and accepted (and not set to “none”) indication that a leap is pending (due to manual entry) will appear on the Dashboard'Timing form. • Leap pending notifications will be provided (in the timeframe appropriate for the specific output) for any output that is capable of reporting pending leap. • Historically, all leapseconds have occurred at either midnight June 30 or midnight December 31 • After the time of the leap has passed, the leap will no longer show as pending.

6.5.1 General Behavior Associated with Manual Entry

The following behaviors apply to all of the manual entries:

- If there is currently a qualified time reference that is capable of providing that particular information, then a manual entry supplying that information will NOT be used. In other words, the information from a qualified time reference is given preference over the manual information. A list of currently qualified time references can be seen on the Dashboard > Timing > Timing References row. Any references in this row that are green are qualified. These represent the pool from which that information may be provided.
- Similarly to the prior point, if a manual entry is being used (this happens when there is no qualified input that can provide that information) and an input becomes qualified that can provide it, then the manual value will be discarded in favor of what the input is supplying. This point may help orient the foundational purpose for these controls: they are not provided to correct errors from inputs (rare), they are provided to enable a method for these values to become known when there is no current input that can supply them.
- All manual entries are acted upon immediately or not at all. In other words, at the time the value is entered, if the situation at that moment is one that will actually allow use of the value (i.e. there is no qualified time input that is already providing it), then the value will be used (be applied on time outputs as needed).
- The S6xx features the capability to remember the last status that was in use for each of these manual controls. This way, there is a good chance the values will still be correct if power is cycled in a situation where some of these values are not being actively updated by a qualified time reference. This would be the case if only an IRIG (or NTP) was providing time input. On this point, it is important to realize that:

– Even if using a manually entered year, the year will increment correctly at the end of the year. This means that on power-cycle the year that will be used won't necessarily be the value that was entered but will also incorporate any year increments that had taken place while operational.
– If using a manually entered pending leap, if the time when the leap is scheduled to occur has not yet occurred when power is cycled, upon power-up the S6xx will remember that a leap had been pending. However, upon discovery of the current time if it turns out that the time for the leap has passed, then the pending leap will be turned off. Of course, if on subsequent power-up a time reference is provided that can supply leap pending status, then the condition will entirely be based upon that status.
– If using a manually entered UTC offset, this value will be updated in the appropriate direction if a leap event occurs (i.e. the time of a pending leap happens). In this way, the UTC offset can increment even when it was originally entered manually and is not being directly updated by any external time reference.

6.5.1.1 Manual Entry Example

The example below illustrates the "pooling" behavior that ALL qualified time inputs (not just the selected time reference) are used to learn current status for any of these manual entries. In this case, two IRIG inputs are initially enabled; the specific configurations shown in Figure 6-6 (access this form via References„³Status). Note that the IRIG input configured for slot A does NOT provide the year whereas the IRIG input configured for slot B does provide the year. Initially, only the no-year IRIG is actually supplied (this is why it is green and the slot B J1 input is red). Figure 6-7 shows the status from the Dashboard„³Timing form. Since the only qualified (and selected) reference does not provide the year (or pending leap or UTC offset) information, the user can provide this information. On the manual inputs portion of the Timing > Input Control form (Figure 6-8) an action is taken to provide all of these values. For this example, they are intentionally provided with wrong values in order to illustrate the behavior when inputs are added later that provide the correct information. Of course, in actual usage (where only the input shown is available) the correct information should be provided.

With only the IRIG no-year input qualified (Figure 6-7) the values shown in Figure 3 were entered. The effectiveness of each of these entries can be seen by the following methods:

- The manually entered year was accepted as can be seen in the upper right of the web application. All time outputs that provide year information will now be providing this year.
- The manually entered pending leap was accepted as can be seen on the Leap Pending row. Outputs that supply pending leap information indicate pending (and direction of the leap) at the time appropriate for those outputs (see section titled Reporting of Leapsecond Pending).
- In release 2.0, the only output that is not based on UTC timescale is the PTP (IEEE-1588) master capability. If a PTP master is configured on one of the LAN ports (2-4), the current value of UTC to TAI conversion can be seen on the Network Timing„³NTPr/PTP Status form. For this example, LAN2 had been configured for PTP master function. Figure 6-10 shows a portion of the status. Note that the Current UTC offset value is shown to be 14 seconds, which is due to the manual entry (Figure 6-8). Note also that a pending leap is NOT shown even though it is indicated on Figure 6-7. This is behavior is illustrated in Figure 6-14.

Now connect the year-capable IRIG that is configured on the slot B J1 input(see Figure 6-6). Figure 6-11 shows that after this input becomes qualified, the correct year is extracted from this input, shown in the upper right of the web interface (and will be encoded onto any time outputs that provide year). Note that the time input that is currently driving the S6xx outputs is still the IRIG without year connected to slot A J1. This is because that input has higher priority. The example illustrates that ALL qualified inputs are used for extraction of the items shown on Figure 6-8. Even though the IRIG with year is not actually driving the precise synchronization output in this S6xx, it is now being used to extract the current year. Note that the year may not be immediately adjusted upon qualification of the IRIG that supplies the year, but it will happen within a few minutes. The message log will provide an entry when the timeline shift occurs. Here¡¦s an example:

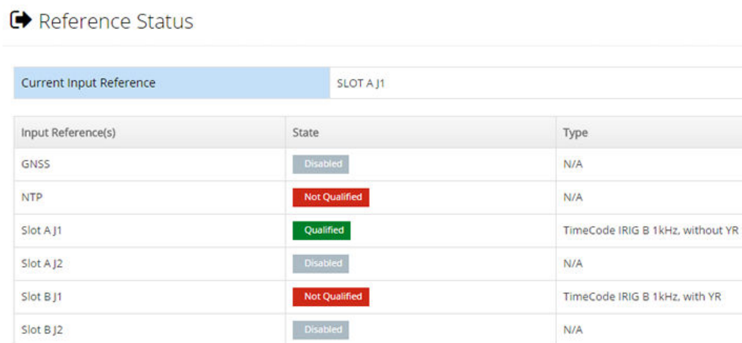
```
Jan 30 18:46:28 SyncServer alarmd: id 152, index 000, severity Notify ALARM SET: Timeline has
been changed
```

Continuing with this example, the year is now derived from an external input but the pending leap and UTC offset values continue to be taken from the user-entry since the IRIG input on BJ1 does not provide these items either. Since GPS provides all the information, if we provide GPS as an input these remaining items will be driven by the status provided via GPS. Since the manual values were intentionally set incorrectly for this example, they should change to the correct values as GPS comes up. Figure 6-12 Shows that with GNSS now qualified (and it is also selected in this case) the leap pending status has been updated because there is actually no pending leap, which is what the S6xx learned from the addition of the GPS input. Similarly, Figure 6-13 shows that the UTC offset is now showing 37 seconds, which is the correct value. Keep in mind in the situation that is the purpose for these manual controls, such as one where only an IRIG is available as input, then of course the manual entry for leap would have been “none” and UTC offset set to “37”, thus allowing for correct information to be encoded on time outputs even though no active input is providing it.

When GPS was connected, we can see the actions in the message log: the leap pending event is cleared, GPS becomes selected as the S6xx reference for time and frequency, the timeline is changed (due to the change in offset).

```
Jan 30 23:29:40 SyncServer alarmd: id 173, index 000, severity Notify, ALARM CLEAR: Leap
event pending cleared
Jan 30 23:29:40 SyncServer alarmd: id 022, index 000, severity Notify ALARM SET: GNSS input
time qualified
Jan 30 23:29:42 SyncServer alarmd: id 025, index 000, severity Notify ALARM SET: GNSS input
selected as frequency reference
Jan 30 23:29:44 SyncServer alarmd: id 024, index 000, severity Notify ALARM SET: GNSS input
selected as time reference
Jan 30 23:33:32 SyncServer alarmd: id 152, index 000, severity Notify ALARM SET: Timeline has
been changed
```

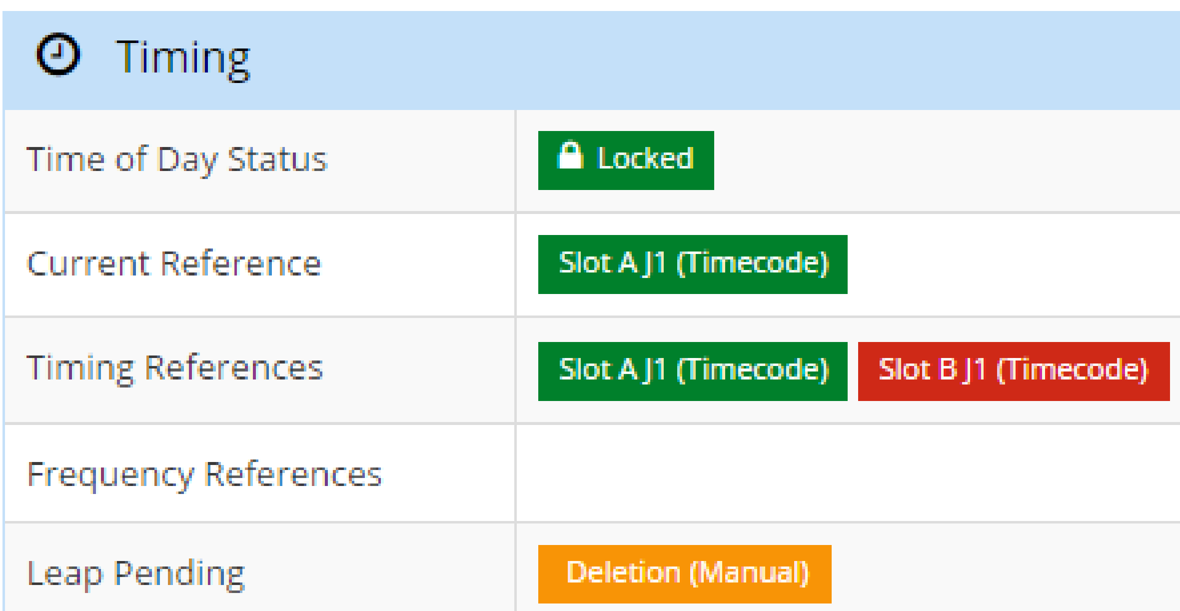
Figure 6-6. Time-Related Information is extracted from all qualified inputs


Reference Status

Current Input Reference	SLOT A J1

Input Reference(s)	State	Type
GNSS	Disabled	N/A
NTP	Not Qualified	N/A
Slot A J1	Qualified	TimeCode IRIG B 1kHz, without YR
Slot A J2	Disabled	N/A
Slot B J1	Not Qualified	TimeCode IRIG B 1kHz, with YR
Slot B J2	Disabled	N/A

Figure 6-7. The qualified (and selected) input does not provide year (or leap) information.



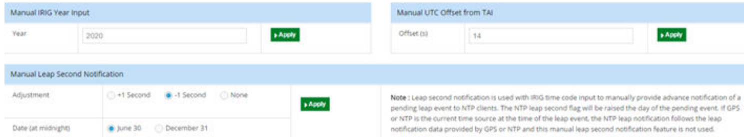


Figure 6-8. Example showing user-entry of all manual inputs

Figure 6-9. Manually entered year is being used

Figure 6-10. Portion of PTP Status

Announce Content

Port identity	00:b0:ae:ff:fe:03:7a:8d, Port:1
Clock class	6
Clock accuracy	within 10 us
Offset scaled log variance	0x3bea
Timescale	PTP
Timesource	Other
Time tracable	True
Frequency tracable	True
Current UTC offset valid	True
Current UTC offset	14 s
Leap 61	False
Leap 59	False
Steps removed	0

Figure 6-11. Qualified (non-selected) input provides year information

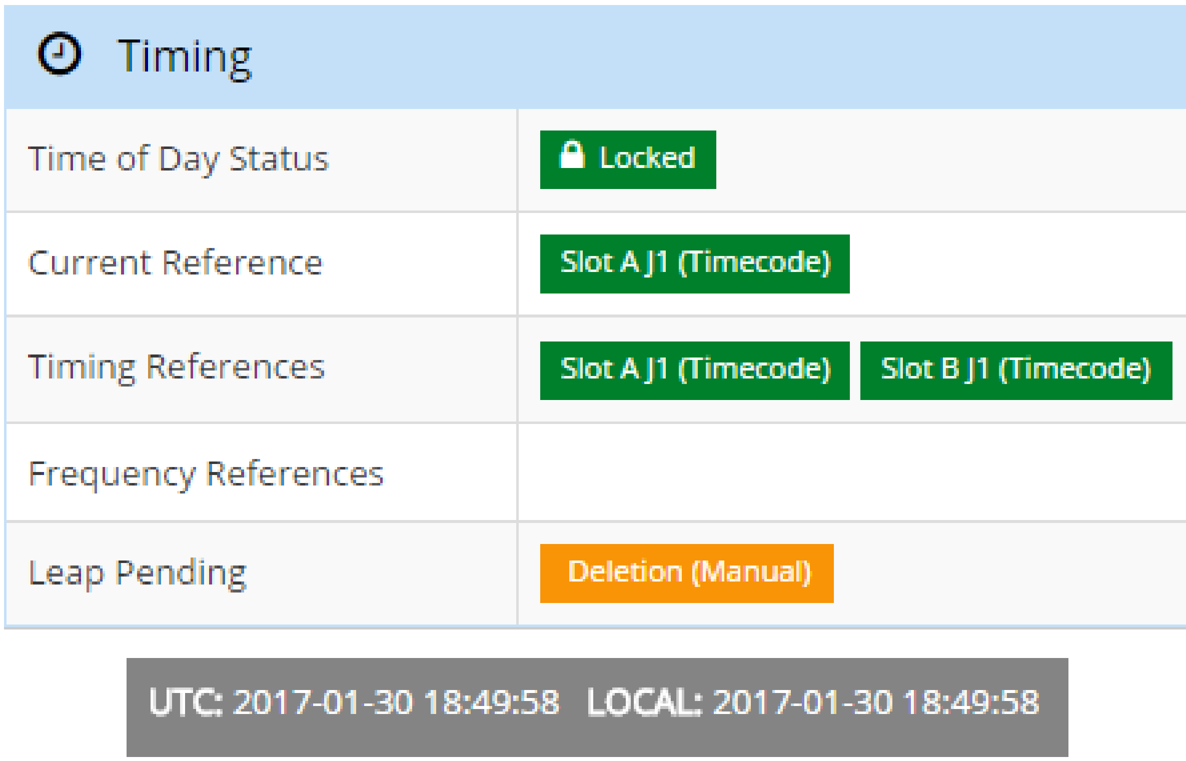


Figure 6-12. Adding GPS cleared the pending leap

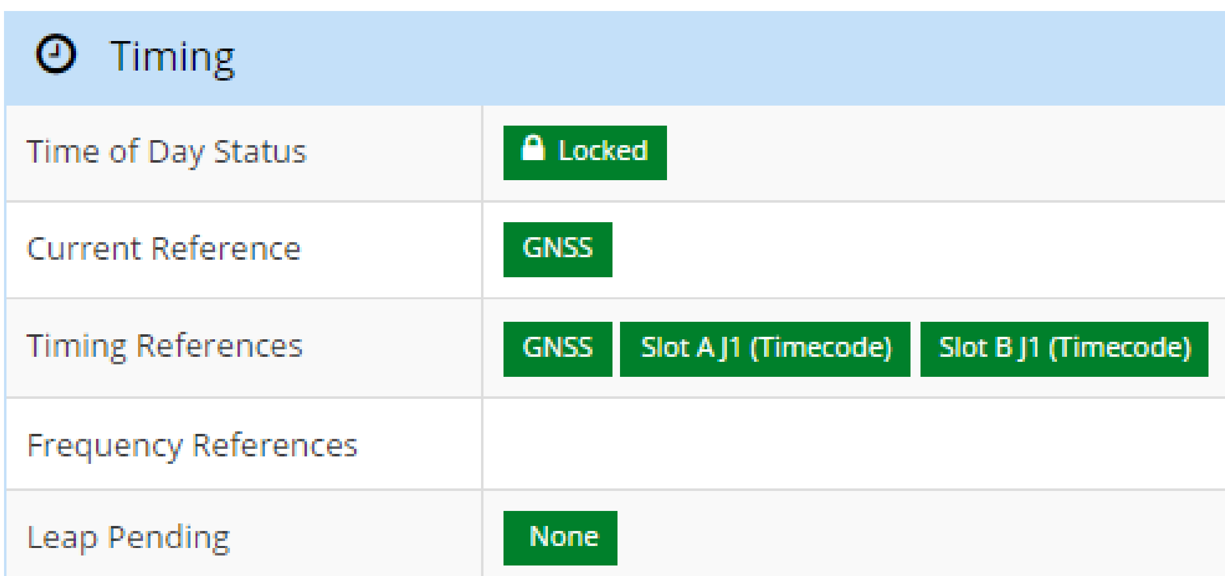


Figure 6-13. Adding GPS provided the correct UTC offset value

Announce Content

Port identity	00:b0:ae:ff:fe:03:7a:8d, Port:1
Clock class	6
Clock accuracy	within 100 ns
Offset scaled log variance	0x3bea
Timescale	PTP
Timesource	GPS
Time tracable	True
Frequency tracable	True
Current UTC offset valid	True
Current UTC offset	37 s
Leap 61	False
Leap 59	False
Steps removed	0

6.5.2 Reporting of Leapsecond Pending

The ability to provide manual entry of pending leapseconds (see Figure 3) provides benefits beyond the basic capability to inform S6xx of an upcoming leap in a circumstance where it has no way to learn of it from supplied timing inputs. The further benefit has to do with the varying rules (based on signal type) about when a pending leap should be declared in relation to the planned moment of the actual leap event. The concept is shown in Figure 6-14.

- The figure shows a timeline that terminates with the application of a leapsecond.
- The figure shows all time inputs/outputs supported in release 2.0 that are capable of providing indication of a pending leapsecond. Specifically:

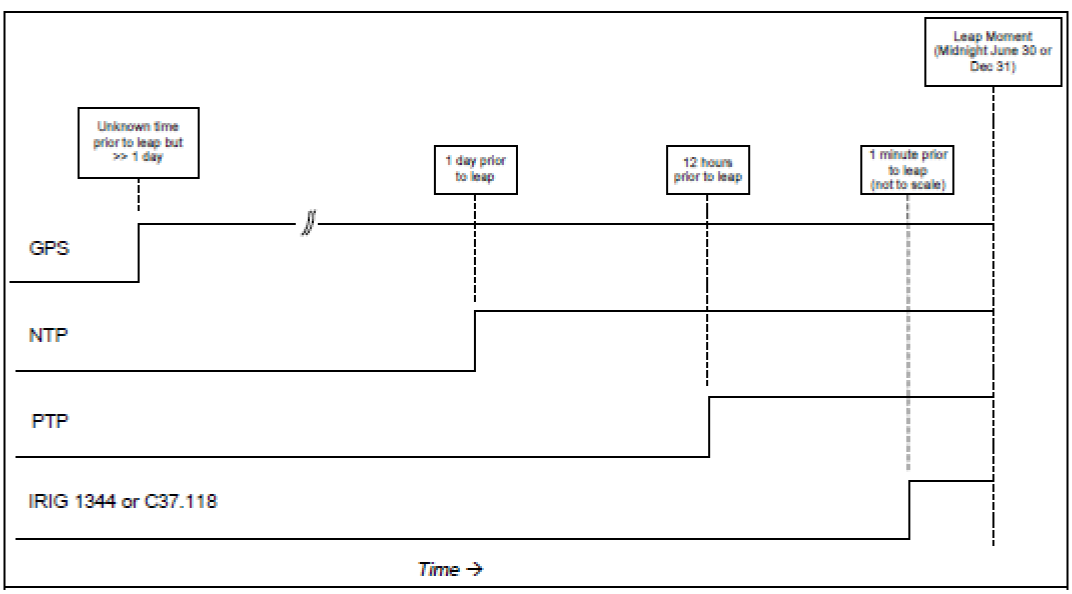
  – GPS is always one of the first sources to encode the news that a leapsecond is forthcoming. Because this input is unique in the list in that it is not also an output, there is no need to report (via GPS) to downstream devices from the S6xx that there is a pending leapsecond. For this reason, there is no limitation on how early a leapsecond may be encoded in GPS or on how early the S6xx will indicate it. This gets at a basic point that whenever the S6xx is aware of a pending leapsecond (from any source, including manual entry) this condition will be shown on the Dashboard„³Timing form. For example, in the following image a pending leap is indicated because it was entered manually (and accepted).

    There is a side-note here: release 2.0 supports multiple satellite constellation configuration. Any GNSS input whose configuration does NOT include GPS will not be capable of learning about pending leapseconds or the current UTC offset, so the discussion above is applicable only to combinations that included the GPS constellation. When GPS is not included, the manual methods for indicating pending leapseconds or setting the correct UTC offset are available.

- The other inputs (NTP, PTP (not available as an input in release 2.0), and the IRIG codes shown) have expected notification timeframes (with respect to the leap moment) as shown. What these mean is that, even if there is knowledge of a leap pending in advance of these timeframes (such as would certainly occur with a GPS time reference), the indication on an output of each type should be “held off” until within that timeframe. As shown, with an NTP output the pending leap should not be indicated any sooner than 1 day prior to the event. With PTP, the leap is held off until ½ day prior to the leap event, and finally these special IRIG codes do not announce the pending leap until the final minute before the leap event.

  You can think about how these timeframes impact each of these signal types both as an input and as an output, there are some interesting consequences:
  – When the leap pending is taken from any of these signals, it will not be detected at the S6xx (at best) until within the appropriate timeframe.
  – The S6xx will always do its best on its outputs to fulfill the complete timeframe for that output. However, what happens when the input providing the pending leap has a shorter pre-notification period than an output that is configured? For example, if the incoming signal that provides the leap notification is an IRIG 1344 and the S6xx is configured to function as an NTP Primary Server, the prenotification of the pending leap on NTP will be (at best) one minute because the IRIG 1344 won’t inform the S6xx earlier than one minute before and therefore this status cannot be conveyed on any output sooner than that.

Figure 6-14. Expected Pre-notification Times for Pending Leap Events



With the prior discussion as background the added utility of the manual leapsecond setting can be understood. First, a nuance is added to the basic behavior described for all manual entries in the section titled General Behavior Associated with Manual Entry which stated:

- If there is currently a qualified time reference that is capable of providing that particular information, then a manual entry supplying that information will NOT be used.

In the case of a manual pending leap entry, we amend this to:

- If there is currently a qualified time reference that is capable of providing leap pending information AND the time until the pending leap is within the expected timeframe for that particular input, then a manual leap pending entry will not be used.
- On the other hand, if a manual leap entry is applied before the expected timeframe for all qualified inputs in the pool, then the manual entry will be accepted. In such a case, once the time until the leap moment falls within the timeframe of any qualified input, the information supplied by that input will overrule (if needed) the manual setting.

6.5.2.1 Examples:

- If GPS is a qualified reference, manual leap pending input will never be accepted since GPS is expected to provide leap pending status (typically) many months prior to the leap moment. There is no formal definition for the timeframe but for sure there will be plenty of notice and hence there is no reason to accept a manual entry.
- If GPS is not a qualified reference, then manual control of leap will be allowed at any time except when the remaining time until leap is within the timeframe of the qualified time input shown in Figure 9 that has the longest timeframe. In this region, the inputs are expected to provide the leap pending status.
- An example where the manual input can help to provide maximum notification to all outputs occurs if IRIG 1344 is the only time input and the S6xx is operating as a PTP GrandMaster. Since the manual input is allowed all the way up to the minute prior to the leap moment, the user can manually enter the pending leap days (even weeks) prior to the leap event. Since the S6xx knows that the IRIG input won¡¦t provide any information until the last minute, the manual input is accepted. There is no problem providing the manual notification early because the S6xx knows to hold off based on the appropriate timeframe for the signal type. In this case with PTP output, the notification will appear in the PTP Announce messages . day prior to the event, just as it would have done if the input had been GPS (or even NTP).

6.6 Provisioning NTP Associations

The SyncServer can have multiple associations, each with a different Role. NTP associations with non-valid IP addresses and domain names are not shown in the Associations list. (If a known good domain name does not appear on this list, there may be a problem with the DNS server configuration or with the DNS service itself.)

Table 6-13 describes the method to add a new NTP association.
Table 6-14 describes the method to modify an existing NTP association.
Table 4-7 provides descriptions of NTP Association configuration parameters.

The list of Current NTP Associations always includes the local Hardware Clock, which:

- Cannot be deleted or edited.
- Is configured as a preferred server
(“server 127.127.47.0 prefer # pseudoaddress for the hardware clock” according to ntp.conf).
- Is displayed at the top of the list.
Note: The NTP hardware reference clock is by default marked with the NTP “prefer” setting. If the user wants to mark a different association as preferred, then the hardware clock should have the “prefer” unselected. The system will not prevent the user from setting multiple associations as “prefer”, although this is usually not useful.

The user should consider adding NTP servers available on the local network to the list of Current NTP Associations.

Note: If the system is using NTP as the reference and the NTP server is performing a leap smear, then all non-NTP outputs of the system will be degraded, especially outputs on the optional I/O modules.

6.6.1 NTP Prefer Selection

By default the SyncServer S6x0 Series has the NTP Prefer selected for the local hardware reference clock. In most operating scenarios the local hardware reference clock (which more often than not will be tracking GNSS) will be the only reference being used. With the Prefer being selected, and no statistically better reference available, the time server will achieve Stratum 1 status on startup or restart as rapidly as possible. If the Prefer is not selected for the hardware reference clock then the NTP daemon will go through a standard validation procedure for a reference clock.

This procedure will take several minutes and should happen by the time the reach indicates 377 on the reference clock association. For optimal operation, Microchip recommends the local hardware reference remain selected as a Prefer in the configuration.

.

Table 6-13. Add a New NTP Association

Method	Steps
Web Interface	NTP > NTPd Config 1. Select the Role with dropdown box as either Server, Peer, or Broadcast. 2. Enter the IP address or DNS name of the NTP association. 3. Select the Port with dropdown box, LAN1, LAN2, LAN3, LAN4, LAN5 or LAN6. 4. Click the “Prefer” checkbox to set this as a prefer association. 5. Select the Burst setting with the dropdown box as N/A, Burst, iBurst, or Both. 6. Select the MinPoll value with the dropdown box. 7. Select the MaxPoll value with the dropdown box. 8. Select the Symmetric key with the dropdown box 9. Click the **+** button in the right side column to add the association. 10. Click the **Save** button to save changes. 11. Click the **Restart** button to make any changes take effect.
CLI	n/a
Front Panel	n/a

Table 6-14. Modify Existing NTP Association

Method	Steps
Web Interface	NTP > NTPd Config 1. Select the NTP Association that is to be modified from the list. 2. Change the Role, if desired, with dropdown box as either Server, Peer, or Broadcast. 3. Change the IP address or DNS name, if desired, of the NTP association. 4. Change the Port with dropdown box, if desired, LAN1, LAN2, LAN3, LAN4, LAN5 or LAN6. 5. Click the “Prefer” checkbox, if desired, to select or deselect this as a prefer association. 6. Change the Burst setting, if desired, with the dropdown box as N/A, Burst, iBurst, or Both. 7. Change the MinPoll value, if desired, with the dropdown box. 8. Change the Symmetric value, if desired, with the dropdown box 9. Change the MaxPoll value, if desired, with the dropdown box. 10. Click the **Save** button to save changes. 11. Click the **Restart** button to make any changes take effect.
CLI	n/a
Front Panel	n/a

6.7 Provisioning NTP Security

6.7.1 NTPd Symmetric Keys

- Generate the current keys.
- Upload a file containing keys from a local PC drive to the SyncServer.
- Download the SyncServer's current key file to a local PC drive.

Use the GENERATE button to clear previous keys and generate new ones.

6.7.2 NTPd Autokey Server

Use the Security > NTP - Autokey Server page to manage (add or remove) Autokey keys for NTP associations where the SyncServer is an NTP server.

Note: Hostname of Autokey Server and Autokey client must be different. Use the Admin - General Configuration Window to set hostname..

Table 6-15. Configure NTP Autokey Server

Method	Steps	Notes
Web Interface	Security > NTPd Autokey Server 1. In the Identity Scheme IFF section, enter the Server Password. This is equivalent to the “crypto pw <server-password>” line in ntp.conf on a generic NTP device. 2. Click the **Generate** button to create the key file. 3. Click the **Save as** button to download IFF Group key file 4. Click the **Restart** button to make any changes take effect.	Configure NTP Autokey Server While the NTP daemon restarts, its services are temporarily unavailable, and it generates the following alarm events: NTP Stratum Change, NTP System Peer Change, NTP Leap Change.
CLI	n/a	n/a
Front Panel	n/a	n/a

6.7.3 NTP Autokey Client

Use the Security > NTP - Autokey Client page to manage (add or remove) Autokey keys for NTP associations where the SyncServer is an NTP client.

Note: Hostname of Autokey Server and Autokey client must be different. Use the Admin - General Configuration Window to set hostname..

.

Table 6-16. Configure NTP Autokey Client

Method	Steps	Notes
Web Interface	Security > NTPd Autokey Client 1. Browse to locate the Group Key File from a secure location. 2. Click the **Install** button to save the AutoKey Client File to the SyncServer. 3. Enter a password and click the **Generate** button. 4. Click the **Restart** button to make any changes take effect. 5. Go to Network Timing > NTPd Config web page. 6. Add role of server, and select "Auto" from Symmetric pull-down. 7. Click the **Save** button. 8. Click **Restart** button.	Install IFF Group Key File While the NTP daemon restarts, its services are temporarily unavailable, and it generates the following alarm events: NTP Stratum Change, NTP System Peer Change, NTP Leap Change.
CLI	n/a	n/a
Front Panel	n/a	n/a

6.7.4 Add NTP Server Association using Autokey Authentication

Use the Network Timing > NTPd Config page to add NTP server associations where the SyncServer is Autokey Client..

Table 6-17. Configure NTP Autokey Client

Method	Steps	Notes
Web Interface	Network Timing -> NTPd Config 1. Add a Role of Server. 2. Select 'Auto' from Symmetric pull-down menu 3. Optional step: Check 'Prefer' for newly added NTPd server association and Uncheck 'Prefer' for Hardware Reference Clock, so that newly added NTPd will be selected as input reference over GNSS. 4. Click the **Save** button. 5. Click the **Restart** button to make any changes take effect.	
CLI	n/a	n/a
Front Panel	n/a	n/a

6.8 Provisioning Outputs

6.8.1 Configuring Network Timing Services

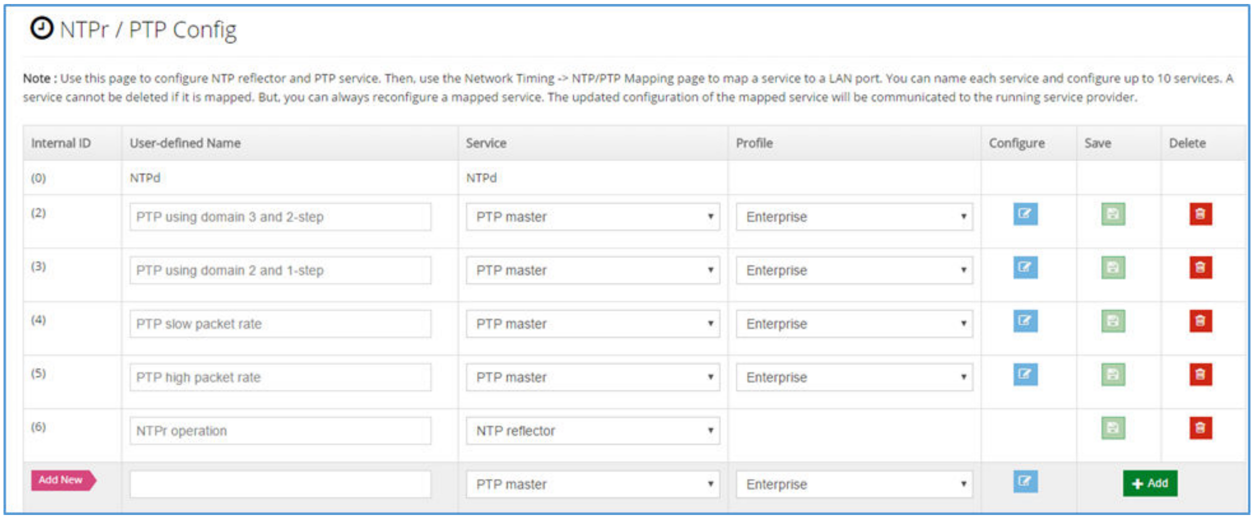
The form Network Timing > NTPr/PTP Config supports generalized configuration of network timing services. The concept is that the ability to create and retain definitions for specific services, independently of the connection method, provides a useful way to aggregate within the S6x0 all network timing services that are of interest for that particular unit. As added services are provided in future releases, this form will evolve to support extended service capabilities. Up to 10 services (rows) can be created.

To use any of the services defined on this form, map that service to the specific physical network port where it should run. This is accomplished on the Network Timing > NTP/PTP Mapping form.

6.8.1.1 Example - Creating a Network Timing Service

The following image shows the timing services configuration form. Five services have previously been configured for this example. See Table 5-8 for descriptions of the parameters (columns) in this form.

Figure 6-15. Configuration of Network Timing Services



To illustrate the process we walk through creating one more row, starting with the following image.

Suppose we want to use the S6x0 as a 1588 (PTP) GrandMaster. As part of an overall network plan, we want this one at a higher priority than another S6x0 that is providing PTP Grandmaster services in this same network. Our intent for doing this is so that if the clock quality being reported by both grandmasters is the same, then the BMCA (Best Master Clock Algorithm) executing at the downstream PTP clients will choose this S6x0 because of its better priority. Here are the steps:

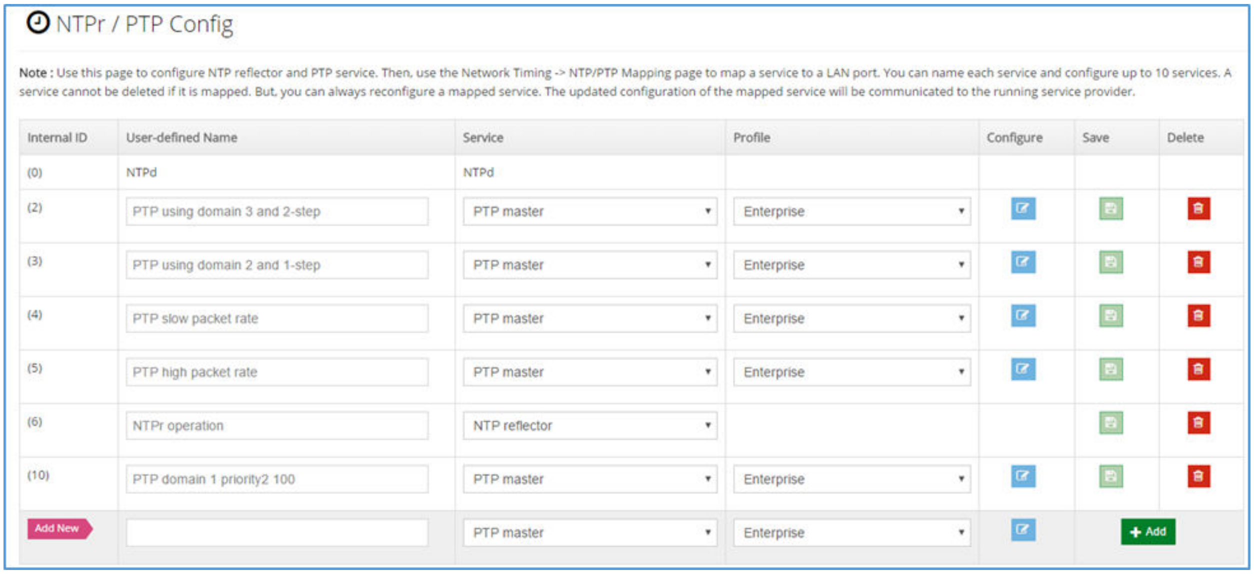
- Using the Add New row, type in a helpful name for this service. This name reminds us that this service has the priority2 setting set to 100 and the PTP domain set to 1. Both of these will be accomplished later in this example.

- At this point there are 2 ways to proceed, both essentially equivalent:
  – Select the +Add control, which will create a new row in the table. From there we can further edit to the desired specific settings. This illustrates a general feature that any row in the table can be edited, so it is not always necessary to create a new one if it is preferred to alter an existing one.
  – Alternatively, continue editing to the final configuration prior to selection of +Add. Doing it this way will result in the new row being saved to the desired settings when it is created (this will be evident since the Save control will be grayed out).

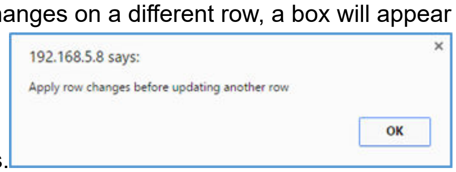
Both of these methods get to the same outcome, there is no clear advantage for either one.

For this example, the +Add control is selected now, resulting in the following image.

Figure 6-16. Example - New Timing Service Configuration



The new timing service is shown on the bottom row. Note that it was auto-assigned ID = 10, the actual value is not important. S6x0 assures that it is unique. Note also that the Save control is grayed out, indicating that there is nothing to save. However, since we haven't yet completed all of the desired configuration there is still work to do.

- Since the default values for Service and Profile columns happen to be what we want for this service, there is no need to change them. In general, if the values did need to be changed from the default, they should done in left-to-right (Service, then Profile, then Configure) order since the columns to the right will adapt based on selections to the left.
- Select the Configure control, which brings up Figure 6-17, which always begins with default values the first time a new service is created. For this example we need to change the Domain and the Priority2 values. Set Domain = 1 and Priority2 = 100, then OK. Figure 6-17 shows the configuration with these changes, just before selecting OK. This action returns back to Figure 6-16 but now the detailed configuration matches the desired setup, as described in the User-Defined Name.
- To complete the configuration, select the Save button for this row. The appearance of the form just before this save action is shown in Figure 6-18. Compare this with Figure 6-16 for the following notes:
- Figure 6-18 shows the Save button is ready to be used (it is not grayed out) and the entire row associated with the new service is highlighted. These are clues that the full configuration has not been completed. Why is that? It's because we made a change on the configuration form (and saved it with the OK) but we have not saved it at the top level (the entire timing service).
  Contrast this with Figure 6-16. Here the Save is grayed out because there are no pending changes (this was before the changes were made on the configuration form).
- If pending (unsaved) changes have been made to any row and an action is taken to make changes on a different row, a box will appear indicating that there are unsaved 

changes.
  Similarly, if there are pending changes and a new form is selected, this form will appear to make sure the action is intended.

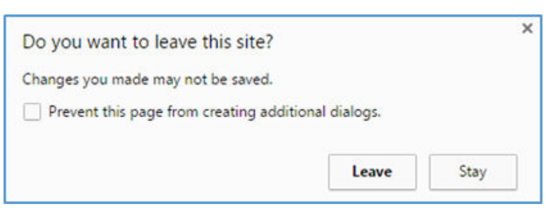


Figure 6-17. Modified configuration for “PTP domain 1 priority2 100” just before OK selected

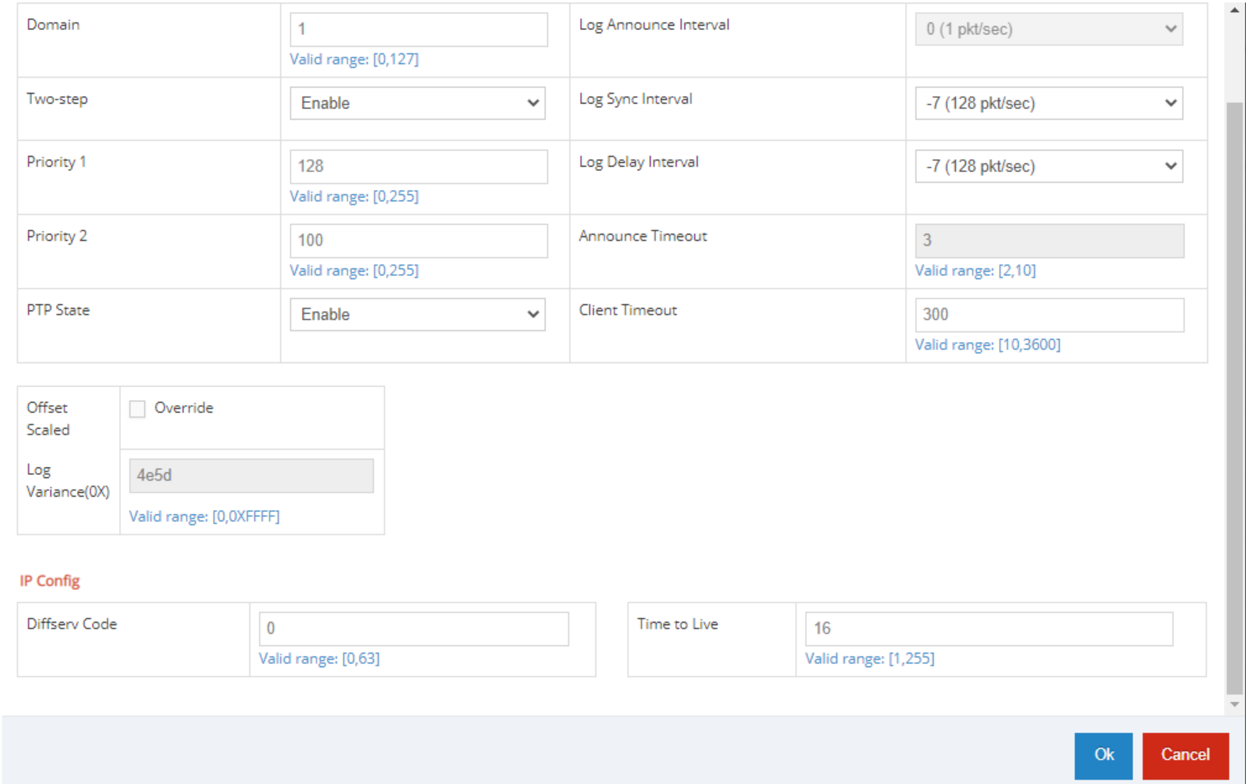
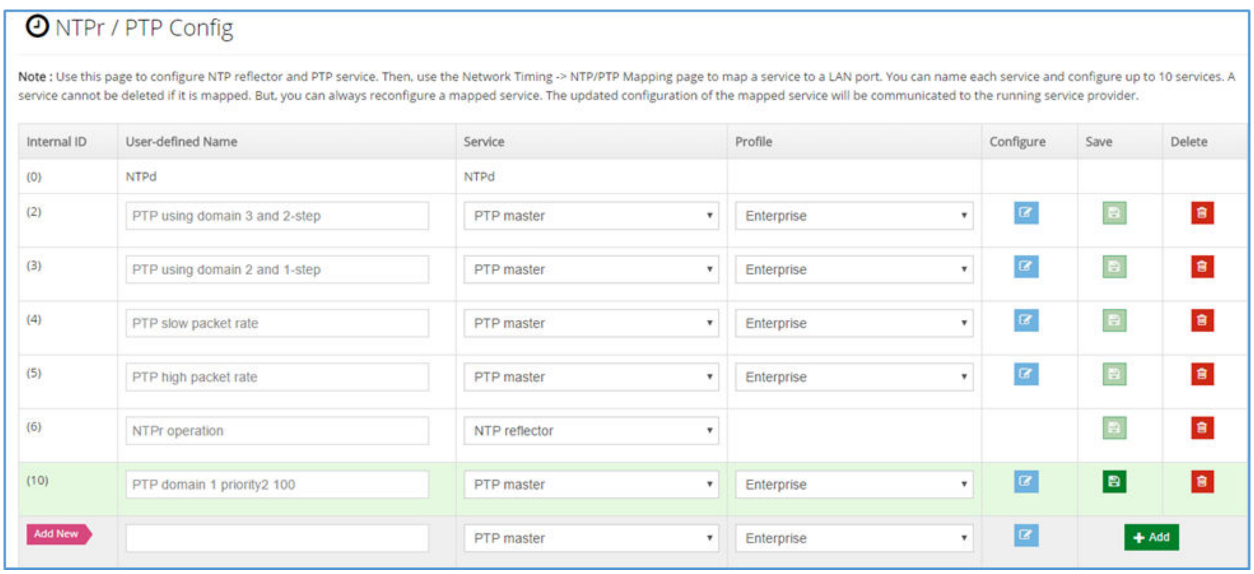


Figure 6-18. New timing service just before final save



Once a timing service has been created its configuration can be changed as desired, including the name. In other words, an existing service can be re-purposed or modified as needed.

Notice that there is a predefined row with internal ID = (0) at the top of the row portion of the following image, named NTPd. The NTPd service has always been available on S6x0 and is supported on all physical network ports. NTPd configuration is accomplished on the Network Timing'NTPd Config form. Rather than create a new method for its configuration, the existing method remains. However, as is seen in Mapping a Network Timing Service to a LAN Port, the method for mapping use of NTPd to physical network ports is consistent with all network timing services, which is why this row (non-deletable and non-configurable) appears on this form.

6.8.2 Mapping a Network Timing Service to a LAN Port

Creation of network timing services Figure 6-15 provides a customizable method for configuring specific services for use on a given S6x0. Selecting Network Timing > NTP/PTP Mapping provides the method to associate a service with the physical network port where is should operate. Figure 14 shows this form as it will appear on first power-up (factory preset).

The form lists all physical ports that support multiple timing services. This is currently LAN 2, 3, 4, 5 6). LAN1 currently supports only NTPd and is always mapped to that service, so it does not appear here. As the S6x0 capability evolves, the set of choices and assignment rules will evolve on this form. The service choices and allowed mapping rules are as described in Table 6-17. The behavior described in Table 6-17 is enforced by the form controls.

Figure 6-19. Factory Preset Mapping Form

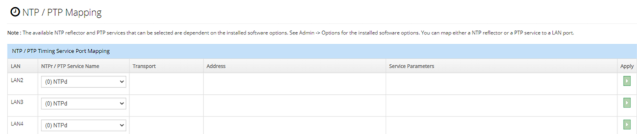


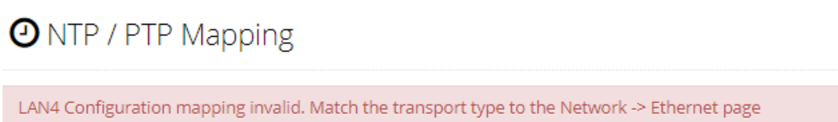
Table 6-18. Network Timing Service Mapping

Network Timing Service	Individual Mapping Rules	Combined Mapping Rules
NTPd	Supported on LAN1, LAN2, LAN3, LAN4, LAN5, LAN6	Always mapped to LAN1. Can be mapped to any combination of other ports as long as no other timing service is mapped to that port.
PTP Master	Can be mapped to any of these physical ports: LAN2, LAN3, LAN4, LAN5, LAN6	Can be mapped to any combination of ports as long as no other timing service is mapped to that port.
NTPr	Can be mapped to any of these physical ports: LAN2, LAN3, LAN4, LAN5, LAN6	Can be mapped to an allowed physical port if PTP Master is not mapped to a port.
PTP Client	Can be mapped to any of these physical ports: LAN2, LAN3, LAN4, LAN5, LAN6	Can be mapped to any combination of ports as long as no other timing service is mapped to that port.

6.8.2.1 Example - Mapping a Network Timing Service

Suppose that the goal is to provide the PTP Master service that was created (prior example Figure 6-18) on LAN4.

The first step (if not already done) is to configure LAN4 with a network configuration. This is accomplished on the Network > Ethernet form. Figure 6-20 shows an example where LAN4 has been configured to IPv4 address 192.168.100.99. Attempting to complete a service mapping to a LAN that has not been configured will result in this message:



Next, the desired service is selected from the list box in the Service Name column. Since this example maps the service to LAN4, the list box from that row is used. Figure 16 shows the selection set. This list will always show the first two columns of whatever has been configured on Figure 6-18. As will be seen, the list does not filter out selections that may not actually be allowed per the combined mapping rules column of Table 6-17; the list always shows all services that could possibly be assigned to that port.

Selection of the service associated with internal ID (10), results in Figure 6-22. Note that this row is highlighted as indication that this assignment is not actually complete. The apply button on the right of this row is now available as indication that something needs to be saved.

Selection of apply will attempt to complete the mapping. This action causes any specific mapping rules (see Table 6-17) to be enforced, which could lead to non-acceptance of the candidate entry (more about this later). In this case the mapping meets all requirements and is accepted, the form after acceptance is shown in Figure 6-23. This service is now active on LAN4.

The current mapping of network timing services to LAN ports can also be observed on the Dashboard >Timing Services form. Figure 6-24 shows how this looks with the example just shown. As can be seen this form also shows LAN1 which in 2.0 release is always mapped to NTPd.

Figure 6-20. Example configuration on Network > Ethernet form

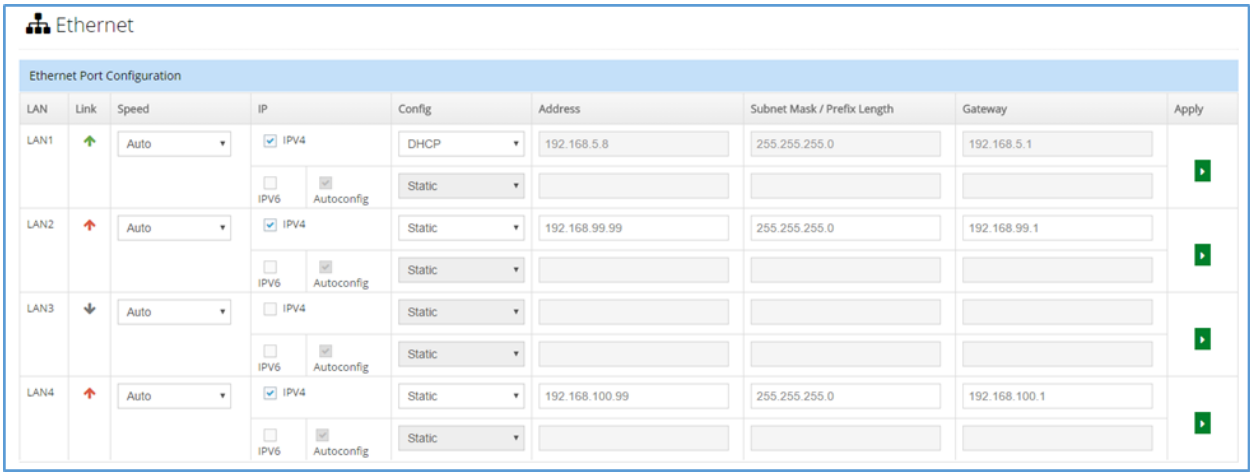


Figure 6-21. Timing Services choices appear in list box

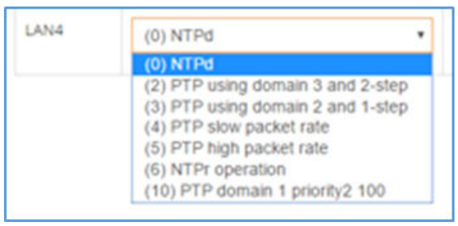


Figure 6-22. PTP Master timing service is in process of being mapped to LAN4

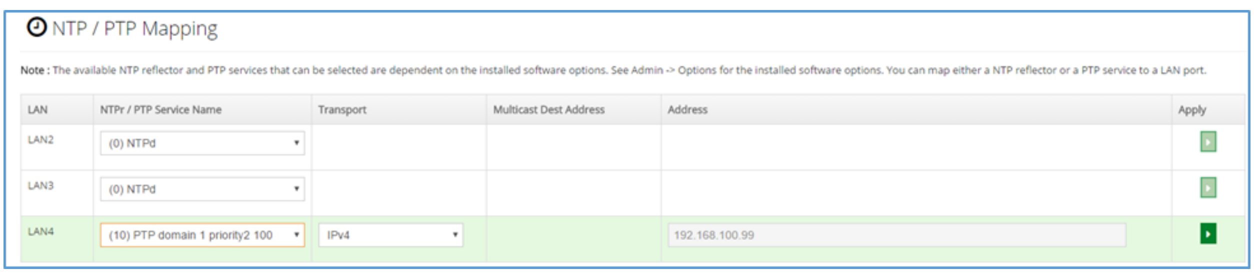


Figure 6-23. Successful completion of mapping new timing service to LAN4

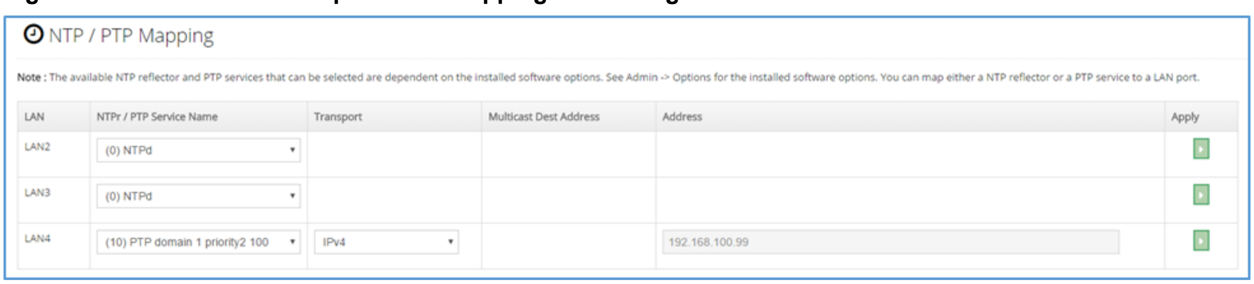


Figure 6-24. Dashboard'Timing Services shows current mapping

Timing Services

LAN	Name	Timing Service	IP
LAN1	(0) NTPd	NTPd	192.168.5.8
LAN2	(0) NTPd	NTPd	192.168.99.99
LAN3	(0) NTPd	NTPd	192.168.101.99
LAN4	(10) PTP domain 1 priority2 100	PTP master	192.168.100.99

6.8.3 Observing Status of Network Timing Services

Previous sections have covered Creating a Network Timing Service and Using a Network Timing Service. This section discusses how to observe the status of a timing service. To start with, keep in mind that a network timing service (defined on Figure 6-15) is only actually in use when it is mapped to a physical network port, accomplished on Figure 6-19. Hence the set of services that will have status are those that have been mapped to a LAN port.

There are two areas on the web interface where timing service status can be observed. For NTPd:

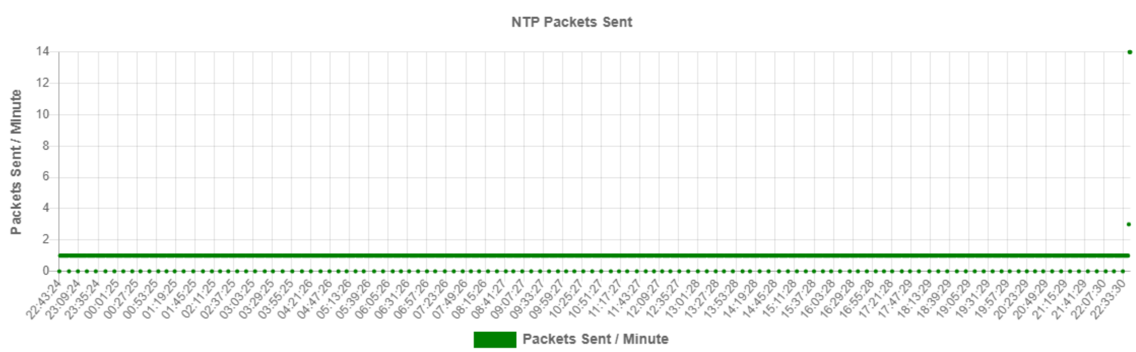
1. Network Timing > Sysinfo provides complete status, showing standard NTP parameter values. The example below shows a typical status when the hardware clock is GNSS. This status is applicable to all LAN ports that are mapped to NTPd.

   Figure 6-25. NTPd status example

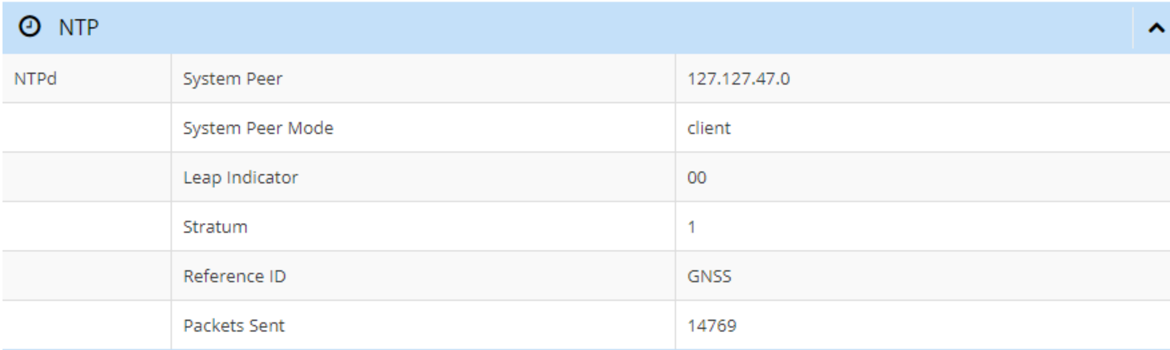
   NTPd Sysinfo

   NTP Daemon Status and Control

System Peer	127.127.47.0	Reference ID	GNSS
System Peer Mode	client	Reference Time	e3b9c7d4.e30d6e0f Mon, Jan 25 2021 22:42:28.886
Leap Indicator	00	System Jitter	0.001907 ms
Stratum	1	Clock Jitter	0.002 ms
Log2 Precision	-19	Clock Wander	0.000 ppm
Root Delay	0.000 ms	Broadcast Delay	-50.000 ms
Root Dispersion	0.004 ms	Symm Auth Delay	0.000 ms
Packets Sent	14742		

2. A summarized status is also available on Dashboard > NTP.



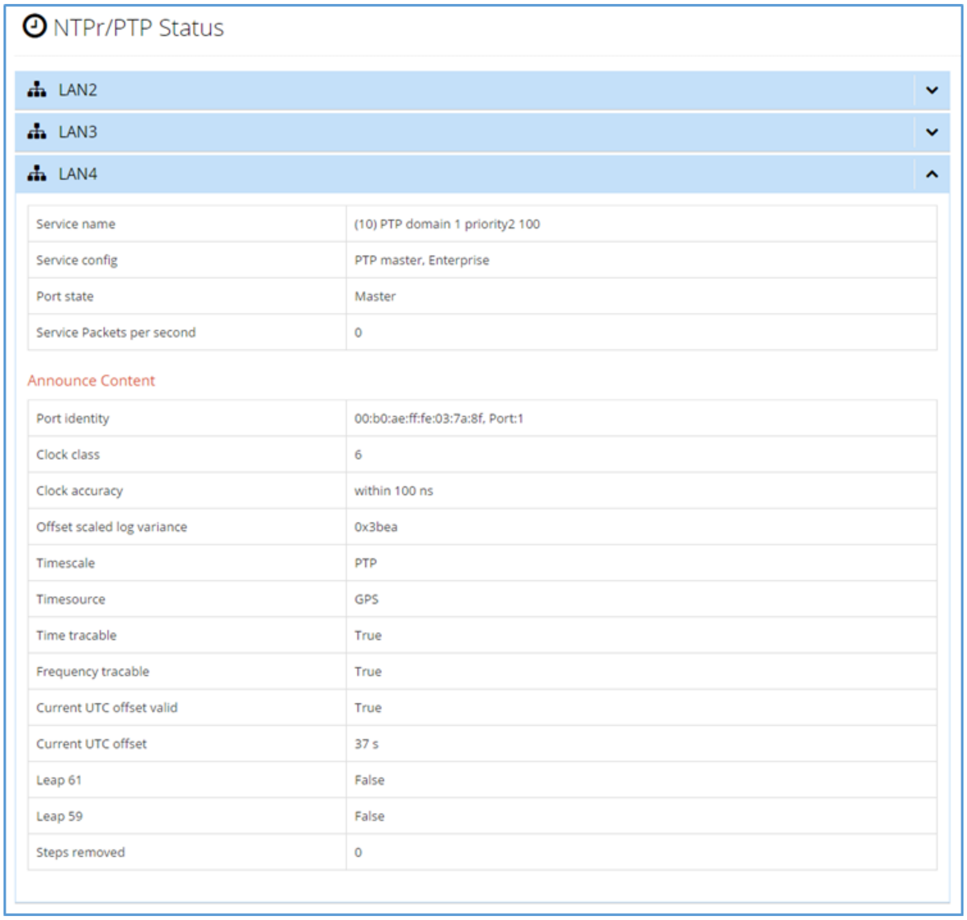
All other timing services status appears at Network Timing'NTPr/PTP Status, which provides the ability to first select the LAN to which a given service is mapped (mapping accomplished on Figure 6-23). In release 2.0 due to the rules described in Table 6-17, only one of the LANs will contain status. This form prepares for expanded capability.

Using the setup from Figure 6-23 where we have mapped a PTP Master onto LAN4, select LAN4 to observe its status. As can be seen in Figure 6-26 the specific service in use is identified (fully configured on Figure 6-18) along with general status, including details about content being transmitted in the PTP Announce messages.

A reduced set of status can be seen at Dashboard > Timing Services Status as shown in Figure 6-27.

When the mapped service is NTPr, the status provided is similar to what is seen for NTPd (see Figure 6-25). Using the example from Figure 6-26, where an NTPr service is mapped to LAN2, the status examples are shown in Figure 6-28 and Figure 6-29.

Figure 6-26. Example status on Network Timing > NTPr/PTP Status form (PTP Master)


NTPr/PTP Status

LAN2

LAN3

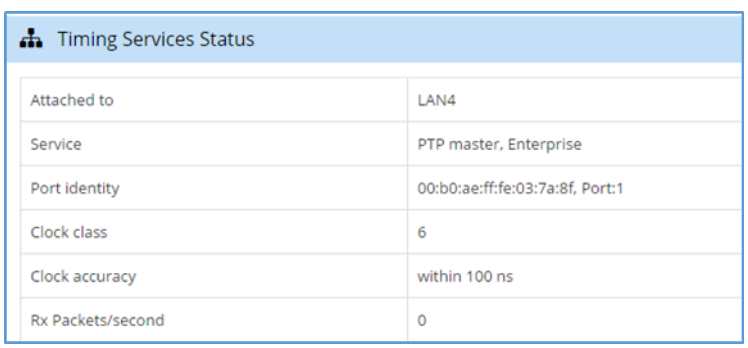
LAN4

Service name	(10) PTP domain 1 priority2 100
Service config	PTP master, Enterprise
Port state	Master
Service Packets per second	0

Announce Content

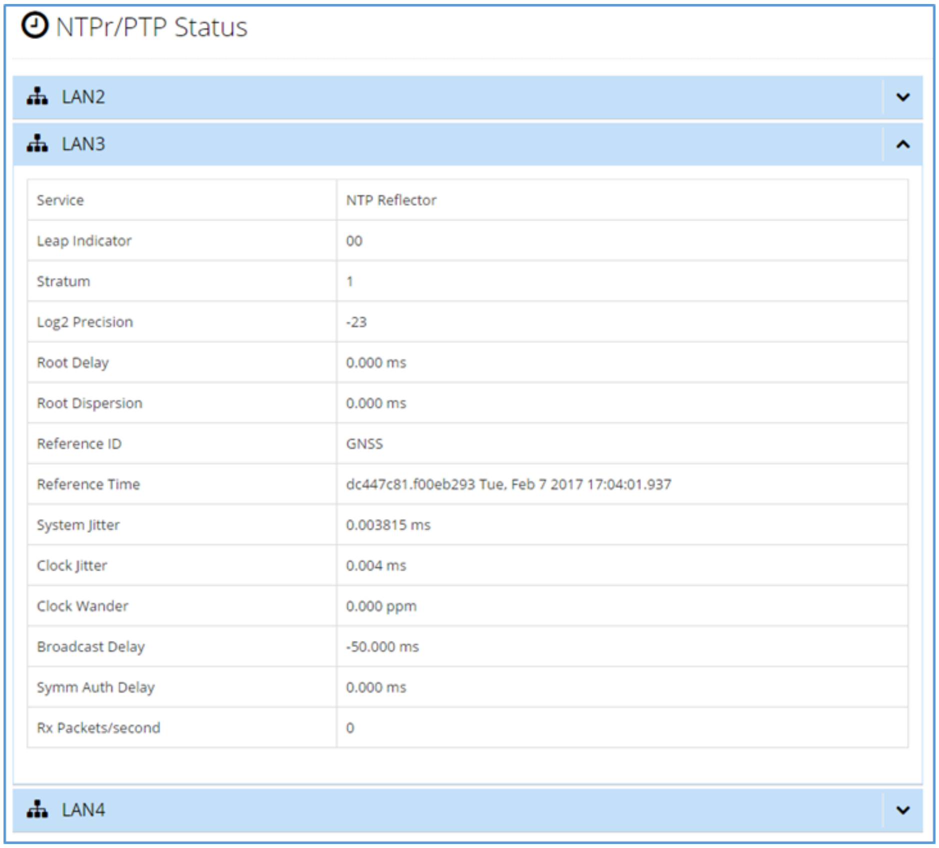
Port identity	00:b0:ae:ff:fe:03:7a:8f, Port:1
Clock class	6
Clock accuracy	within 100 ns
Offset scaled log variance	0x3bea
Timescale	PTP
Timesource	GPS
Time tracable	True
Frequency tracable	True
Current UTC offset valid	True
Current UTC offset	37 s
Leap 61	False
Leap 59	False
Steps removed	0

Figure 6-27. Timing Service Status on Dashboard > Timing Services Status (PTP Master)


Timing Services Status

Attached to	LAN4
Service	PTP master, Enterprise
Port identity	00:b0:ae:ff:fe:03:7a:8f, Port:1
Clock class	6
Clock accuracy	within 100 ns
Rx Packets/second	0

Figure 6-28. Example status on Network Timing'NTPr/PTP Status form (NTPr)


NTPr/PTP Status

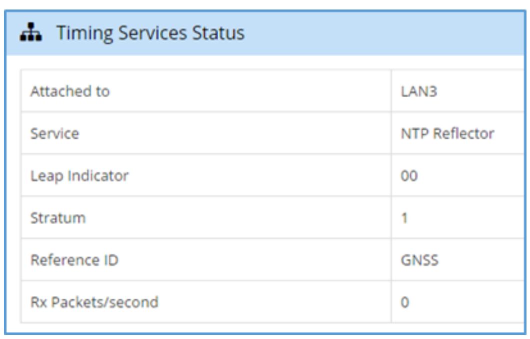
LAN2

LAN3

Service	NTP Reflector
Leap Indicator	00
Stratum	1
Log2 Precision	-23
Root Delay	0.000 ms
Root Dispersion	0.000 ms
Reference ID	GNSS
Reference Time	dc447c81.f00eb293 Tue, Feb 7 2017 17:04:01.937
System Jitter	0.003815 ms
Clock Jitter	0.004 ms
Clock Wander	0.000 ppm
Broadcast Delay	-50.000 ms
Symm Auth Delay	0.000 ms
Rx Packets/second	0

LAN4

Figure 6-29. Timing Service Status on Dashboard'Timing Services Status (NTPr)


Timing Services Status

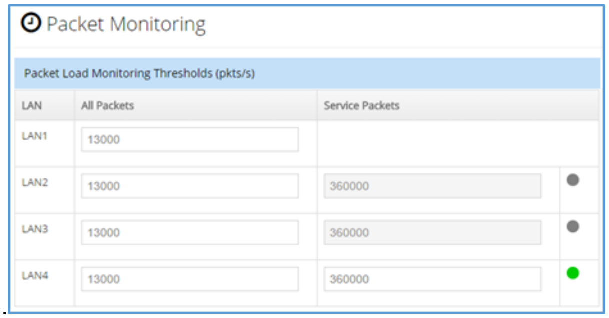
Attached to	LAN3
Service	NTP Reflector
Leap Indicator	00
Stratum	1
Reference ID	GNSS
Rx Packets/second	0

6.8.4 Monitoring Network Packets

The S6x0 provides capability to monitor and limit incoming packets on each of its LAN ports. The capability is covered in Security - Packet Monitoring (security license required). The relationship between the packet thresholds configured there and the mapped network timing services is as follows:

- For any LAN that has NTPd mapped (LAN1, 2, and 3 in Figure 6-24) those incoming timing service packets are only included in the All Packets column thresholds (not Service Packets column).
- For any LAN that has PTP Master or NTPr mapped (LAN4 in Figure 6-24) those incoming timing service packets are only included in the Service Packets column threshold (not All Packets column). Additionally, if a LAN has one of these services mapped to it, that is only LAN where the Service Packets column threshold value will be used. If such a mapping exists, it is indicated with a green dot and the threshold value in that row is allowed to be modified. The form below shows the Packet Monitoring form when

the mapping is from example in Figure 6-24. The green dot is lit for LAN4 because NTPr is mapped to LAN4.



6.8.5 Provisioning the PTP Server Output

Table 6-19. Configure New PTP Server Output

Method	Steps	Notes
Web Interface	Network Timing > NTPr/PTP Config 1. Use the Service dropdown box to select PTP master in the “Add New” row at the bottom of the window. 2. Use the Profile dropdown box to select the desired profile in the “Add New” row. 3. Click the blue Configure icon in the “Add New” row. The Configurable Parameters widow will open. 4. Change the parameter settings to the desired values. Click OK. 5. Click the green +Add button	
	Network Timing > NTP/PTP Mapping 1. Use the NTPr/PTP Service Name dropdown box to select the PTP service name for the desired port. 2. Click the Apply button.	Map PTP master to the desired LAN port.
CLI	n/a	n/a
Front Panel	n/a	n/a

Table 6-20. Editing Existing PTP Server Output

Method	Steps	Notes
Web Interface	Network Timing > NTPr/PTP Config 1. Use the Service dropdown box to select PTP master in the desired row. 2. Click the blue Configure icon in the Configure column of that row. 3. Change the parameter settings to the desired values. Click OK. 4. Click the Apply button.	

...........continued		
Method	**Steps**	**Notes**
	Network Timing > NTP/PTP Mapping 1. Use the NTPr/PTP Service Name dropdown box to select the PTP service name for the desired port. 2. Click the Apply button.	Map PTP master to the desired LAN port.
CLI	n/a	n/a
Front Panel	n/a	n/a

The SyncServer only support TAI timescale. The ARB timescale is not used.

Per the enterprise profile specification, the PTP output will not be enabled until the UTC offset is known. This must be manually entered on the Timing - Input Control Window page if the system has not obtained this information from the reference. For example, the UTC offset must be manually entered for IRIG references.

IEEE 1588 2.1 should only be configured for the PTP master configuration when using with a 1588 2.1 client.

6.8.6 Provisioning the PTP Server - PTP Output Power Profiles

Three types of PTP power profiles for grandmaster operations are supported. As with all PTP Master functionality, the PTP Master option must be installed to activate any of these (installed options are shown on Admin > Options). The supported power profiles are:

- Power Utility Profile IEC/IEEE 61850-9-3:2016
- Power Profile IEEE. C37.238-2017
- Power Profile IEEE C37.238-2011

All of these profiles use Layer-2, Multicast as covered in IEEE Std 1588-2008, Annex F. Additionally, they all use the peer-to-peer delay mechanism. Further details can be found in the standards documents with same name as the profile.

As with all network-based timing services, the power profiles are configured on the Network Timing > NTPr/PTP Config form. The top level Service is PTP Master, which, when selected, will allow each of these power profiles to be selected from the Profile selection control in that row. See Configuring Network Timing Services. Once a service has been configured, a separate form (Network Timing > NTP/PTP Mapping) is used to attach the service to the desired network port(s). See Mapping a Network Timing Service to a LAN Port.

Here's a summary of basic similarities and differences between these profiles. It may be helpful to bring up the configuration form for a service created for each of these profiles. This is accomplished by creating a timing service of the desired profile, then selecting the blue box from the Configure column for that row. This shows everything that can be configured for that profile.

- They all share the same set of basic PTP data set configurations, which are grouped by the “PTP Data Set” title on the configuration form for each profile. These are standard 1588 attributes. The only differences are that some settings have different ranges and defaults. For example, C37.238-2017 specifies default Domain of 254. The configuration forms are aware of any specific default and range differences between these profiles.
- The C37.238-2011 profile calls for support for VLAN tag insertion, so controls for VLAN Id and VLAN priority are provided. While not specifically required for other profiles, all of the configurations support it. However, only the C37.238-2011 profile defaults the VLAN enable/disable control to Enable.
- The C37.238 profiles call out support for a couple of IEEE Std 1588-2008 management messages. ALTERNATE_TIME_OFFSET_INDICATOR and ORGANIZATION_EXTENSION. Tables 81 and 35 in IEEE Std 1588-2008 show the structure of these TLV (Type Length Value) messages. However, rather than supply them as separate messages (as called out in IEEE Std 1588-2008) with C37.238 profiles they are appended to the Announce messages that are routinely multicast. To support these requirements the configuration forms for both C37.238 profiles include configuration (where appropriate) for both of these messages. Further details:
  On the configuration form the area marked C27.238 TLV is actually the ORGANIZATION_EXTENSION message, but specifically as required by the profile. This TLV is always appended to each Announce message. Working through the relevant elements in the message structure:

- The organizationID for both C37.238 profiles is 0x1C129D. This is not user configurable. This value is always automatically encoded for this field.
- The organizationSubType is 0x000001 for profile C37.238-2011, 0x000002 for profile C37.238-2017. These are not user configurable. The appropriate value is always encoded for this field.
- Per IEEE Std 1588-2008, the dataField portion of the ORGANIZATION_EXTENSION message is allowed to have unique structure definition. For these profiles, the following elements are defined:

  The GrandmasterID is part of the dataField. For C37.238-2011 the GrandmasterID range is restricted to 3 - 254 and defaults to 3. For C37.238-2017 the GrandmasterID range is unrestricted. This value is user configurable for both C37.238 profiles.

  grandmasterTimeInaccuracy is an element in the data field. It provides a time error estimate in nanoseconds (the range is uint32). This field generally follows the standard Announce message clockAccuacy value except grandmasterTimeInaccuracy is essentially a continuous value compared with the 18 discrete values defined for clockAccuracy.
  On the configuration form the area marked Alternate Time Offset Indicator TLV provides control for the ALTERNATE_TIME_OFFSET_INDICATOR message. Unlike the ORGANIZATION_EXTENSION TLV which contains C37.238 custom fields, this TLV maps directly to all of the data fields in table 81 of IEEE Std 1588-2008. Each of these is user-configurable so whatever is configured for each field will be incorporated into the outbound TLV. Additionally an Enable/Disable control is provided to support withholding this TLV if desired.

The SyncServer does not support SNMP MIB for Power Profile.

6.8.7 Viewing PTP Clients for PTP GM Outputs

The SyncServer S6x0 can list up to approximately 800 PTP clients by LAN port, with sorting based on client PTP attributes. This feature does not apply to the default or Enterprise using Multicast messaging.

This feature is useful for:

- Initial PTP network setup
- Assuring expected PTP clients are connected to expected SyncServer LAN port(s)
- Checking PTP client settings from one location.

Table 6-21. Viewing PTP Clients for PTP GM Output Ports

Method	Steps	Notes
Web Interface	Network Timing > PTP Client List 1. Select the desired PTP GM port using the LAN dropdown box . 2. Use the Display dropdown box to select the number of client records to display for the selected LAN. 3. Click the Refresh button.	
CLI	n/a	n/a
Front Panel	n/a	n/a

6.8.8 Provisioning the Serial Timing Output

The serial timing outputs (on port labeled “DATA/TIMING”) can be configured for NMEA, NENA, or serial legacy output format.

Table 6-22. Configure Serial Timing Output

Method	Steps	Notes
Web Interface	Timing > Serial 1. Select the NMEA radio button. 2. Click the check box or combination of check boxes for the desired type(s) of NMEA output format: - NMEA - 0183 ZDA Output - NMEA - 0183 GGA output - NMEA - 0183 GSV output - NMEA - 0183 RMC output 3. Click the **Apply** button.	Select NMEA output format. See Table 6-23 below for details about NMEA output formats.
	Timing > Serial 1. Select the NENA radio button. 2. Click the check box for the desired type of NENA output format. - DDD HH:MM:SS DTZ=XX - WWW DDMMMYY HH:MM:SS - YYYY DDD HH:MM:SS DZZ 3. Click the **Apply** button.	Select NENA output format. NENA ASCII time code is sent in **broadcast mode**, in which the code is sent once per second at the beginning of the second (Data/ timing serial port).
	Timing > Serial 1. Select the Legacy Serial Output radio button. 2. Click the **Apply** button.	F8 - Continuous Time Once-per-Second DDD:HH:MM:SSQ Note: F9 - Time On Request DDD:HH:MM:SS.mmmQ (direct request to Console port)
	Timing > Serial 1. Click the **Off** radio button at the top of the dialog box. 2. Click the **Apply** button.	Turn Serial Timing Output off.
CLI	n/a	n/a
Front Panel	n/a	n/a

Table 6-23. NMEA183 Output Format Details

Format	Description
ZDA	All fields are updated except for timezone fields, which are always 00. $GP, $GL, and $GB are used to indicate GPS, Glonass and Beidou respectively. Example: *$GPZDA,235626,29,11,2016,00,00*40

...........continued

Format	Description
GGA	All fields are updated except for the 2 DGPS fields, which are NULLed. $GP, $GL, and $GB are used to indicate GPS, Glonass and Beidou respectively. Example: $GPGGA,235626,3724.7719,N,12156.8643,W,1,14,0.8,14.3,M,-29.8,M,,*41

GSV	All fields are updated.
	$GP, $GL, and $GB are used to indicate GPS, Glonass and Beidou respectively.
	Example:
	`$GPGSV,4,1,23,1,46,231,45,3,58,319,46,4,165,0,0,9,2,265,0*74`
	`$GPGSV,4,2,23,11,21,219,38,14,35,58,43,16,9,151,39,22,77,321,47*77`
	`$GPGSV,4,3,23,23,35,277,47,25,7,39,33,26,24,125,50,31,52,54,43*41`
	`$GPGSV,4,4,23,32,10,72,36*78`
	`$GLGSV,3,1,23,2,20,99,23,3,58,46,49,4,35,322,44,12,21,31,0*55`
	`$GLGSV,3,2,23,13,63,78,46,14,38,174,41,15,2,192,35,18,5,228,43*5F`
	`$GLGSV,3,3,23,19,19,277,48,20,10,330,32*68`

RMC	All fields are updated except for speed and course, the 2 magnetic variation field, which are all NULLed. $GP, $GL, and $GB are used to indicate GPS, Glonass and Beidou respectively. Example: $GPRMC,235626,V,3724.7719,N,12156.8643,W,,,291116,,,A*7D

6.8.9 Provisioning Outputs on Timing I/O Module

The standard configuration offers a broad yet fixed selection of signal I/O. J1 is dedicated to time code and rate inputs, J2 to sine wave inputs, and J3-J8 to mixed signal outputs. See Table 1-4 for the standard Timing I/O Module configuration.

The FlexPort™ Technology option enables the 6 output BNCs (J3-J8) to output any supported signal (time codes, sine waves, programmable rates, etc.) on all configurable ports via the secure web interface.

Note: The SyncServer S6x0 uses IRIG 1344 version C37.118.1-2011. Control bits 14 - 19 will always be zero, and the encoded IRIG time will be UTC (if using an input 1344 IRIG as the reference the 2011 rules are applied to get that value). Hence, any code receiving S6x0 IRIG 1344 output should work regardless of which version they are decoding (since there is nothing to add or subtract).

.

Table 6-24. Configure IRIG and Other Outputs on Timing I/O Module

Method	Steps	Notes
Web Interface	Option Slot A > Timing I/O Card 1. For desired output J3-J8, use dropdown box to select the general signal output type of “Pulse”, “Timecode” “Sine” or Off. 2. For TimeCode, use the dropdown box to select the type of IRIG: 3. For Pulse, use the dropdown box to select Fixed Rate or Programmable Period. 4. For Fixed-rate Pulse, use the dropdown box to select the rate or period. 5. For Programmable Period Pulse, enter the period, with a resolution of 10ns, and a range of 100 ns to 86400 s. 6. For Sine, use the dropdown box to select the frequency, 1M, 5M or 10M. 7. Enter phase offset value (for fixed-rate pulses or timecode outputs) It has a range of -0.499999800 to 0.499999800 s. 8. Click the **Apply** button.	Timecode Choices: • A004 (DCLS, YR, CF, SBS) • A134 (10Khz, YR, CF, SBS) • B000 (DCLS, CF, SBS) • B001 (DCLS, CF) • B002 (DCLS) • B003 (DCLS, SBS) • B004 (DCLS, YR, CF, SBS) • B005 (DCLS, YR, CF) • B006 (DCLS, YR) • B007 (DCLS, YR, SBS) • B120 (1kHZ, CF, SBS) • B121 (1kHZ, CF) • B122 (1kHZ) • B123 (1kHZ, SBS) • B124 (1kHZ, YR, CF, SBS) • B125 (1kHZ, YR, CF) • B126 (1kHZ, YR) • B127 (1kHZ, YR, SBS) • B1344 (DCLS) • B1344 (1kHZ) • E115 (100Hz, YR, CF) • E125 (1KHz, YR, CF) • G005 (DCLS, YR, CF) • G145 (100kHz, YR, CF) • C37.118.1 • NASA 36 (DCLS) • NASA 36 (1kHz) • XR3 (250Hz) • 2137 (1kHz) • 2137 (DCLS)
CLI	n/a	n/a
Front Panel	n/a	n/a

Note: The web page may allow a larger range for the phase offset value, but the supported range is from -0.499999800 to 0.499999800.

Please note that for the 1PPS falling edge pulse, the maximum supported negative offset is -499,970,000 ns.

During startup and holdover recovery, the fixed-rate pulse count may adjust. For example, if 10 MPPS is configured, there may not be exactly 10 million pulses during every 1 second window during startup and holdover recovery.

6.8.10 Provisioning Outputs on Timing I/O with Telecom Module

Table 6-25. Configure T1, E1, and Other Outputs on Timing I/O with Telecom Module

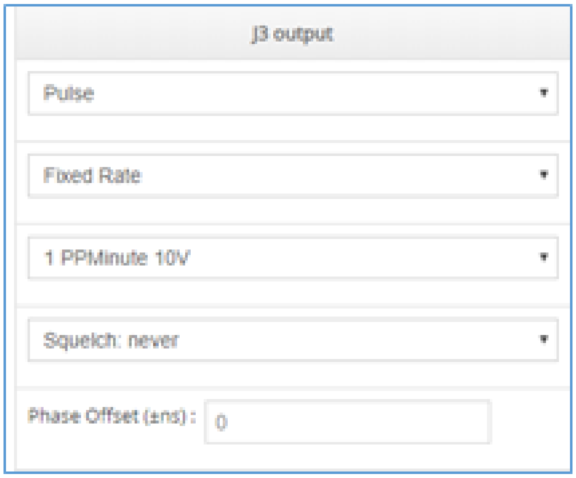
Method	Steps	Notes
Web Interface	Option Slot A > Timing I/O Card T1 Output 1. For T1 output on J7, use dropdown box to select signal type of T1 Output. 2. Click the Edit button. 3. Use the dropdown box to select the frame type of ESF, D4 or freq1544kHz. 4. Click the **Apply** button. E1 Output 5. For E1 output on J8, use dropdown box to select signal type of E1 Output. 6. Click the Edit button. 7. Use the dropdown box to select the frame type of CCS, CAS, or freq2048khz. 8. Click the **Apply** button. Timing I/O Outputs For other ports, seei information in Table 6-23.	Tekecom Signal Type Choices • T1 • E1 • CC and JCC • JSW • CC (50/50 duty cycle) • CC (5/8 duty cycle) • JCC (with 400 Hz) • JCC (no 400 Hz)
CLI	n/a	n/a
Front Panel	n/a	n/a

6.8.11 Provisioning Outputs on Timing I/O HaveQuick/PTTI Module

For BNC connections J3 - J6, along with support for all time and frequency output capabilities that are associated with the standard timing I/O module (090-15201-006), additional outputs associated with HaveQuick/PTTI are supported. J7 and J8 connections have a unique connector and are dedicated to PTTI output BCD codes (covered later).

J3 - J6 identically support the following HaveQuick/PTTI capabilities:

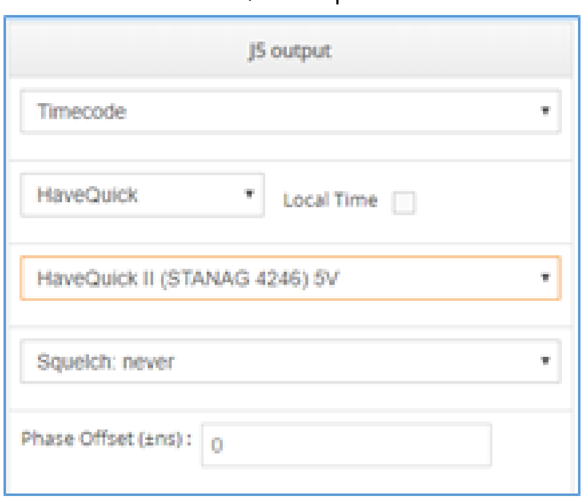
- 1 PPS and 1 PPMinute, both of which are included in the set of GPS-UE (User Equipment) interface signals shown in figure 4 of ICD-GPS-060, have additional signal level options. Using J3 as an example, the unique (to this module) 1 PPMinute 10V selection is shown. This selection, as well as other unique ones, is found near the end of the selection list for this control. Other selections specific to this module include: 1 PPMinute 5V, 1PPS 10V, and 1PPS 5V.
  The combined capability for these 2 specific outputs is thereby extended to 3 signal levels: TTL (the common setting for all modules) plus the 2 new ones unique to this module: 5V and 10V, as shown in the following image.



- A set of HaveQuick codes is supported. Each timecode is provided with 2 signal level options: TTL or 5V. The code structure is identical for either choice.
  - ICD-GPS-060A. This is the originating HaveQuick code defined in document of same name. See figure 8 and associated descriptions in that document. Note that J1 input also supports this timecode.
  - HaveQuick II (STANAG 4246). This code is the same as ICD-GPS-060A but removes the 8 TFOM bits at the end of the code. Note that J1 input also supports this timecode.
  - HaveQuick Extended (STANAG 4430). This code adds leap second content (compared to ICD-GPS-060A). Note that J1 input also supports this timecode.
  - HaveQuick I (STANAG 4246). This is an abbreviated version of HaveQuick II (STANAG 4246). This timecode additionally removes Year of century and day of year, so it is effectively only current time of day. Not supported as an input on J1.

Configuration of the HaveQuick output is an extension of the existing Timecode top-level selection, as shown in the following image. For example to configure HaveQuick II (STANAG 4246) 5V on J5 connection:

1. Select Timecode on top-level control for that connection. This enables selection of all supported timecode categories on the 2nd control.
2. Select HaveQuick from the available list on the 2nd control.
3. Select the desired HaveQuick output code on the 3rd control, in this case HaveQuick



II.

4. Select Apply to complete the configuration.

J7 and J8 support BCD timecode outputs on RJ45 connections since these codes require a 2-wire balanced output (not possible with BNC connection). The base code is defined in ICD-GPS-060A/B (figure 6 in revision A, figure 3-3 in revision B). Along with the standard BCD code, an abbreviated version is also supported. This version transmits the full 50 bits, but only the first 24 bits (UTC time of day) are meaningful. The remaining bits are set high.

For test purposes a selectable 1PPS or 1 PPMinute output is also available on the connection. Pinouts are as shown in Table 6-25 below.

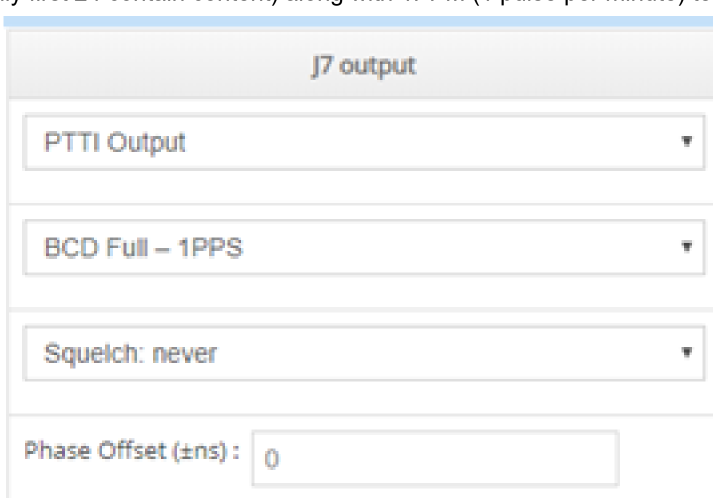
Table 6-26. J7 & J8 Connector Pin Assignments - Timing I/O Module with HaveQuick/PTTI Connections

Pin	Signal
1	PTTI BCD Tx+ (code out)
2	PTTI BCD Tx- (code out)
3	1PPS/PPM out, TTL level (for test purposes only)
4	Ground
5	Reserved, do not connect
6	N/C
7	Reserved, do not connect
8	Reserved, do not connect

Electrical characteristics for code outputs on pins 1 and 2 are as described in ICD-GPS-060 revision B, section 3.4.3.3.

To configure BCD codes for output on J7 or J8 is straightforward:

- Navigate to the form using the OPTION SLOT A (or B) > Timing I/O + HQ/PTTI selection on the left-side column of the web interface.
- The only top-level choices will be off (no output) or PTTI Output, as shown in the figure. Select PTTI Output.
- The 2nd control lists the 4 available options:
  - BCD Full - 1PPS. This will generate the full BCD code along with 1PPS test signal on pin 3.
  - BCD Full - 1PPM. This will generate the full BCD code along with 1PPM (1 pulse per minute) test signal on pin 3.
  - BCD Abbrev - 1PPS. This will generate the abbreviated BCD code (still 50 bits, but only first 24 contain content) along with 1PPS test signal on pin 3.
  - BCD Abbrev - 1PPM. This will generate the abbreviated BCD code (still 50 bits, but only first 24 contain content) along with 1PPM (1 pulse per minute) test signal on pin



3.

Select Apply to complete the configuration.

6.8.12 Provisioning Programmable Pulse Output

The following table shows the Timing I/O modules that can provide a programmable pulse output when installed in the SyncServer S650. The Programmable Pulse Output license must be installed to use this feature, Only the J7 connection on the applicable modules can be configured as Pulse > Programmable Pulse. If two of the applicable modules are installed in the S650, there can be 2 independent programmable pulse configurations operating simultaneously, one on each of the J7 connections.

Table 6-27. Modules that Support Programmable Pulse Output

Supports Programmable Pulse	Does Not Support Programmable Pulse
Timing I/O module Timing I/O module with Fiber Input	Timing I/O module with Telecom Timing I/O module with HaveQuick/PTTI
Timing I/O module with Fiber Output	10 MHz Low Phase Noise (LPN) module

In Summary, the programmable pulse feature supports controls to generate on-time (UTC) events based on pattern-matching of any digits in the following common time description format:

DDD:HH:MM:SS.<fractional second>

Where

DDD = Day of the year

HH = Hour of the day

MM = minute of the hour

SS = seconds of the minute

<fractional seconds> = time of the second in decimal digits down to 10 ns

Additional capability is provided to define wildcard digits that will allow repeat pulse outputs whenever the first non-wildcard digit is matched in time (explained later).

The width (stop time) of the generated pulses can also be configured. Other than this control, the signal characteristics are the same as Pulse > Fixed Rate outputs on the J7 connector.

6.8.12.1 Configuration and Usage

Select the appropriate option slot from the left-side navigation pane, then configure at the J7 Output location on the form. For the example shown below in Figure 6-30, the module in SLOT A is used and the J7 output is shown to already be set up for the Programmable Pulse capability. Note that in the region just above the J7 configuration it is shown that the Programmable Pulse Output Option is installed. If it were not installed, this setting would not be available. All currently installed options are listed at Admin > Options.

Figure 6-30. Option Slot Window - Timing I/O Module with Programmable Pulse License Installed

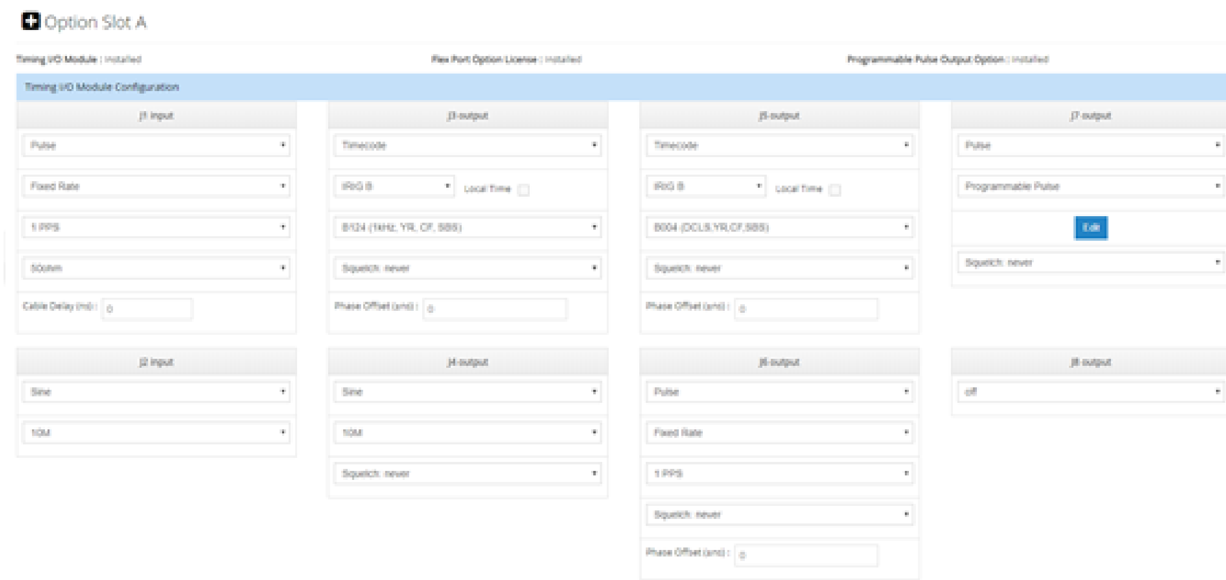
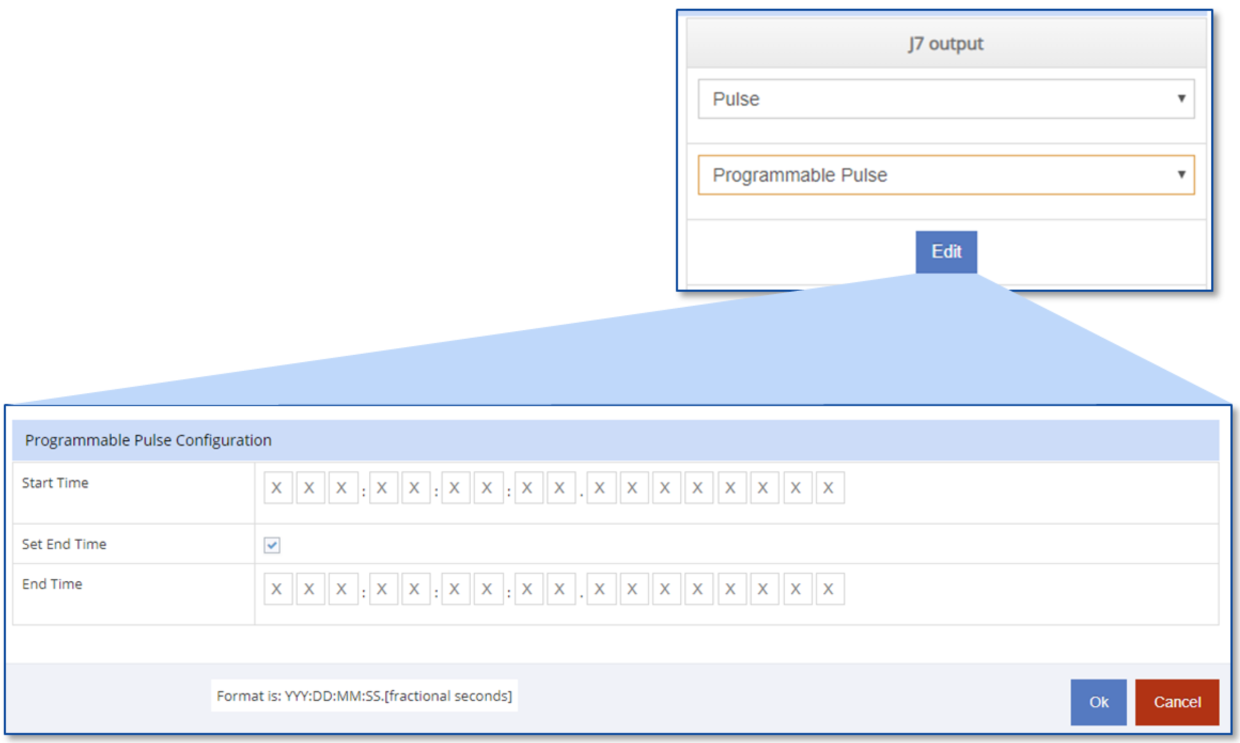


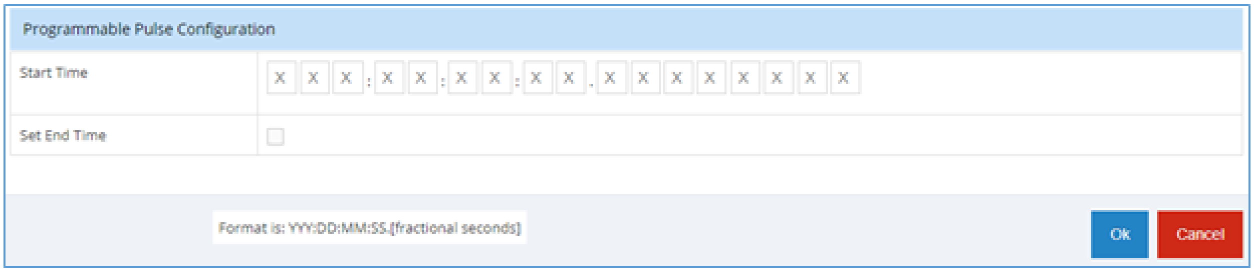
Figure 6-31. Programmable Pulse Form



With the Programmable Pulse setting, an Edit button appears on the form. First-time selection brings up the configuration form which is used to create the specifically desired output behavior. The bottom of the form provides a reminder of time region covered by each of the configuration boxes.

The Start Time row is used to define a time (or times) when pulses should be generated. The “X” that is defaulted into each of the boxes is a wildcard which, as will be seen, is used to match all times for that particular time partition. Other than the wildcard character, numeric values are allowed within the appropriate range for each box. For example, the hour entries allow 0 - 2 for the tens of hours and 0 - 9 for single hours (e.g. 00 - 23 combined range).

Figure 6-32. Programmable Pulse Configuration



The simplest usage is to provide numeric entry (no wildcards) for every box. This will have the effect of generating only 1 pulse per year, but it is a helpful way to understand the most basic operation. In words, The configuration below will produce a single pulse at the associated J7 connector with rising edge occurring on the 100th day of the year, 16th hour of that day, 12th minute of that hour, 44th second of that minute, 500 nanoseconds after the start of the 44th second (note that there are 8 fractional seconds digits, so the rightmost is tens of nanoseconds, hence the value shown is 500 ns).

Since the end time control is not used in this case, the pulse width is defaulted to the shortest possible, which is 10 ns.

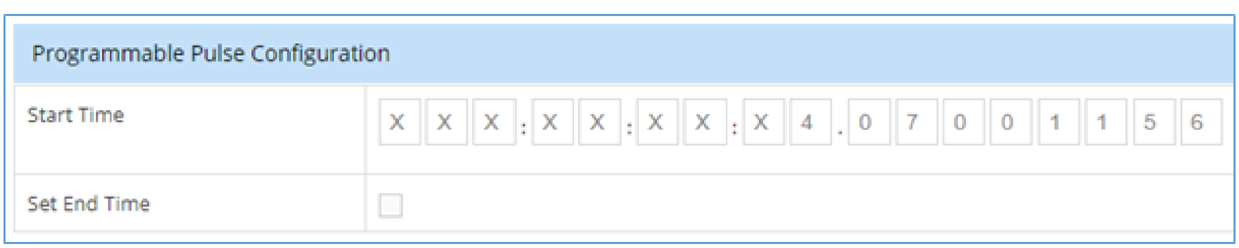
Since having capability to generate a precisely timed output only once a year is limiting, the wildcard can be used to greatly expand the utility. The behavior associated with the wildcard is as follows:

- The wildcard “X” means that all values are a match for the box that contains it.
- Working from the left (start at hundreds digit of day of year entry) the first non-wildcard value defines the rate at which pulses will be generated (example will demonstrate this).
- Again working from the left, as soon as a non-wildcard is encountered (i.e. a number is encountered), there can be no more wildcards. Tip: when entering wildcards if you first enter the rightmost one then all positions to the left will be auto-filled with wildcards.

Here's an example:

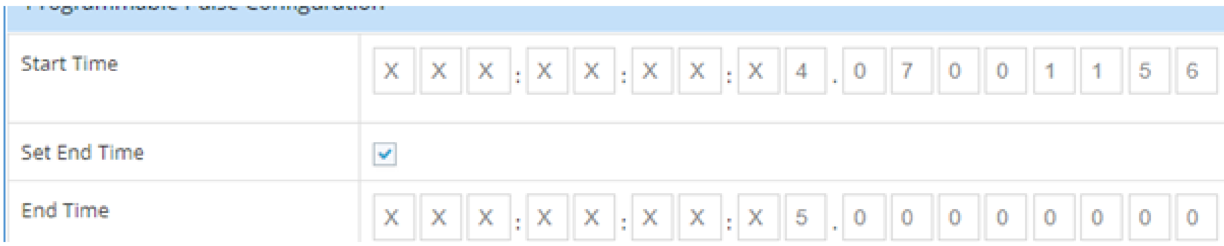
- Wildcards are entered for all entries from the left through the tens of seconds digit. The current time for all of these wildcard entries will never prevent generation of an output pulse. Another way of saying this is that a pulse will be generated whenever the time matches the remaining numerically-assigned entries.
- The first numeric digit is a 4 in the seconds location. Since everything to the left is a wildcard it means that outputs will occur sometime in every second that ends in 4. This would be 6 different times in every minute: seconds 04, 14, 24, 34, 44, and 54.
- Since there are further non-zero digits to the right of the 4, the actual time of the pulse outputs will be 70 milliseconds (the 070), 11 microseconds (the 011), and 560 nanoseconds (the 56) after every second in the minute that ends in “4”.

This approach can be used to generate a variety of time-aligned repeating pulse patterns.



For all above examples, the pulse width will be 10 ns (the default). For precise control of the pulse end time the set end time capability is used. Following the wild card example, the figure below shows a result after checking the set end time box. This brings up another set of entries that follow the same rules as the start time entries previously described. The difference is that these define when to end (go from high-to-low) the pulse. The example below shows that when wildcards are used, both start and stop must share the same wildcard positions, which is enforced by the interface behavior. The example shown will generate pulse widths of about 1 second, short of that amount by 70.01156 ms since only the start time has that additional delay (of course, that amount could also be added to the stop time to make it exactly one second width).

Because the end time setting is just as configurable and precise as the start time, this capability can be used as a method to generate a precise falling edge event (or series of events). Thought of in this way, the example below will generate a precise falling edge at 5, 15, 25, 35, 45, and 55 seconds of every minute. If there are situations where precise start (on rise) and stop (on fall) are needed, this scheme can support it.

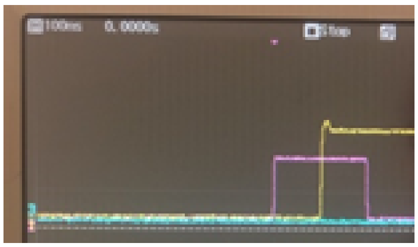


This capability can also be used as a precise method to bracket a signal of interest. As a simple example, suppose we want to frame an on-time PPS rising-edge with a pulse that begins 100 ns prior to the PPS and ends 100 ns after the PPS. The setup shown below will accomplish this:

- Since we are using the wildcard at the 1 seconds digit, the start time will initiate a pulse at 999.9999 milliseconds after the start of each second, which is the same thing as 100 ns prior to the start of the next second.
- The end time is set to occur 100 ns after the start of each second.

The image below shows the result on a scope. The yellow waveform is an on-time rising-edge PPS signal. The magenta waveform is the programmed pulse generated by this setup. Note that it straddles the PPS signal by 100 ns on either side.

This example also illustrates the behavior when the end time value is a smaller value than the start time, which might seem illogical (how can the pulse end before it starts?). The way to think of it is that there is always cause-and-effect between start and end time. If the programmed pulse hasn't started, then there is never anything to stop. Using the example, if you think of the startup of this configuration beginning at the top of a second, on that second the end time is encountered first (100 ns after start of second). However, since there hasn't yet been a start time match, nothing happens. Later in that same second, the start time match occurs (100 ns prior to the next second) and the programmed pulse actually starts. Then, 100 ns into the next second, the end time matches the wildcard and the programmed pulse ends. This process will continue on every second thereafter. This technique can be used to bracket any time of interest, even if it requires end time to be smaller than start time.



To complete any setup, the OK control in lower right is chosen, which returns back to the slot module configuration form. The specific programmable pulse configuration is retained while on the module configuration form, but it is not actually configured until the Apply on the slot module configuration form is selected (same as is used for any module configuration). If you forget to Apply, a warning dialog will appear so you'll have the opportunity to save the programmable pulse configuration if that is what you wanted.

Table 6-28. Configure Programmable Pulse Outputs on Timing I/O Module

Method	Steps	Notes
Web Interface	Option Slot A/B > Timing I/O Card 1. On J7 configuration, use dropdown box to select the general signal output type of “Pulse”. 2. Use the dropdown box to select Programmable Pulse output. 3. Click the Edit button. The Programmable Pulse Configuration window will appear. 4. Enter the desired Start Time. Format is:DDD:HH:MM:SS.[fractional seconds] 5. For Set End Time, check the box. 6. Enter the desired End Time. Format is: DDD:HH:MM:SS.[fractional seconds] 7. Click the **OK** button. This closes the Edit form but does not actually configure the changes (see next step). 8. Select Apply on the module configuration form to complete the configuration.	The Programmable Pulse license is required to use this feature.
CLI	n/a	n/a
Front Panel	n/a	n/a

6.9 Making Time-Interval or Event Timestamp Measurements

With the Time Interval Measurement license installed, if the unit has a module installed that allows the J1 connection to be configured as Pulse > Fixed Rate > 1 PPS then it is capable of making time-interval and event timestamp measurements.

6.9.1 Measurement Basics

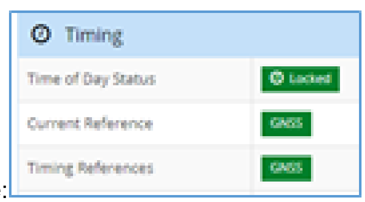
The time-interval measurement function on S6xx is similar to measurement on a traditional time-interval stand-alone instrument: measurement of the time-difference between 2 inputs. A common use-case is to compare a reference PPS signal with a test PPS signal to assess its alignment with respect to that reference. This is the capability provided by S6xx. There are some differences:

- There is only one input needed: the PPS to be measured. This is connected to the J1 input on the desired module (if there are 2 modules, then either J1 can be used).
- The J1 input is internally measured against the reference PPS. A simple way to think of it is that this reference is the same as the 1PPS output generated by the S6xx. Other than accounting for cable delays, if you think of taking the S6xx PPS output to one input of a counter and the test PPS to the other input and making time-interval measurements, this is what is being done automatically in the S6xx.
- Unlike using a time-interval counter, which does not have time awareness, the S6xx records the actual time as part of each measurement which can very helpful when analyzing results.
- If the J1 input stops while the measurement is running (e.g. disconnected or squelched at the source) no measurements will be taken during that period, but if the signal later returns the measurements will automatically proceed. The gap in data collection will be reflected in the time of measurement for the results, so loss-of-signal anomalies during measurement are easily identified in post-processing.

The polarity of each time-interval measurement is with respect to the reference PPS. If the J1 input PPS occurs after the reference, the result will be positive. If the J1 input PPS occurs before the reference, the result will be negative. In general, the “closest reference PPS” will be used for each measurement which effectively makes the measurement range -0.5 to +0.5 seconds.

The Event Timestamp function on S6xx is simple to explain: When a rising-edge input occurs on J1, that event is timestamped and recorded. The time-of-occurrence is saved with full time information, so the result ends up as a sequence of times when J1 input events occurred. There is no expected input rate for these events, they will be tagged whenever they occur. The sustained maximum rate where no events will be missed is 100 events/second (lower when serial/network connection used). An Event Overflow alarm can be used to provide a warning when this rate is exceeded. The alarm follows all standard alarm conventions and can be configured as desired at Admin > Alarms.(see Admin - Alarm Configuration Window)

General notes applicable to either measurement function:

- The reference used for either measurement is the same as whatever is being used for normal synchronization. A typical example would be GNSS as the S6xx timing reference.
- The measurements will function even if there is no reference into the S6xx (for example, S6xx will measure even if it is freerunning with no awareness of the current time). While this allows for some special case measurements, users should ensure that the time-of-day status (see Dashboard > Timing) is in Locked state if the objective is to make accurate measurements against a good reference. This would be an optimal display for this use-case:

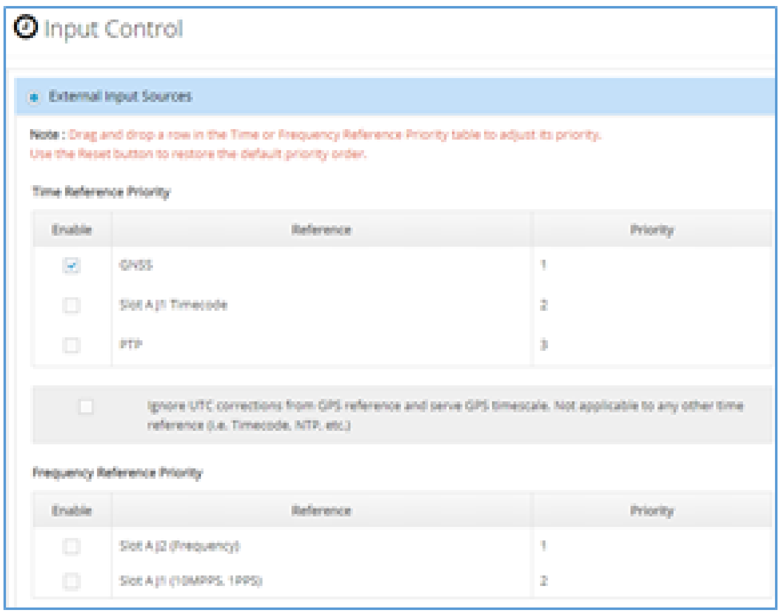
6.9.2 Measurement Setup

The first item is to connect the signal to be measured to whichever J1 input will be used. Simply connect it. The signal range expected is the same as for a PPS when used as an input sync reference. For either measurement type, set the first 3 choices as shown: Pulse, Fixed Rate, 1 PPS. The impedance and Cable Delay(ns) controls can be set as desired. The Cable Delay control reduces the measurement value by the amount entered, which you might do to eliminate transmission time due to cable.

Note: For event timestamp measurements there is no expectation that the input must occur at a 1 PPS rate, but this setting should be used. The events will be timestamped as they occur.

Note: Input LOS alarms could be generated if the input is slower than 1PPS. Microchip recommends disabling the LOS alarm actions on the Admin->Alarms page under this condition.

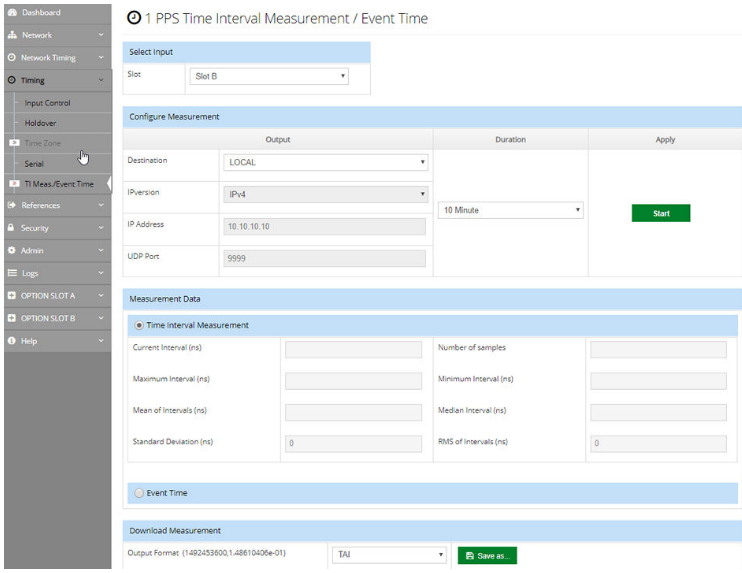
Next, since it generally makes no sense to also allow use of this input also as a sync input reference, the J1 connection should not be enabled on the Timing > Input Control form, as shown here. Disabling J1 as a timing input reference source does not restrict its usage for measurement.



6.9.3 Making the Measurement

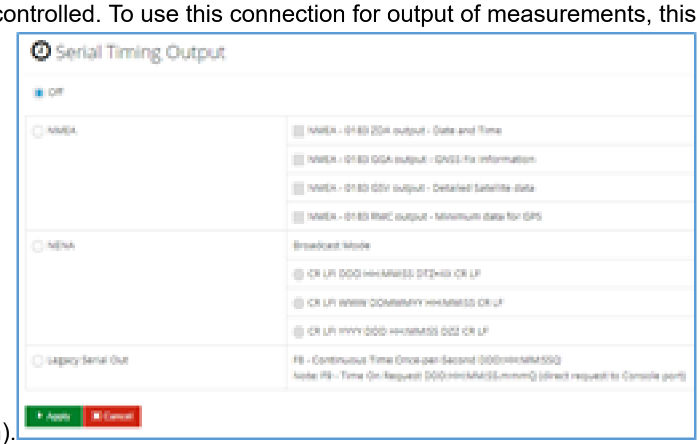
Either type of measurement is controlled on the Timing > Meas./Event Time form shown below.

Walking through the form top to bottom:



- The Select Input Slot control identifies which slot module J1 connection will be used for the measurement. Selection is only possible if the S6xx contains 2 slot modules and both are capable of supporting measurement. If there is only a single module no choice can be made and the control will show the correct slot. This control is common to time-interval and event timestamping measurements.
- The Configure Measurement section provides 3 areas of measurement control. These controls are all equally applicable to time-interval and event timestamping measurements.
- The Output section provides choice on the method to use for data transmission/storage:
  – Setting Destination to LOCAL directs the measurement results to local storage on the S6xx. Regardless of measurement type up to 86,400 measurements can be stored (the number of seconds in one day). The storage capacity is based on actual data, not measurement time. For example, if using Event Time mode and one event occurs each day, then the storage capacity is 86,400 days. If local storage becomes filled, new measurements will continue to be saved, pushing the oldest ones out as needed so that the contents of the storage (when filled) will always be the most recent 86,400 measurements.

    With this setting none of the other selections in the Output section are relevant (they are grayed out).
  – Setting Destination to SERIAL directs the measurement results to the Data/Timing 9-pin serial connection on the S6xx. Any terminal program that supports serial connection can be used to collect (and log if desired) the results. Since there are other possible uses for this connection it may be necessary to de-activate other enabled functions currently assigned to it. The Timing > Serial form is where these other uses are controlled. To use this connection for output of measurements, this form must have setting to Off

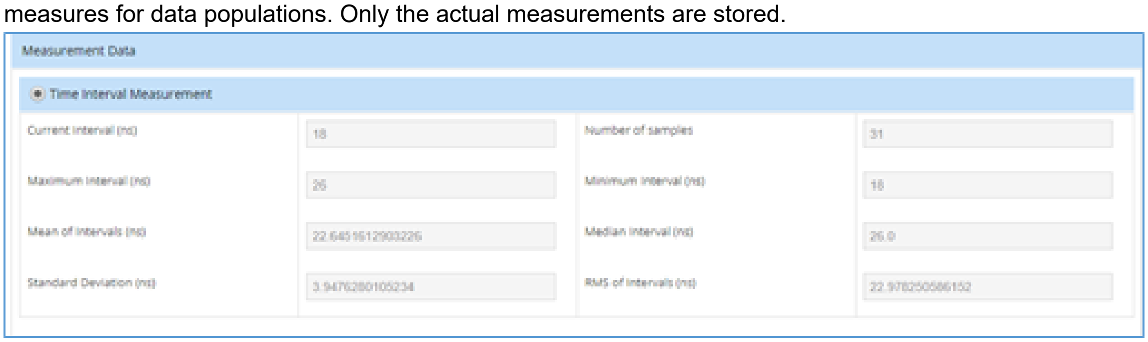
    (as shown).
  – Control of serial port settings is provided on the Admin > Serial Port Config form. This form provides independent serial port controls for the console port (not used for measurement output - upper 9-pin serial connector) and the Time of Day Port (on the left side of the form), which is the lower 9-pin connection labeled Data/Timing port on the S6xx. Configure these settings to agree with the terminal program settings

on the device used to receive the measurements. Note that lower baud rates will lower the number of event time measurements that can be made each second. For example 9600 baud may limit event time measurements to 25 per second instead of 100 per second.

With SERIAL setting none of the other selections in the Output section are relevant (they are grayed out).

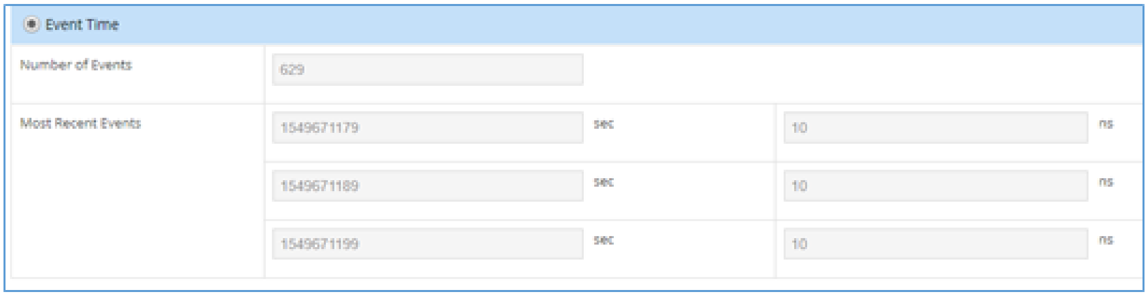
  – Setting Destination to NETWORK directs the measurement results to the LAN1 ethernet connection (same physical connection as the WebGUI). With this setting, the other controls are used to specify the connection that will receive the LAN1 output: IP version, IP Address, and UDP port.

- The Duration section provides control for how long the measurement should run. The control provides a range of bounded choices, all of which will open and close the measurement window for the indicated time, initiated by activation of the Start control. The measurement window will self-terminate regardless of whether or not any actual measurements occurred.
  The continuous selection keeps the measurement window open endlessly upon Start selection.
- The Apply section provides the measurement start and stop control. The control is context-aware and always shows the action that will occur upon its application. Selecting Start begins the measurement and grays out other control settings since the measurement parameters are “locked in” as long as the measurement is running. Whenever the measurement is running the control will indicate Stop.
  When the Destination setting is LOCAL the Start and Stop controls have additional significance:
  – Following selection of Start any data collected so far can be downloaded (See Download Measurement section of form). Downloading while measurement is running will not cause any loss of data collection.
  – Following selection of Stop and until the next Start is selected, any stored data from the prior measurement remains available for downloading. Upon next Start, this prior data is cleared in order to begin new data collection.
- The Measurement Data section provides control of which type of measurement to make:
  – If Time Interval Measurement is selected, the measurement performed is a time-interval measurement (every second) of the user-provided J1 input PPS compared with the S6xx system PPS. While the measurement runs, if the measurement Destination is set to LOCAL, the data shown below is periodically updated. Along with the current time-interval measurement, the other results are well-known statistical measures for data populations. Only the actual measurements are stored.



  – If Event Time is selected, the measurement performed is to timestamp the time of occurrence of every positive edge (the “event”) at the J1 input. While the measurement runs, if the measurement Destination is set to LOCAL, the data shown below is periodically updated. This is a sampling of 3 recent timestamped events (this display may not always show consecutive events, but the stored data will not miss any events as long as the sustained input event rate is not greater than 100 events/second).
  Number of Events shows the total events that have occurred since the start of this measurement

  Most Recent Events shows recent timestamps in the format of <TAI seconds> <fractional seconds>. TAI time is the number of seconds since midnight Jan 1, 1970 and is the timescale used for IEEE-1588 (PTP). For the example shown below, the 3 events are seen to be precisely 10 seconds apart. The source for these events was an S6xx programmable pulse capability configured to generate an event whenever the UTC seconds contains a 6, resulting in events at 06, 16, 26, 36, 46, and 56 seconds every minute.



- The Download Measurement section provides the method to save measurement results wherever desired in the host environment. This option is available only when the Destination for the measurement is/was LOCAL. Results can be saved while the measurement is still running or any time after it has stopped. Details about downloads based on selection:
  Time Interval Measurement:
  – If format is UTC
    Filename is of this form: SyncServer_time_interval_measurement_UTC_1549673170.txt

    Data format is of this form (last field is fractional seconds):

    ```
    2019-02-11,16:45:02, -2.00000000e-09
    2019-02-11,16:45:03, -2.00000000e-09
    2019-02-11,16:45:04, 4.00000000e-09
    ```

    File Header is of this form (directly compatible with Microchip TimeAnalyzer):

    ```
    #Title: SyncServer Time Interval Measurement: Timescale = UTC
    #Type: Phase
    #Frequency: 1
    ```

  – If format is TAI
    Filename is of this form: SyncServer_time_interval_measurement_TAI_1549673165.txt

    Data format is of this form (last field is fractional seconds). These are the same measurements as UTC data above, the only difference is time of measurement (left column) is the TAI seconds:

    ```
    1549903539, -2.00000000e-09
    1549903540, -2.00000000e-09
    1549903541, 4.00000000e-09
    ```

    File Header is of this form (directly compatible with Microchip TimeAnalyzer). Note that the #Start information provides the TAI time of the first measurement in traditional format (it won't appear if there are no measurements made).

    ```
    #Title: SyncServer Time Interval Measurement: Timescale = TAI
    #Type: Phase
    #Frequency: 1
    #Start: 2019-02-09 00:46:01
    ```

    Event Time Measurement:

    Example data is being sourced by an event every 10 seconds.
  – If format is UTC
    Filename is of this form: SyncServer_event_time_UTC_1549904290.txt

    Data format is of this form (YYYY-MM-DD, HH:MM:SS, <fractional seconds>). Each row is the time of an event:

    ```
    2019-02-11,16:56:53, 1.00000000e-08
    2019-02-11,16:57:03, 1.00000000e-08
    2019-02-11,16:57:13, 1.00000000e-08
    ```

File Header is of this form (directly compatible with Microcbip TimeAnalyzer)

```
#Title: SyncServer Event Time Capture: Timescale = UTC
#Type: Phase
#Frequency: 1
```

– If format is TAI
Filename is of this form: SyncServer_event_time_TAI_1549904286.txt

Data format is of this form (<TAI seconds>.<fractional seconds>):

```
1549904260.000000010
1549904270.000000010
1549904280.000000010
```

File Header is of this form (directly compatible with Microchip TimeAnalyzer). Note that the #Start information makes it easy to know in traditional format the TAI time of the first event (it won't appear if there are no events).

```
#Title: SyncServer Event Time Capture: Timescale = TAI
#Type: Phase
#Frequency: 1
#Start: 2019-02-11 16:57:30
```

6.10 Provisioning Alarms

This section describes the controls used to provision and manage alarms in the SyncServer S6x0. For a list of all alarms, see Chapter 8: System Messages.

The Web GUI allows you to perform the following:

- Provision the severity level
- Show current alarm settings
- Show current alarms
- Display alarm status

Alarms are also indicated by an LED on the front panel.

Table 6-29. Configuring Alarm Settings

Method	Steps	Notes
Web Interface	Admin > Alarms Configure Alarm 1. Enter the “Auto ACK” value (Auto Acknowledgement) for the alarm. 2. Use the drop-down box for “Severity” to set the alarm to “Major”, “Minor”, or “Notify”. 3. Enter the “Reporting Delay” value (in seconds) for the alarm. 4. Use the check box for “Send Trap” to enable/ disable an SNMP trap for the alarm. 5. Use the check box for “Write Log” to enable/ disable recording in the log when the alarm is triggered. 6. Use the check box for “Send Email” to enable/ disable email notification for the alarm. 7. Click the **Apply** button. Clear Alarm 8. Use the check box for “Clear Now” for the alarm to be cleared. 9. Click the **Apply** button.	Auto-Acknowledge has the has same effect as a manual “Clear Now” (described below). It just does it automatically after the specified number of seconds. Setting this value to zero causes Auto- Acknowledge to be disabled. Information about Transient events is shown indicating that they are not configurable This causes some of the alarm report mechanisms to extinguish that particular alarm indication. These include Dashboard > Alarms, Alarm summary at top of Web GUI, Physical alarm connector, front panel Alarm LED, and Alarm information on front-panel display.This is just an acknowledgement of the alarm, but of course has no ability to impact the underlying condition.
CLI	n/a	
Front Panel	n/a	

6.11 Saving and Restoring Provisioning Data

6.11.1 Backing up Provisioning Data

Table 6-30. Backing Up Provisioning Data

Method	Steps	Notes
Web Interface	Admin > Config Backup/Restore/Reset 1. Enter a password for Backup and Restore. 2. Use the radio button to select “Backup”. 3. Click the “Save As” button. Enter the desired file name and navigate to the desired location to store the file. 4. Click the **Apply** button.	
CLI	n/a	
Front Panel	n/a	

6.11.2 Restoring Provisioning Data

Table 6-31. Backing Up Provisioning Data

Method	Steps	Notes
Web Interface	Admin > Config Backup/Restore/Reset 1. Enter a password for Backup and Restore. 2. Use the radio button to select “Restore”. 3. Navigate to the location of the backup file and select it. 4. Click the **Apply** button.	Password for Backup and Restore should be the same.
CLI	n/a	
Front Panel	n/a	

6.12 Provisioning for SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that allows you to manage network devices. SNMP is based on a client-server query-response mode that requires an Ethernet connection. A manager application (software installed on a computer) is the client generating the queries, and an agent (software on the SyncServer S6x0) is the server generating responses. The SyncServer S6x0 SNMP supports traps and the MIB-II system MIB.

SyncServer S6x0 supports SNMPv2c and SNMPv3. SNMPv3 provides additional security features not available in SNMPv2c. In addition to the functions of SNMPv2c, SNMPv3 allows user and trapuser levels that are based on authentication and privacy settings. The authentication algorithm is either HMAC-SHA-1-96 or MD5, with up to a 32-character key. The privacy settings are based on the AES128 encryption standard.

Port 161 is the port of standard SNMP interactive communications and port 162 is the trap port.

SNMP functionality is provisioned on the SyncServer S6x0 using the web interface.

Note: Changing an SNMP configuration parameter (such as community or SNMPv3 user), will cause SNMP to restart and the MIB2 sysuptime will restart counting upward.

6.12.1 SNMP Status

The SyncServer S6x0 supports a proprietary MIB, S650.mib, which provides selected status information for the unit.

The SyncServer S6x0 also supports selected MIB-II functionality:

- SNMPv2-MIB::system
- IF-MIB::interfaces (ifTable)
- IF-MIB::ifXTable
- RFC1213-MIB::at
- IP-MIB::ipAddressTable
- IP-MIB::icmp
- RFC1213-MIB::tcp (partial support)
- RFC1213-MIB::udp (partial support)
- SNMPv2-MIB::snmp
- IPV6-MIB::ipv6IfTable

6.12.2 SNMP Traps

Each alarm trap OID from the SyncServer S6x0 represents a unique alarm. There are some objects defined in the S650ALARM.mib which are reserved and not supported. If the alarm ID is not listed in Chapter8, Table 8-1, then the corresponding SNMP alarm object is not supported.

Each container contains the following sub-info in its own OID:

- Alarm/Event ID
- Date&Time
- Severity
- Alarm/Event Description
- Index
- Alarm Action
- Sequence Number

The alarm OIDs are under 1.3.6.1.4.1.9070.1.2.5.7.4.1.

The Alarm/Event ID element should be used to determine which alarm or event was generated. Alarm and Event IDs are listed in Chapter 8: System Messages.

Note: The SNMP MIB can be downloaded from the SyncServer S6x0 on the Help web page. The LAST-UPDATED and REVISION fields in the MIB can be used to determine the revision of the MIB. Older versions of the S650ALARM MIB will be compatible with newer versions of firmware, but will not support newer features.

Up to 10 SNMP trap recipients can be configured.

6.12.3 Provisioning to Generate v2 Traps

Use the set snmp trapversion command to provision the trap version to v2.

By default, the SyncServer S6x0 will generate v2 traps.

Table 6-32. Provisioning to Generate v2 Traps

Method	Steps	Notes
Web Interface	Network > SNMP Traps 1. Enter IP address for SNMP manager 2. Select SNMPv2c 3. Enter community name 4. Click "Save"	
CLI	n/a	
Front Panel	n/a	

6.12.4 Provisioning to Generate v3 Traps

Table 6-33. Provisioning to Generate v3 Traps

Method	Steps	Notes
Web Interface	Network > SNMP Traps 1. Enter IP address of SNMP manager 2. Select SNMPv3 3. Enter SNMPv3 user name 4. Enter auth password 5. Select MD5 or SHA for auth 6. Enter privacy phrase 7. Click "Save"	For SNMPv3 traps, both a user and a trapuser need to be configured identically, depending on the SNMP trap manager. In addition, the SNMP manager should use the specified user/trapuser to connect to the SyncServer S6x0. This will ensure that a SNMPv3 trap will be successfully received by the manager using the corresponding trapuser username.
CLI	n/a	
Front Panel	n/a	

6.12.5 Updating v2 Communities

Table 6-34. Adding / Removing v2 Communities

Method	Steps	Notes
Web Interface	Network > SNMP 1. Update user / community names 2. Click “Save”	All character except (<), (&), (>), (“), (') are accepted for SNMPv2 community names.
CLI	n/a	
Front Panel	n/a	

Note: Configuring blank SNMPv2 read and write community names will disable SNMPv2.

6.12.6 Adding and Removing SNMP v3 Users

SNMPv3 provides additional security features not available in SNMPv2c. In addition to the functions of SNMPv2c, SNMPv3 allows user and trapuser levels that are based on authentication and privacy settings. The authentication algorithm is either HMAC-SHA-1-96 or MD5, with a key of up to 32 characters in length. The privacy settings are based on the AES encryption standard, with a key of up to 32 characters in length. All keys are uppercase.

Table 6-35. Adding/Removing SNMP v3 Trap Users

Method	Steps	Notes
Web Interface	Network > SNMP 1. Enter user name 2. Enter privacy phrase if required 3. Enter authentication phrase 4. Select authentication or “authentication & privacy” 5. Select MD5 or SHA 6. Click “Save”	
CLI	n/a	
Front Panel	n/a	

Note: All character except (<), (&), (>), (“), (') are accepted for SNMP usernames, authentication or privacy keys.

6.13 Provisioning HTTPS Certificate

Table 6-36. Provisioning a Self Signed HTTPS Certificate

Method	Steps	Notes
Web Interface	Security > HTTPS > Self Signed Certificate 1. Use the dropdown box to select the RSA Key bit. 2. Enter the Common Name. 3. Enter the Days to Expiration. 4. Enter the ISO Country Code. 5. Enter the State. 6. Enter the Locality. 7. Enter the Organization name. 8. Enter the Organizational Unit. 9. Enter the Email Address. 10. Select check box for Regenerate Keys. 11. Click “Apply”	
CLI	n/a	
Front Panel	n/a	

6.14 Provisioning BlueSky

6.14.1 BlueSky Software Option Specifications/ Requirements

- GPS receiver-equipped SyncServer S600 or S650 models only
- Serial numbers starting with SCA19 or later.
- Software Version 4.1 or later installed in the SyncServer
- Not available for SyncServer S650 SAASM or SyncServer S650 M-Code models
- Enabling the GPS Data Validator Detector will reduce standard NTP operations to a maximum rate of 6000 NTP requests per second. The NTP Reflector timestamping capacity remains unchanged at 360,000 NTP requests per second.

6.14.2 BlueSky Overview

The GNSS BlueSky capability provides an extensive set of detectors that monitor many aspects of GNSS as observed at that specific S6xx installation. General monitoring categories include tracking, spoofing, RF health, and navigation message content. The capability is highly configurable, ranging from observation-only up to use of threshold-driven alarms to automatically restrict use of GNSS as a source of synchronization when specific conditions are detected.

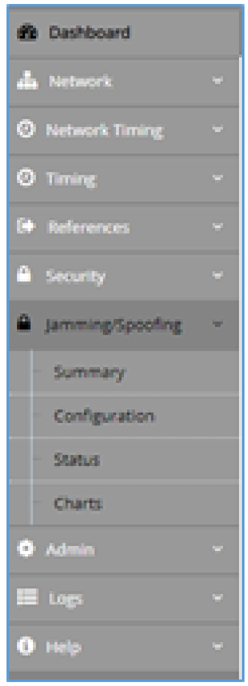
Along with the fundamental detector capability, many results can be charted as well as saved externally for further analysis.

A site-survey monitoring capability is also included that provides an excellent tool for evaluating the actual GNSS tracking capability at the chosen antenna installation. See topic *Site Survey*

6.14.3 Getting Started

The following image shows left panel navigation to access BlueSky capability.

Figure 6-33. BlueSky Navigation - Top Level



Basic steps to get GNSS BlueSky capability up and running:

1. Enable process for any detector groups you want to run.
   These are controlled on BlueSky summary form (Figure 6-34) in the *Action* column and are disabled (not running) from factory. Navigate to this form per Figure 6-33. Use the *Action* column to start running any detector group. The settings will be retained if unit is power-cycled.

   Also, consider enabling GNSS Site Survey on summary form to evaluate the GNSS installation. More about this in the Cumulative Site Survey Chart section.
2. Enable any alarms and associated behaviors.
   Primary alarm enable/disable controls for BlueSky detectors are on the configuration form (Figure 6-35). Navigate to this form per Figure 6-33 These alarms are disabled from factory. Along with basic enable/disable controls, advanced use of these alarms to control GNSS use for sync can also be configured here. See *Alarms and associated controls* for details. Other alarm-specific controls are found on Admin > Alarms form. Scroll to specific BlueSky alarms and configure as desired.

   All of these settings will be retained if unit is power-cycled.
3. Monitor results.
   The status form (navigate per Figure 6-33, see example at Figure 6-37) provides live updates for all detectors.

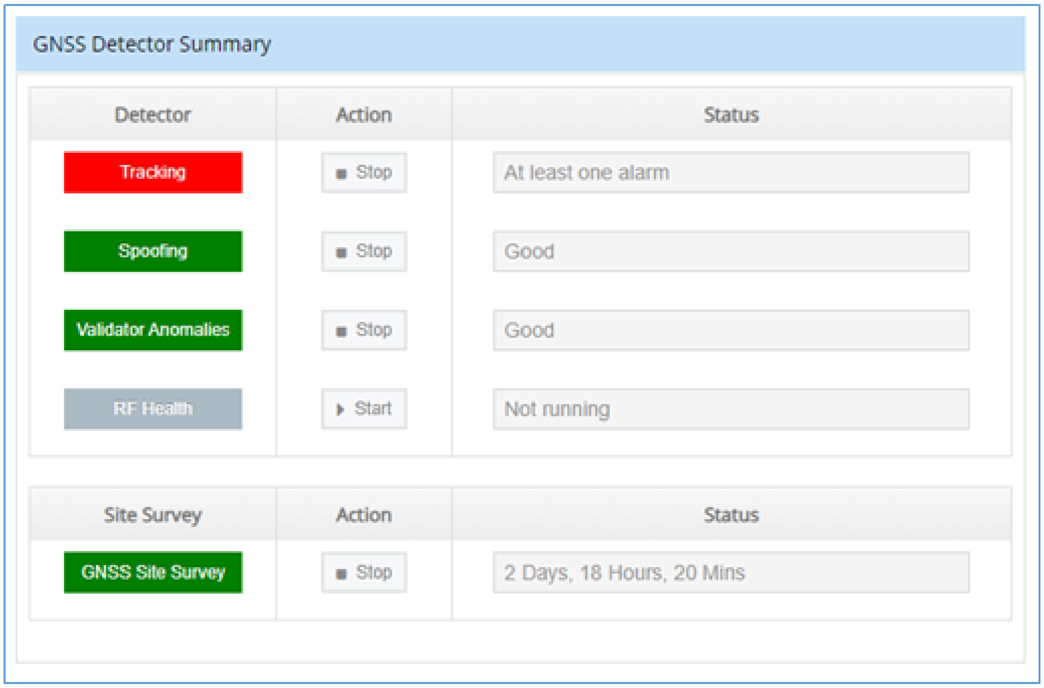
   Many detectors provide charts and download capability. Navigate per Figure 6-33 and see explanations and examples in Charts section

   If alarms have been enabled, they can be monitored using all of the capabilities associated with alarms in general. Also, status form and many charts provide indication of detector results compared with associated thresholds.

6.14.4 Summary Form

The following image shows the BlueSky summary form. This form provides the highest level status view and control capability. Based on what is seen here, you may choose to drill-down to other forms for greater detail.

Figure 6-34. BlueSky Summary Form



General notes on the summary form:

- The *Detector* column provides high-level categorization of BlueSky capabilities (Tracking, Spoofing, Validator Anomalies, and RF Health). These categories (in this same order) are carried through the configuration and status forms.
  Color coding of the detector status:
  - Green: process is running and there are no alarms in this category.
  - Red: process is running and there is at least one alarm in this category (note: alarms can only occur if they are enabled on the configuration form).
  - Gray: the process is not running (user control on this form).
- The *Action* column provides user control to start or stop the process associated with each detector group.
  - The control shows what will happen if the control is selected. For example, if the control shows *Start*, it means the process is currently not running and selecting it will start the process for that detector group. The response is unconditional (there is no way for it to fail).
  - The current state of these controls is retained even if the unit is power-cycled or rebooted, so there is no need to revisit these controls in either of those circumstances.
  - When the next-action control shows *Stop* it always means that the process is currently running. This doesn't always mean it is receiving data, but it will do so whenever data is available. Selecting *Stop* will terminate further data collection for any detectors that are part of that category, but any data collected so far remains available such as charts and ability to download detector data.
  - Selecting *Start* clears any existing data in order to begin a new data collection process for detectors in that group. This action will transition detector column from gray color to green (or red if an alarm is quickly introduced). There is no ability to use this control to "pause" the data collection since the subsequent start will clear out the old.
  - The *Status* column provides additional detail about current condition of detectors in that group. Most notable is indication if there are any alarms currently active within that detector group.

6.14.4.1 Site Survey

The *Site Survey* section at bottom of the Summary form is not a top-level detector group like the rows above it, which is why it is given its own sub-section on the form. Since it has process start and stop control, it fits conveniently on this form. When running, the site survey process generates a sky chart that provides useful information about the tracking capability of the GNSS antenna installation (see section titled *Cumulative Site Survey Chart* for detail).

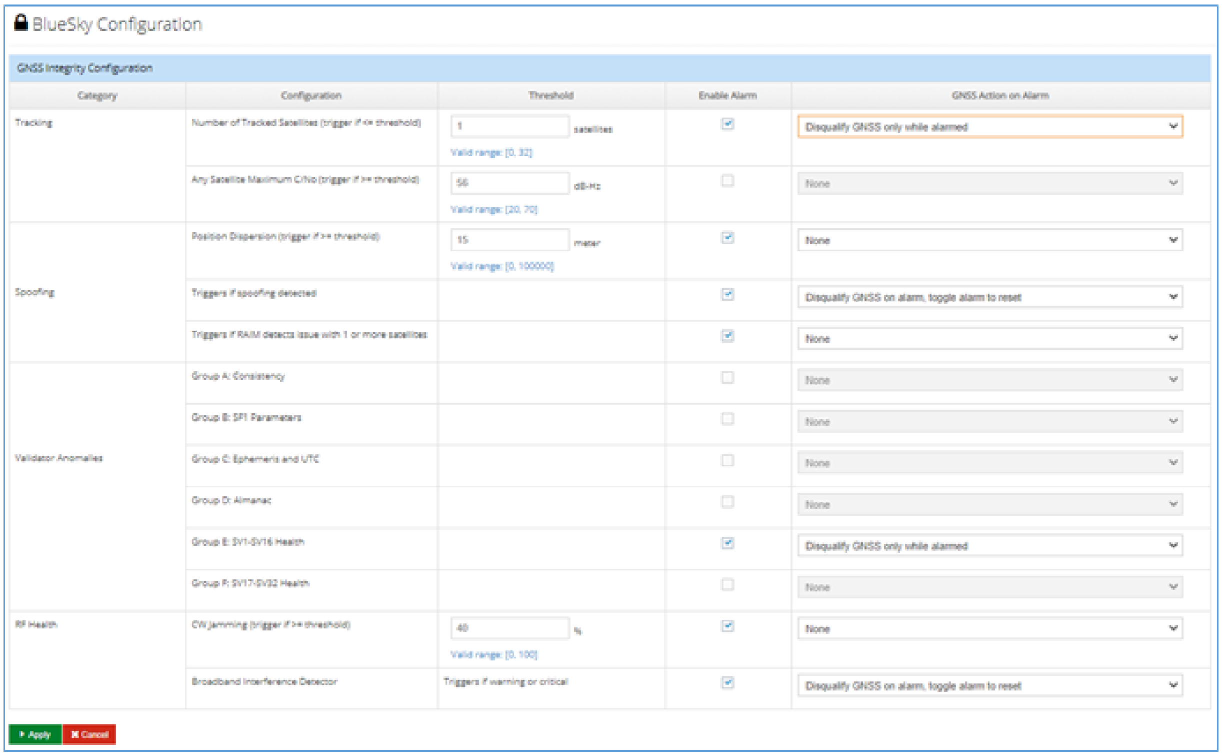
The use of the start/stop action control provides a way to initiate a new accumulation when desired (select stop, then start). Specific function for each column:

- Site Survey column: green if process is running, gray if it is not running.
- Action column: identical to the detector controls. It is used to start or stop the site survey process.
- Status column: when not running indicates: *Not running*. When it is running, this field indicates how long the current site-survey has been running.

6.14.5 Configuration

The following image shows the BlueSky configuration form, which is the single place where almost all configurations related to BlueSky are accomplished (exception: start/stop of detector processes is controlled on the Summary form.

Figure 6-35. BlueSky Configuration Form



6.14.5.1 Category Column

The *Category* column aggregates groups of detectors using the same categories shown on the summary form (Figure 6-34). As an example of use, if 1 or more of the detectors in the *Tracking* group is in an alarm state, this will cause tracking status on summary form to indicate “At least one alarm” and cause the *Tracking* label in left column to highlight red (as shown in the previous image.

6.14.5.2 Detector Details - Tracking Category

This category aggregates detectors that are derived from satellite tracking characteristics.

6.14.5.2.1 Tracking Count

This detector compares a user-set threshold vs. current GNSS total satellite tracking count. As shown in the previous image, a user-entry is provided to set the threshold. The *set* condition occurs when the actual tracking count is equal to or less than user-set threshold. *Clear* condition is tracking count exceeds user-set threshold.

Related items:

- Status form (Figure 6-37) provides current total GNSS tracking count. Field highlights red when set condition is met.
- Tracking count chart (Figure 6-42) provides tracking count history as a stacked-bar chart, partitioned by GNSS constellation. Chart also indicates current user-selected threshold.
- *Save as* allows download of tracking count history, partitioned by constellation.

- Tracking counts can also be seen on dashboard main section as well as Dashboard à GNSS.

6.14.5.2.2 Satellite Maximum CNo

This detector compares a user-set threshold vs. current GNSS Maximum CNo values from all tracked satellites. As shown in the previous image, a user-entry is provided to set the threshold. The *set* condition occurs when the Maximum CNo value is equal to or greater than the user-set threshold. *Clear* condition is Maximum CNo value less than user-set threshold.

Related items:

- Status form (Figure 6-37) provides current Maximum CNo value. Field highlights red when set condition is met. Additionally status form shows individual constellation maximum CNo values.
- Maximum CNo chart (Figure 6-49) provides maximum CNo history. Chart also indicates current user-selected threshold.
- *Save as* download provides overall maximum CNo history as well as individual constellation maximums.

6.14.5.3 Detector details – Spoofing Category

This category aggregates detectors that are associated with spoofing or possible outlier satellite behavior.

6.14.5.3.1 Position Dispersion

This detector compares a user-set threshold vs. a current calculated “position dispersion”. This metric can detect erroneous position entries as well as timing anomalies that may be introduced due to use of satellites that exhibit outlier behavior (for whatever reason). As shown in the previous image, a user-entry is provided to set the threshold. The *set* condition occurs when the current position dispersion value is equal to or greater than user-set threshold. *Clear* condition is current position dispersion less than user-set threshold.

Related items:

- Status form (Figure 6-37) provides current position dispersion value. Field highlights red when *set* condition is met.
- Position dispersion chart (Figure 6-47) provides position dispersion history. Chart also indicates current user-selected threshold.
- *Save as* download provides position dispersion history.

6.14.5.3.2 Spoofing

This detector monitors for unusual changes in GNSS signals that could be indicative of external manipulation. The detection methods rely upon multiple GNSS constellations being included (configurable at References > GNSS Config). Successful use of this detector depends upon S6xx starting up with legitimate signals. There is no user-assignable detection threshold since the only possible results are as shown in Table 6-39 along with associated detector condition mapping.

6.14.5.3.3 Receiver Autonomous Integrity Monitor (RAIM)

RAIM provides a capability to identify and reject use of satellites based on outlier contribution to potential solutions. This detection is possible when there are more satellites available than are needed for actual solution, which is a typical condition due to the generally high-availability of trackable satellites. If an individual satellite becomes associated with multiple outlier candidate solutions, it may be “RAIMed out” (removed from use in solution).

There is no user-assignable detection threshold since the only possible results are as shown in Table 6-37 along with their detector mapping. Additional RAIM-related content is provided on status form (Figure 6-37).

Table 6-37. Possible RAIM detector responses

Satellite ID reported result on status form	Detector condition
0	clear
Non-zero (PRN of RAIMed satellite)	set

6.14.6 Detector Details – Validator Anomalies Category

This category aggregates detectors that evaluate received GPS navigation messages against a variety of defined rules such as consistency (message-to-message, satellite-to-satellite) and illegal conditions such as out of range parameters.

Since each rule evaluates to either FAIL (detector condition set) or PASS (detector condition clear) there are no user-configurable detection thresholds.

Note: The Validator detector only evaluates GPS satellites, and does not monitor satellite signals from other constellations.

Related item: The BlueSky status form (Figure 6-37) provides current status for every validator anomaly rule. Further details are provided in the section *Validator Anomalies status*.

6.14.7 Detector Details – RF Health Category

This category aggregates detectors that are associated with RF input conditions presented at the GNSS input connection (labeled “GNSS”).

6.14.7.1 CW Jamming

This detector assesses strength of interfering CW (continuous wave) signals that may be present at the GNSS connection. CW interference closer to GNSS satellite RF center frequencies (not all are same) will result in higher jamming values.

The CW jamming detector compares a user-set threshold vs. the current measured jamming percentage. As shown in Figure 6-35, a user-entry is provided to set the threshold. The *set* condition occurs when the current CW jamming percentage is equal to or greater than user-set threshold. *Clear* condition is current CW jamming percentage less than user-set threshold.

While normal jamming levels will be site and installation-dependent, a typical jamming level for an install where there are no significant issues will result in values < 10%.

Related items:

- Status form (Figure 6-37) provides current CW jamming value. Field highlights red when set condition is met.
- CW Jamming chart (Figure 6-51) provides metric history. Chart also indicates current user-selected threshold.
- *Save* as download provides CW Jamming history.

6.14.7.2 Broadband Interference

This detector responds to both CW and broadband interference. Unlike the CW Jamming detector which provides a 0 – 100 percent measure, this detector provides states as indicated in the following table. The *warning* state indicates that jamming is suspected although there likely is no direct impact on satellite tracking capability. The *critical* state indicates a higher detection level and likely results in inability to use satellites for timing (could result in S6xx in holdover state).

Table 6-38. Possible broadband interference detector responses

Reported on status form	Detector Condition
Unknown	Detector is clear
OK	Detector is clear
Warning	Detector is set
Critical	Detector is set

6.14.8 Alarms and Associated Controls

Every detector row in the previous image provides an identical independent set of alarm-related controls. So, while each detector has unique behavior, the control and response of alarms associated with detectors are all the same. If you understand how it works for one detector, you understand how it works for all of them.

For reference, all alarms associated with the BlueSky functionality are shown in Figure 6-52 and Figure 6-53, as presented on the Admin > Alarms form. These figures show that the BlueSky alarms are not “special” alarms but are foundationally part of the generic alarm system for S6xx products. These alarms support the same set of basic controls that all other alarms support (for example, control of alarm severity).

The BlueSky alarms **do** introduce additional capabilities that go beyond generic alarm capabilities. These are all configured on the Configuration form, shown in the previous image, and details are covered in following sections.

A note on terminology: References are made to whether or not a detector condition is set or clear. This is the underlying condition determined by the current status of the detector and whatever threshold may currently exist (in some cases user settable). Just because a detector is set does not mean that its associated alarm is also set as will be covered in the next section.

6.14.8.1 Alarm Enable/Disable

Every detector row in the Configuration form, shown in the previous image, provides an alarm enable/disable checkbox for that detector. This adds a layer of alarm function that does not exist for other S6xx alarms, allowing "per detector" control of which ones can produce alarms. The functionality provided by the checkbox for a given detector is:

- When checked (and applied) the detector will actually set and clear alarms per the detector set/clear descriptions provided earlier in this section.
- When unchecked, no actual alarms will be produced by this detector. Additionally, if the alarm had been set at time of "uncheck" (and apply), the alarm will clear (because it has been user-disabled).

For example, Configuration format has the first row detector (Number of tracked satellites) alarm enabled and 2nd row detector (max CNo) detector alarm disabled. This means that the *BlueSky GNSS tracking count detector* alarm is currently operational (able to generate alarms) but the *BlueSky GNSS max CNo detector* alarm is not.

6.14.8.2 Specific Detector Alarms

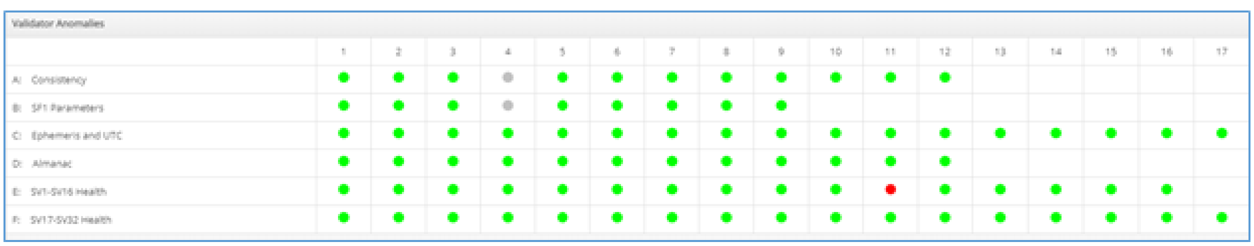
Every detector has its own alarm, controlled by the enable/disable selection covered in prior section. The naming of these alarms can be seen in Figure 6-52 and Figure 6-53, taken directly from the generic alarm configuration form at Admin > Alarms. Here's an example of how set and clear alarm indications for tracking count detector appear in the message log (Log > Messages).

Apr 14 18:36:03	SyncServer alarmd:	Id: 186, Index: 000, Severity: major, Alarm: set, Msg: Bluesky GNSS tracking count detector
Apr 14 18:37:35	SyncServer alarmd:	Id: 186, Index: 000, Severity: major, Alarm: clear, Msg: Exit bluesky GNSS tracking count detector

The *validator anomalies* detector group presents a special situation because there are numerous individual detectors. While the alarm enable/disable control is one-per-row for the A-F rows (see Figure 6-35), each row contains many detectors, all of which are presented on the BlueSky status form (see Figure 6-37). The actual alarm reporting accommodates this by adding column content when identifying validator alarms. For example, the figure below shows a message log entry for validator row E alarm being set. The label appends that this one is column 11. The net effect is that every rule has a unique alarm even though the enable/disable control is "per row".

Id: 199, Index: 011, Severity: major, Alarm: set, Msg: BlueSky GNSS validator E 11 detector

The sub-portion of the status form shows that the "LED" in row E, column 11 is red. This shows the correspondence between alarm reporting and status form indication. In this case we say that the validator rule condition associated with E 11 is currently FALSE which has illuminated the LED and caused the actual alarm shown from message log (because the E row has alarm enabled).



6.14.8.3 Use of Detector Alarms to control GNSS Qualification Behavior

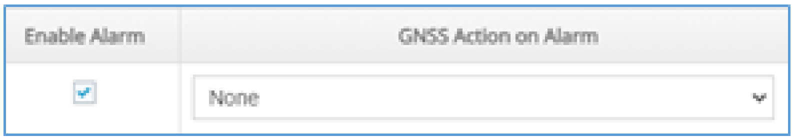
The behaviors covered in this section are common to every BlueSky detector. Before getting into details, it is worth covering the high level:

- Alarms and behaviors covered here are only possible when the associated detector alarm is enabled (covered in prior section *Alarm enable/disable*).
- Both controls covered here provide the ability to disqualify the use of GNSS as a source of synchronization for S6xx. This is a powerful capability and so these specific alarms are provided to inform whenever this becomes a reason for GNSS not being used.

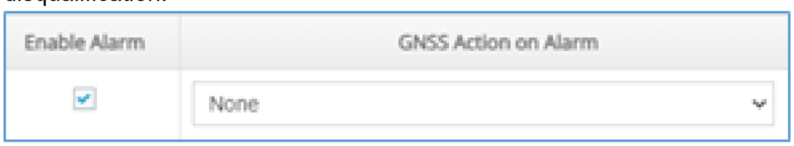
The control method is shown on Figure 6-35. Look at rightmost column titled *GNSS action on alarm*. This is a drop-down list that provides all of the needed control. Examples of each are shown in that figure.

- Degenerate case: The base alarm for the detector is not enabled, so the GNSS actions are not considered. In this case the drop-down list box is grayed out indicating that it is not functional. Example shown below: the alarm enable is not checked so the advanced control (the subject of this section) is grayed out as indication that it is not functional and not selectable. Several examples are shown in Figure 6-35.

- Alarm enabled, list box set to *none*. This is also a degenerate case for the advanced GNSS qualification behavior. With this setting the detector will produce normal alarms but no GNSS action is taken when alarm is set. Several examples are shown in Figure 6-35.

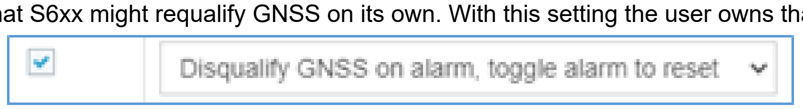


- Alarm enabled, list box set to *Disqualify GNSS only while alarmed*. This setting causes this detector to prevent GNSS from being used as a possible time and frequency reference whenever the detector alarm is set. Whenever the detector alarm is NOT set (i.e. it is cleared) this detector will not be a reason for GNSS disqualification.



  The alarm associated with this reason for GNSS disqualification is shown here and will set and clear just like any other alarm.

- Alarm enabled, list box set to *Disqualify GNSS on alarm, toggle alarm to reset*. This setting causes this detector to prevent GNSS from being used as a possible time and frequency reference whenever the associated detector alarm is set. Additionally, if the underlying detector alarm clears, this setting does **not** release (allow) GNSS for possible use as a sync reference. As the setting indicates, once this alarm sets, if the user is ready to re-allow GNSS to qualify for use as a sync reference, they need to toggle the alarm enable/disable control (the check box) off (with apply) then on again (with apply). This setting allows user to investigate the issue without concern that S6xx might requalify GNSS on its own. With this setting the user owns that action.



  Here is the actual alarm that indicates that GNSS is disqualified due to this setting:

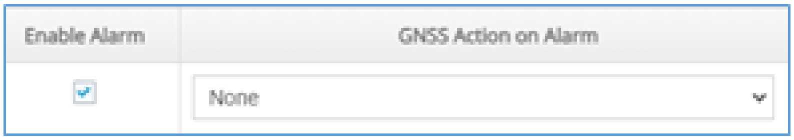
6.14.8.4 GNSS Disqualified Behavior with Multiple Detectors Alarmed

Prior section describes how any single BlueSky detector can be configured for alarms and control of GNSS qualification in relation to that detectors alarm. This section illustrates how the behavior extends into cases where multiple detectors are alarmed with the various GNSS-related qualification configurations.

Figure 6-36 provides an abstract representation used for explanation. The left block is like the alarm portion of configuration form (see Figure 6-35) with the 3 narrow columns on right representing the enable alarm control and the other 2 possible selections where GNSS can become disqualified (using the drop down list box). The “none” choice is implied by neither of the right-most columns being checked. The 2 boxes on the right are the BlueSky GNSS disqualification alarms.

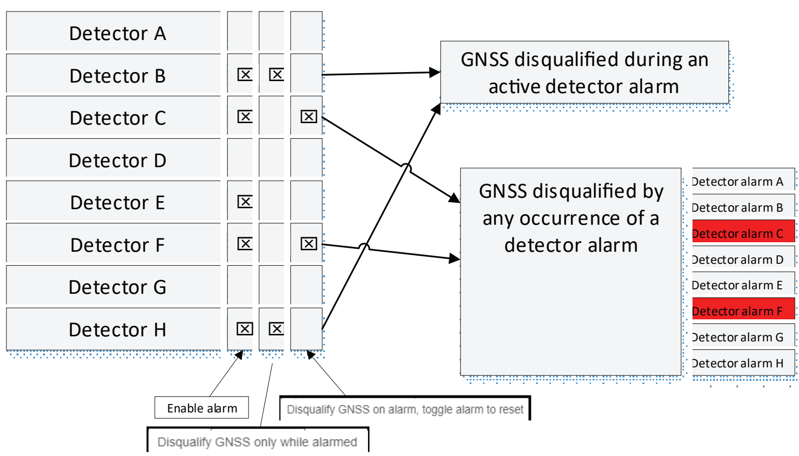
Walking through the figure:

- Detectors with no X in the *Enable alarm* column cannot produce any alarm. These are Detectors A, D, and G.
- Detectors with X only in Enable alarm column are configured as shown in the following image, and therefore can alarm but never impact GNSS usage. This is only detector E.



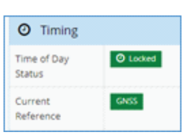
- Detectors with X in *Enable alarm* and X in *Disqualify GNSS only while alarmed* will drive their own detector alarm and ALSO drive the *GNSS disqualified during an active detector* alarm whenever their detector alarm is set. Since only detectors B and H are configured this way they have arrows connected to this alarm to indicate that they alone currently can drive it (and its consequent behavior covered in prior section)..
  The *GNSS disqualified during an active detector* alarm will be set (and result in GNSS being disqualified for use as a sync reference) when **any** detector connected to it is alarmed. This alarm will be clear only when **all** detector alarms connected to it are clear.
- Detectors with X in *Enable alarm* and X in *Disqualify GNSS on alarm, toggle alarm to reset* will drive their own detector alarm and ALSO drive the *GNSS disqualified by any occurrence of a detector* alarm whenever that base detector alarm is set. Since only detectors C and F are configured this way they have arrows connected to this alarm to indicate that they alone currently can drive it (and its consequent behavior covered in prior section). The *GNSS disqualified by any occurrence of a detector* alarm will be set (and result in GNSS being disqualified for use as a sync reference) when **any** detector connected to it becomes alarmed. As covered in prior section this alarm will not clear even if the underlying driving detector alarm clears. Notice that this box shows a right-hand column listing each of the detectors. This is illustrating that this alarm retains (and reports to user) the detector(s) that are responsible for this alarm to being set. This is needed because, even if all of the detectors that have caused this alarm to set have themselves become cleared, this alarm will remain set. In that situation the user still needs to know why this alarm is set; having the alarm report the sourcing detectors provides this information.

Figure 6-36. BlueSky Alarm Releationships



6.14.8.5 Example 1: Multiple detectors alarmed with Disqualify GNSS only while alarmed setting

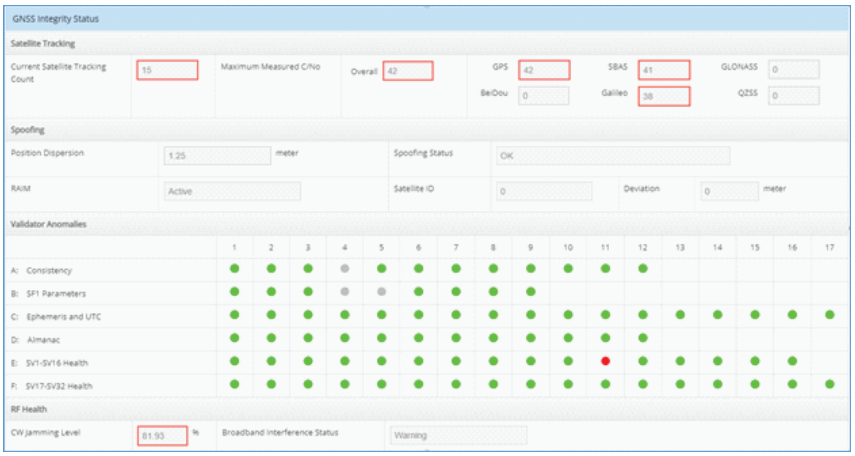
This scenario begins with S6xx locked to GNSS.



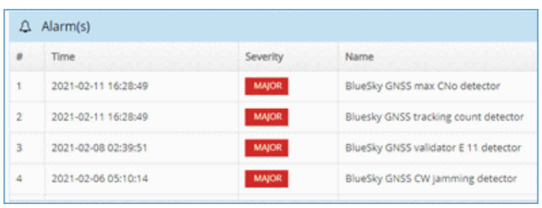
We use the detectors shown below for the example since they are easy to trigger via configuration. Notice that, to easily cause detectors to set, these thresholds are set to values that typically **would** trigger the alarm, but in normal use they would be set to values that could be cause for concern if the detectors became set. The alarm for each is enabled but no GNSS action.

Looking at the status form we see these detectors are outlined in red:

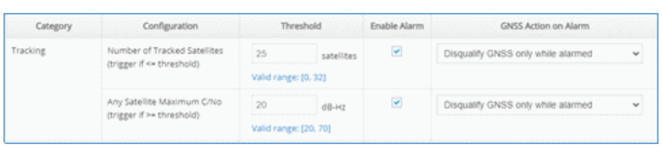
- Tracked satellites detector shows it is set because 15 is less than 25 (configuration setting above)
- Max CNo detector shows it is set because 3 constellations are each having a max value above the threshold set above (20).



On Dashboard > Alarms we see the indication that all of these detectors are actually generating alarms (associated alarm enable is set for each of them). In this case they are all set to severity of Major, but that can be controlled on Admin > Alarms.

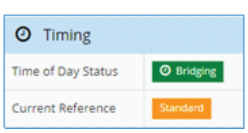


Now, add the *GNSS Action on Alarm* setting shown below for only these detectors. Recall that with this setting if either of these detectors is actually alarmed (the detector must be set and configured with alarm enable for that to occur as is the case here) then GNSS will be disqualified from use as a sync reference. Only if both of them are NOT alarmed will GNSS be allowed to try to qualify.



In normal usage the above setting would have likely been made at the time the alarm was originally enabled, so when an alarm first set for either detector that would have immediately disqualified GNSS. For purposes of illustration, this action is added later just to show the incremental functionality of the controls.

Upon configuring per above we see that this S6xx goes into Bridging since GNSS is no longer allowed to qualify.



A little while later we end up in holdover, which is the normal progression on loss of reference.

Timing	
Time of Day Status	Bridging
Current Reference	Standard

We see below that we have the GNSS disqualified during an active detector alarm additionally set, allowing the user to understand why the S6xx is now in holdover. Notice that this alarm (unlike the next example) does not explicitly identify the detector alarm(s) that are causing it to be set. The reason for that is that it MUST be the case that one or more currently set detector alarms are the reason, in this case it is *max CNo* and *tracking count*. If the user isn't sure which of these are driving it, it is a simple matter to look at the configuration form: only those configured with this *GNSS Action* can be the drivers. Although not shown, for this example the configuration form shows that the *validator E 11* and *CW jamming* alarms are enabled but the GNSS Actions are set to none for both of them. They have no impact on GNSS qualification.

1	2021-02-11 16:33:45	MAJOR	GNSS disqualified during an active detector alarm
2	2021-02-11 16:28:49	MAJOR	BlueSky GNSS max CNo detector
3	2021-02-11 16:28:49	MAJOR	Bluesky GNSS tracking count detector
4	2021-02-08 02:39:51	MAJOR	BlueSky GNSS validator E 11 detector
5	2021-02-06 05:10:14	MAJOR	BlueSky GNSS CW jamming detector

The thresholds for these detectors are changed so that the detector conditions are cleared. Of course, in real usage this represents the underlying condition changing – it is not the normal use-case that the user would simply change the thresholds to make the alarm go away!

Tracking	Number of Tracked Satellites (trigger if <= threshold)	1 satellites Valid range: [0, 32]	☑	Disqualify GNSS only while alarmed
	Any Satellite Maximum C/No (trigger if >= threshold)	60 dB-Hz Valid range: [20, 70]	☑	Disqualify GNSS only while alarmed

In reaction to above change, we immediately see that the remaining alarms are only for the other detectors. Because both of the detectors associated with GNSS disqualification have cleared, the GNSS summary alarm has also gone away. The S6xx proceeds to relock to GNSS since the reason for not allowing GNSS for sync has been removed.

Alarm(s)

#	Time	Severity	Name
1	2021-02-08 02:39:51	MAJOR	BlueSky GNSS validator E 11 detector
2	2021-02-06 05:10:14	MAJOR	BlueSky GNSS CW jamming detector

6.14.8.6 Example 2: Multiple detectors alarmed with Disqualify GNSS on alarm, toggle alarm to reset setting

This is similar to the prior example except now we use the other GNSS disqualification setting as shown below. Once again, these detectors are set to values where both detector conditions will be set.

Tracking	Number of Tracked Satellites (trigger if <= threshold)	23 satellites Valid range: [0, 32]	☑	Disqualify GNSS on alarm, toggle alarm to reset
	Any Satellite Maximum C/No (trigger if >= threshold)	20 dB-Hz Valid range: [20, 70]	☑	Disqualify GNSS on alarm, toggle alarm to reset

Here's the resulting Dashboard > Alarms. Notice now that along with the individual detector alarms, each one has caused an independent disqualification alarm. They are both of the form: GNSS disqualified by occurrence, but each one explicitly names the specific detector that is causing it. The reason we need this is that, with this GNSS disqualification setting, the reason for disqualification does not go away even if the detector alarms clear, so some sort of "history trail" is needed with the GNSS disqualification alarms themselves.

Alarm(s)

#	Time	Severity	Name
1	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of max cNo detector alarm
2	2021-02-11 17:57:22	MAJOR	BlueSky GNSS max CNo detector
3	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of tracking count detector alarm
4	2021-02-11 17:57:22	MAJOR	Bluesky GNSS tracking count detector

As expected, the GNSS disqualification alarms cause the S6xx to end up in holdover:

Timing	
Time of Day Status	Holdover
Current Reference	Standard

Next, change thresholds so that the underlying detector conditions will be cleared which should also clear the base detector alarms.

Category	Configuration	Threshold
Tracking	Number of Tracked Satellites (trigger if <= threshold)	1 satellites Valid range: [0, 32]
	Any Satellite Maximum C/No (trigger if >= threshold)	60 dB-Hz Valid range: [20, 70]

In response, we see the base detector alarms are gone, but the GNSS disqualification alarms remain as they should. These alarms don't clear unless the user toggles the base alarm off, then on. Because these alarms actually name the detector that is responsible it, the user always knows which detectors (whether they are currently alarmed or not) are responsible for the GNSS disqualification. If it is desired to re-allow use of GNSS, the alarms always identify which specific detectors need to have their alarms toggled.

#	Time	Severity	Name
1	2021-02-11 18:02:23	MINOR	Entered time holdover state
2	2021-02-11 18:02:22	MINOR	Entered freq holdover state
3	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of max cNo detector alarm
4	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of tracking count detector alarm

Going to the configuration form, the alarm for *max CNo* detector is disabled (and applied), then re-enabled (and applied). This is the user action to clear out a “disqualified by occurrence …” alarm for any detector. Of course, it won't work if the underlying detector condition happens to still be set. Since this action was only taken for max CNo alarm, the GNSS disqualification condition remains due to the tracking count detector continuing to be set.

#	Time	Severity	Name
1	2021-02-11 18:02:23	MINOR	Entered time holdover state
2	2021-02-11 18:02:22	MINOR	Entered freq holdover state
3	2021-02-11 17:57:22	MAJOR	GNSS disqualified by occurrence of tracking count detector alarm

Performing the same alarm toggle action for the tracking count detector clears the above alarm as well. This eventually leads to re-lock of GNSS since there are no remaining GNSS disqualification alarms.

Timing	
Time of Day Status	Locked
Current Reference	GNSS

6.14.8.7 Special Case alarm behavior

While the BlueSky alarms are fundamentally generic S6xx alarms, because they have added unique controls there are alarm-related behaviors that are unique to these alarms:

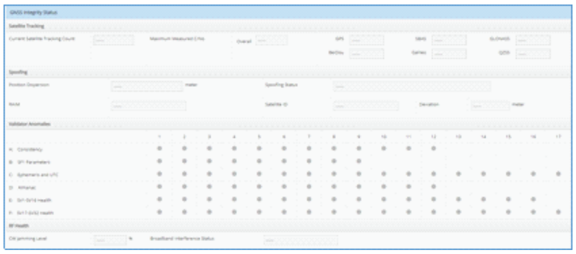
- If the alarm enable/disable control for a detector is changed from enabled to disabled when that detector is alarmed, the alarm will clear. Also, any support that alarm was providing for GNSS-related alarms (see section *Use of Detector Alarms to control GNSS Qualification Behavior*) will be removed.
- If the alarm enable/disable control for a detector is changed from disabled to enabled when that detector condition is set, then its alarm will set.
- If a detector group process is stopped when there are alarms currently set for any detectors in that group, those alarms will clear. Also, if there are any GNSS-related alarms connected to any base detector alarms in that group, they will also clear.

6.14.9 Status

Figure 6-37 shows the status form which provides live updates (most recent status) for all detectors. Some general notes about the form:

- All status results are lost if unit is rebooted/power-cycled. However, many of the charted results (see *Charts* section) can be saved to external storage.

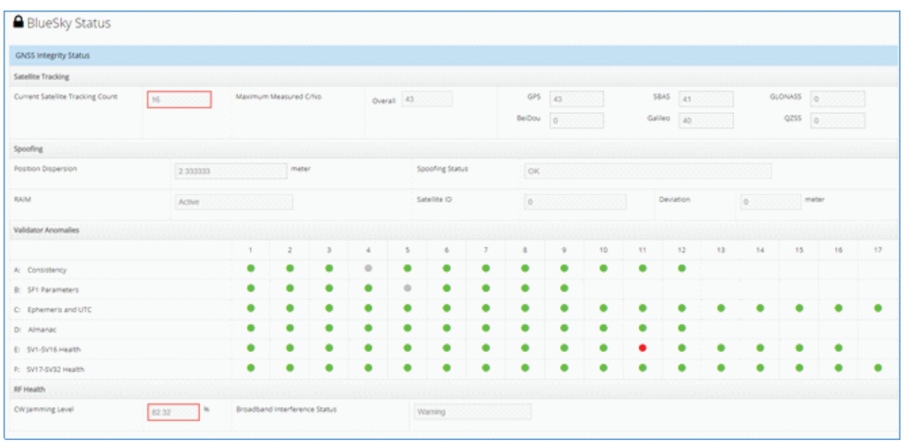
- The 4 major groups (*Satellite Tracking*, *Spoofing*, *Validator Anomalies*, and *RF Health*) align with groupings provided on *Detectors* (summary) and *Configuration* forms. This scheme helps to organize a reasonable hierarchy for usability: BlueSky > Detector groups > Individual detectors. The utility of this approach is shown by looking at Figure 6-34, which summarizes that only the Tracking group currently contains an alarmed detector. User can then drill down by looking at status form to see which specific detectors are responsible.
- While results on the status form self-update, the rate at which values update are not all the same. The form has the capacity to update at a generally fixed interval (around 5 seconds) but the underlying detectors can have different rates at which they produce new data.
- If the process is not running for a detector group (controlled on detector summary form, see *Summary form*), the results in that group will be appropriately indicated as unavailable. Figure below shows what status form looks like with **all** detector groups not running.



- Assuming that a given detector process is running, if a specific detector condition is set (meets or exceeds its threshold, which in some cases is user-configurable) the set condition will be indicated on the status form, regardless of whether it is configured to actually generate alarms. The is the one place to always see detector *condition*. Whether or not a detector that is set will propagate information beyond this form depends upon the setting of the associated alarm enable/disable control (see Figure 6-35). When alarm is enabled, then the set condition will drive all alarm-related behaviors. When the alarm is not enabled, the set condition becomes information-only content highlighted on the status form.

From the example shown in Figure 6-37, it is easy to see the detectors that are currently set (does not necessarily mean alarmed). For the Validator Anomalies group, this condition is shown with a red dot, for all other detectors the value is outlined in red.

Figure 6-37. Example - BlueSky Status Form



6.14.9.1 Tracking Count Status

This detector shows the current satellite tracking count. When the value is equal to or less than threshold configuration (see Figure 6-35) it will be outlined in red.

Related items:

- Tracking count threshold can be set on configuration form (Figure 6-35).
- Tracking count chart (Figure 6-42) provides tracking count history as a stacked-bar chart, partitioned by GNSS constellation. Chart also indicates current user-selected threshold.
- *Save as* (Figure 6-42) allows download of tracking count history, partitioned by constellation.
- Tracking counts can also be seen on dashboard main section as well as Dashboard à GNSS.

6.14.9.2 Satellite Maximum CNo Sstatus

This detector shows the current overall highest CNo (Carrier-to-Noise Ratio) of all currently tracked satellites. When the value is equal to or greater than threshold configuration (see Figure 6-35) it will be outlined in red.

Additional status showing CNo maximums for individual GNSS constellations is also provided.

Related items:

- CNo maximum threshold can be set on configuration form (Figure 6-35).
- Maximum CNo chart (Figure 6-49) provides maximum CNo history. Chart also indicates current user-selected threshold.
- *Save as* allows download of CNo maximum history, including partitions by constellation.
- Current CNo can also be seen on Dashboard > GNSS as well as *Current Sky View* chart by hovering mouse over any satellite.

6.14.9.3 Position Dispersion Status

This detector shows the current position dispersion value. This metric is used to detect erroneous position entries as well as timing anomalies that may be introduced due to tracking and use of satellites that exhibit outlier behavior (for whatever reason). When the value is equal to or greater than user-set threshold (see Figure 6-35) it will be outlined in red.

Related items:

- Position dispersion threshold can be set on configuration form (Figure 6-35).
- Position dispersion chart (Figure 6-47) provides position dispersion history. Chart also indicates current user-selected threshold.
- *Save as* download provides position dispersion history.

6.14.9.4 Spoofing Status

Current status for the spoofing detector is next to title in Spoofing group labeled *Spoofing Status*. This detector monitors for unusual changes in GNSS signals that could be indicative of external manipulation. The detection methods rely upon multiple GNSS constellations being included (configurable at References > GNSS Config). Successful use of this detector also depends upon S6xx starting up with legitimate signals. The possible status responses and relationship to detector set/clear are shown in Table 6-39. If the detector is set, the status field will be outlined in red.

Table 6-39. Possible Spoofing Detector Responses

Reported on Status Form	Detector Condition
Unknown	Clear
OK	Clear
Spoofing indicate	Set

6.14.9.5 RAIM Status

RAIM (Receiver Autonomous Integrity Monitor) provides a capability to identify and reject use of satellites based on outlier contribution to potential solutions. This detection is possible when there are more satellites available than are needed for actual solution, which is a typical condition due to the high-availability of trackable satellites. If an individual satellite becomes associated with multiple outlier candidate solutions, it may be “RAIMed out” (removed from use in solution).

There is an entire row associated with RAIM status, found in the *Spoofing* group. The RAIM-related fields in that row are labeled RAIM, Satellite ID, and Deviation.

- The RAIM field status provides an indication of current system capability to use RAIM. For example, conditions with too few tracked satellites might not allow RAIM to function. The possible responses in this field are
  - Inactive or Unknown: RAIM detector not currently able to make decisions
  - Active: RAIM able to make decisions (doesn’t mean that there is a RAIM detection set)

  There is no set/clear threshold associated with this status.

Table 6-40. Possible RAIM Satellite ID detector responses

Satellite ID reported result on status form	Detector Conditon
0	Clear
Non-zero	Set

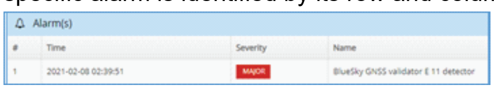
- The Satellite ID field provides the status used to set/clear this detector, as shown in Table 6-40. There are no user-definable detection thresholds. In the event that there is more than one satellite being RAIMed, the ID indicates the one with the greatest bias. When the detector is set, this field is outlined in red.

6.14.9.6 Validator Anomalies Status

This category aggregates detectors that evaluate received GPS navigation messages against a variety of defined rules such as consistency (message-to-message, satellite-to-satellite) and illegal conditions such as out of range parameters.

Figure 6-37 shows the status presentation for the validator anomalies detector group. Every small circle (looks like an LED) represents a specific rule (detector) that is evaluated in the GPS navigation message. There are 6 distinct rows (A – F) each of which has the standard set of detector configuration controls (see Figure 6-35). Those controls apply to all of the rules (detectors) in that row. Key points:

- Each detector is capable of producing a unique alarm. For example, when the E row is configured with alarm enabled, the detector at E11 produces alarm shown below. This is the general form for all validator alarms, the specific alarm is identified by its row and column.



- The alarm and GNSS action control level for each detector is for the entire row associated with that detector. For this example, since E11 is generating an alarm, any detector in row E is capable of generating an alarm. So, if the E5 and E7 detectors were also set then we would have 3 distinct alarms currently active.
- For the GNSS-action behavior (see detailed description in *Use of Detector Alarms to control GNSS Qualification Behavior*) if **any** alarm is set for a given row then that GNSS-action applies.
- Each detector (the small circles) evaluates its specific rule for every tracked GPS satellite. The condition for the detector to set is if at least one satellite evaluates to FALSE (it is failing the test associated with that rule). For example, if we are tracking 7 GPS satellites then every rule is running 7 tests whenever its opportunity to run occurs. If only one of the 7 per-satellite tests of that rule fails, then that detector sets. In this release the specific satellite (or satellites) that are responsible for a detector being set are not identified. You can infer from a “red dot” that at least one satellite has failed the test.

6.14.9.6.1 LED Behavior

The status shown for each rule has the following meanings:

- Green dot: the most recent update of this rule found NO rules violations from any tracked GPS satellite. Also, there have been tracked GPS satellites within the timeout period (otherwise this dot would be gray).
- Red dot: the most recent update of this rule had **at least one** rule violation from a tracked GPS satellite. Also, there have been tracked GPS satellites within the timeout period (otherwise this dot would be gray).
- Gray dot: This rule has either a) not ever run since the validator anomaly process (see Figure 6-34) was started or b) no GPS satellites have been tracked for a *timeout* period. Currently timeout = about 15 minutes. This condition should be thought of as: status of this rule is unknown.

6.14.9.6.2 Rule Groupings

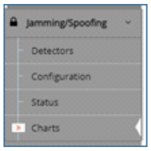
The A – F categories are generally grouped around navigation message subframe groups and their general content, which is reflected in the group names. Groups E and F represent general operational status conditions (e.g. satellite health) whereas the other groups are associated with anomalous behaviors that could be indicative of a variety of problems.

6.15 Charts

The chart section of the S6xx BlueSky capability provides a powerful set of tools to evaluate satellite-related current and historic behavior.

6.15.1 General Characteristics

Access all charts via this navigation:



Once there the following properties apply (use Figure 6-40 for description):

- A drop-down list box provides control of which chart will be viewed. Changing the selection will directly bring up the selected chart.
- If data associated with the viewed chart can also be downloaded to external storage a “save as” control is provided at bottom of form.
- For charts that support “save as”, the data can be downloaded at any time without impacting the data collection process.
- Every form has a *Refresh* control, but the functionality is not the same for each chart. Detail is provided with each chart description.
- Some charts do not self-update and sampling rates (how often new data may be available to update a chart) are not the same for every chart. In general, data update rates are in the range from 2 to 5 minutes.
- Navigating to any chart will always provide the most recent available data.
- For charts that provide specific detail about individual constellations, the color-mapping of these constellations is consistent across all charts. Along with this, the same color mapping is used on Dashboard > GNSS graphical presentation.
- In general, user-controls on the charts such as chart type, zoom range (some charts), and anything else are NOT remembered upon form exit and re-entry.

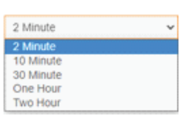
6.15.2 Common Attributes of Vs Time Charts

There are currently 4 charts that have the x-axis as time. They are the Tracked Satellites, Position Dispersion, Maximum C/No, and CW Jamming charts. While they all have different y-axis content, they share behaviors on x-axis. This section provides a common reference for those behaviors.

- All of these charts self-update. When new data is sampled the chart will automatically update to show it.
- The sampling interval for new data is approximately 2 minutes.
- The “NOW” time is the right-side of the graph. A good way to think of it is like a strip chart recorder: the older “recorded” data continues to slide more and more to the left to make way for the newer data. The most recent data is always far right.
- The data associated with each chart is driven from a 21,600 sample database. Since the data sampling interval is 2 minutes, the database can hold (2 min) x (21600) = 43200 minutes = 30 days before it fills. Upon filling, all databases drop oldest data to incorporate newest data.
- All of these charts have user-configurable thresholds (see Figure 6-35) that can be used to generate alarms when crossed. The appropriate current threshold is shown (red horizontal line) on each of these charts to allow visual comparison of actual collected data vs. the threshold. The thresholds are shown regardless of whether or not they are configured to actually generate alarms upon being crossed.

6.15.2.1 Zoom behavior

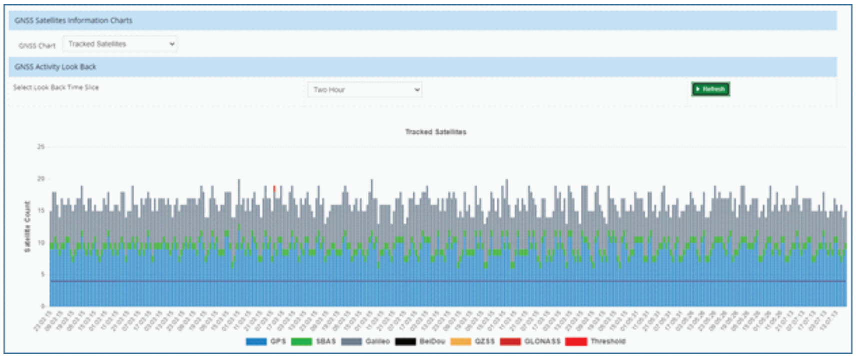
Because these charts are supported by such large amounts of underlying data, zoom controls are provided with similar behavior on all of them. Figure 6-42 and Figure 6-38 are used here to help explain, both of which show tracked satellites charts but with the extreme ranges of zoom capability. The zoom control is in the row above the chart that is labeled *Select Look Back Time Slice*. The user zoom control is the drop-down list box in the center which has the choices shown below.



The control indicates the time interval between data points that will be shown on the chart. This control setting does not alter the rate of data collection into the database; it is purely a chart visual control. To update the chart with a new "zoom" selection, select *refresh* at the right end of this row.

The 2-minute interval setting shows every value that has been collected up to the most recent 12 hours. The other larger interval choices increase the total time range presented but do so by decimating (presenting 1 out of every N actual samples) the data. For example, selecting 10-minute interval will show 5x more range than 2 minute, but only 1 out of every 5 samples are shown to accomplish this. The largest setting (2 hour) will show the entire 30 days of database range but to do so results in 60-to-1 decimation. In all cases the right-side of the chart is the most recent data so that if the full range of collected data can't be shown for that zoom choice, the older data will not be shown.

Figure 6-38. Example of maximum x-axis time range – zoom set to 2 hours per plotted value



6.15.3 Current Sky View chart

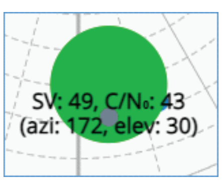
An example is shown in Figure 6-40. The polar plot provides a sky view of all satellites (colored dots) currently tracked by this S6xx unit.

- Distance from center is the elevation (in degrees) from horizon. Outer edge of circle is 0 degrees (i.e. horizon), 90 degrees (center of circle) is directly overhead from the antenna.
- Moving around the circle (at any elevation) shows the azimuth (direction referenced to North) in degrees. For example, 270 degrees is due west. Note that the outer edge of circle has azimuth labels.

Constellations are color coded per the legend left of the chart. In the example we see that GPS, SBAS, and Galileo are being tracked.

This chart does NOT self-update. To refresh the chart select refresh, or exit and return, or refresh the browser. The actual sampling rate for the chart is approximately every 5 minutes so just because the chart is refreshed does not mean that new data will result from it.

Hovering the mouse over any satellite brings up detail on that satellites elevation and azimuth as well as SV (Satellite Vehicle) number and C/No (carrier-to-noise ratio) for that satellite. Here's an example: The satellite "bubble" enlarges continuing to match its original color. Detail shown includes satellite vehicle number, C/No (carrier-to-noise of tracking), and detail about the sky location.



6.15.3.1 Sky View Save As Format

The content of viewed chart can be externally saved using the *Save As* control at bottom of the form. The format is nearly self-explanatory (see example below). Here are details:

- The 3 rows starting with # are informational
  - Row 1 provides a title for chart and identifies time information is UTC (of course this will only actually be true if the S6xx actually has UTC time).
  - Row 2 provides UTC time at which this data was collected

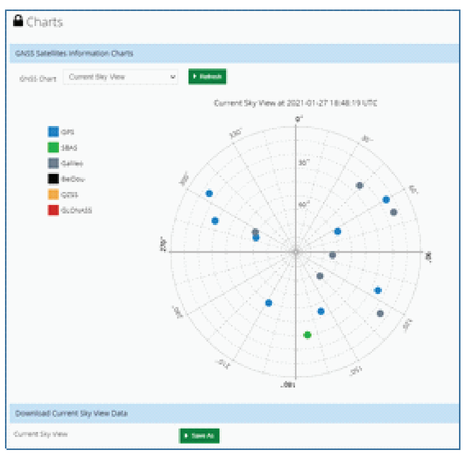
  - Row 3 is a legend for what the data represents. In sequence shown these are the 4 items that were identified in chart detail description
- The remainder is the data itself:
  - Column 1 names the associated constellation
  - All data is comma-separated

The saved file is appropriately named: SyncServer_GNSS_Skyview.txt

Figure 6-39. Example Sky View Save as…

```
#Title:·GNSS·Current·Sky·View:·Timescale·=·UTC¶
#Time:·2021-01-27·20:03:19¶
#Constellation,·<SVId>,·<CNo>,·<Azimuth>,·<Elevation>¶
GPS,·5,·41,·29,·11¶
GPS,·16,·48,·294,·62¶
GPS,·18,·47,·103,·66¶
GPS,·20,·43,·134,·21¶
GPS,·23,·44,·134,·15¶
GPS,·26,·46,·190,·77¶
GPS,·27,·46,·264,·31¶
GPS,·29,·45,·75,·25¶
GPS,·31,·43,·194,·17¶
SBAS,·49,·43,·172,·30¶
Galileo,·2,·44,·150,·37¶
Galileo,·15,·32,·218,·22¶
Galileo,·27,·41,·308,·30¶
Galileo,·30,·43,·238,·76¶
Galileo,·36,·46,·58,·47¶
¶
```

Figure 6-40. Sky View Chart



6.15.4 Tracked Satellites Chart

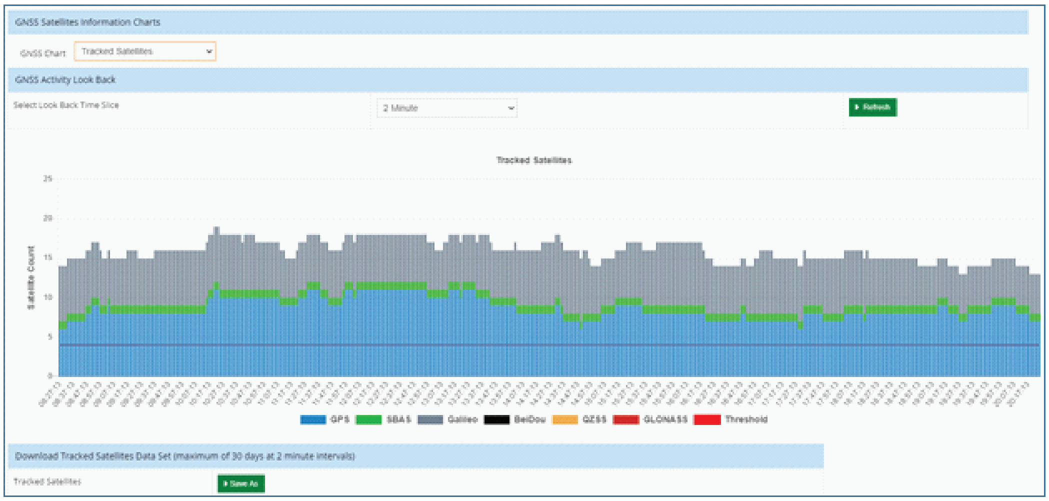
An example is shown in Figure 6-42. The plot is a timeline (with "NOW" at far right) of history of tracked satellites. As with all plots that distinguish satellite constellations, they are color coded consistently, per the legend shown below the data.

Each data column is a stacked bar that distinguishes any constellations that were tracked at that time. More detail for a given stacked bar can be seen by hovering the mouse over any portion of the chart (Figure 6-41). The top shows the x-axis time for results being shown.

Figure 6-41. Example mouse hover

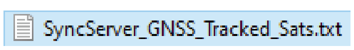
This chart shares common behavioral attributes with all other “vs. time” charts. These are covered in section titled: *Common attributes of Vs. Time Charts*

Figure 6-42. Tracked Satellites chart – 2 minute interval per data value



6.15.4.1 Tracked Satellites Save As Format

Figure 6-42 shows that tracked satellites data can be saved to external storage. The saved file is given a relevant name:.



Shown below is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning. Notice that:

- The sample points are 2 minutes apart (as has been described elsewhere)
- Individual constellation tracking counts are provided with each sample
- A full database will result in 31,200 data rows

```
#Title: GNSS Tracked Satellites: Timescale = UTC
#UTC, <GPS tracked>, <SBAS tracked>, <Galileo tracked>, <BeiDou tracked>, <QZSS tracked>,
<GLONASS tracked>
2020-12-29,01:25:15, 10, 1, 6, 0, 0, 0
2020-12-29,01:27:15, 11, 1, 6, 0, 0, 0
2020-12-29,01:29:15, 11, 1, 6, 0, 0, 0
2020-12-29,01:31:15, 12, 1, 6, 0, 0, 0
2020-12-29,01:33:15, 12, 1, 6, 0, 0, 0
```

6.15.5 Cumulative Site Survey Chart

The primary purpose of this chart (Figure 6-44) is to provide a large-sample assessment of how well the antenna placement is supporting actual tracking of satellites. The concept is simple: use the “sky trails” created by the orbiting satellite constellations (SBAS is geostationary and not included) to effectively provide a sampling source to see where (and how densely) actual tracking is occurring. Unlike the other charts, this one is largely a stand-alone capability. There are no alarms associated with it. The chart itself is the main result for user to assess the quality of the installation from an “ability to track” perspective.

There is only one other high-level control associated with this chart: start/stop of the accumulation process on the Detector summary form (see Figure 6-34). Once started, the accumulation runs continuously until user selects stop. Transitioning from stop to start clears out the prior accumulation and begins a new one.

The fundamentals of the chart are:

- The chart type is a conventional “sky view”
  - Distance from center is the elevation (in degrees) from horizon. Outer edge of circle is 0 degrees (i.e. horizon), 90 degrees (center of circle) is directly overhead from the antenna.
  - Moving around the circle (at any elevation) shows the azimuth (direction referenced to North) in degrees. For example, 270 degrees is due west. Note that the outer edge of circle has azimuth labels.
- The value in each grid location is always the number of satellites (user can filter the included constellations) that have been tracked in that location since the data collection started. Each grid accumulates its count until user stops the process.
- The density of the count in each grid is indicated by the “heat” color in that grid.
- A “mouse hovering” mechanism is in place that allows detailed status for the selected grid to be observed.
- The update rate is about every 5 minutes. What this means is that about every 5 minutes the sky is sampled and any grids that contain a tracked satellite(s) increment their count by the number of satellites in that grid.
- This chart does not self-update (i.e. while observing the chart it will not automatically update the chart). However, it always collects data “behind the scenes”. To get the latest update of this chart, select the refresh control.

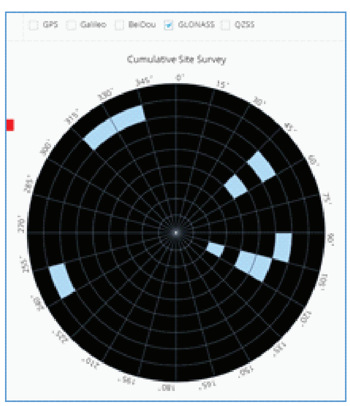
The two main things that the chart can be useful for are:

1. Identifications of zero or low-density grids caused by poor antenna placement (physical or RF blockages in a given sky segment). Also, if all grids are lower density than expected it could be indicative of a general installation issue such as excessive signal loss in path.
2. Identification of zero or low-density grids caused by no (or few) satellites ever orbiting over that sky segment (no opportunity to track). There is a selection filter evaluate this by constellation. Keep in mind that if a constellation is not configured (References > GNSS Config) then of course it will have zero occurrences even if was actually available for tracking at that location.

6.15.5.1 Select Constellations Row

This row is used to filter which constellations are included in the chart. Check the constellations to be included and select refresh to update the chart. This is purely a presentation layer action, the underlying accumulation always accumulates all constellation data. Figure 6-43 shows what the chart in Figure 6-44 looks like if we restrict to only GLONASS satellites. As with all chart controls, the filter selection is not “remembered” if you exit this form and later return. It always enters with all constellations included.

Figure 6-43. Filter set to only GLONASS



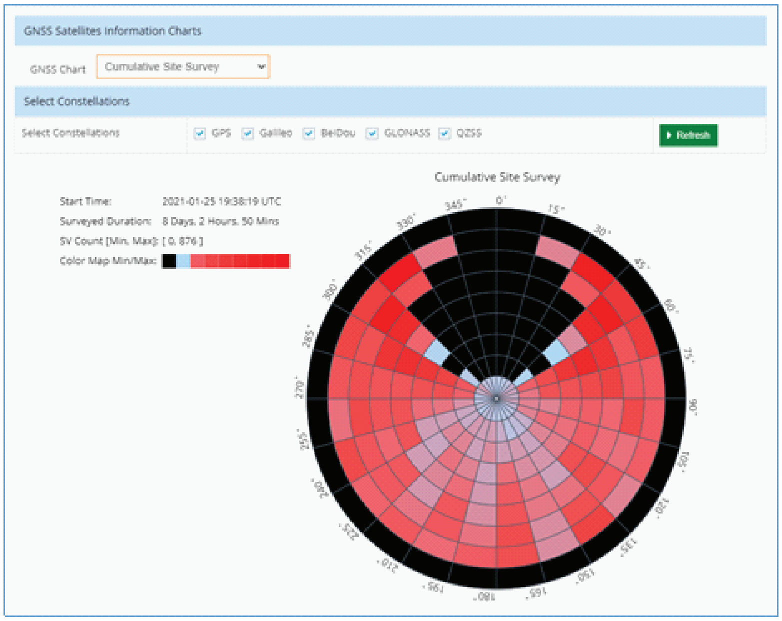
6.15.5.2 Left-Side Chart Information

Look at content upper-left of chart in Figure 6-44 for following descriptions:

- *Start Time*: This field is set when the current cumulative site survey session is started.
- *Surveyed Duration*: Shows how long the current survey has been running.

- *SV Count[min, max]:* This shows the minimum and maximum accumulation of SV (Satellite Vehicles) in all bins (remember there are 216 bins which come from 9 elevation zones x 24 azimuths = 216). In the example of Figure 6-44 we see that there is at least one bin (grid) with zero hits (these are all of the black ones) and at least one that has 876 hits (brightest red).
- *Color Map Min/Max:* This is the color legend for the graph itself. No hits = black, very few hits = light blue, anything else = increasing intensity of reddish hues with maximum grid(s) most red.

Figure 6-44. Cumulative site survey chart (no constellation filter)



6.15.5.3 Information on the chart itself

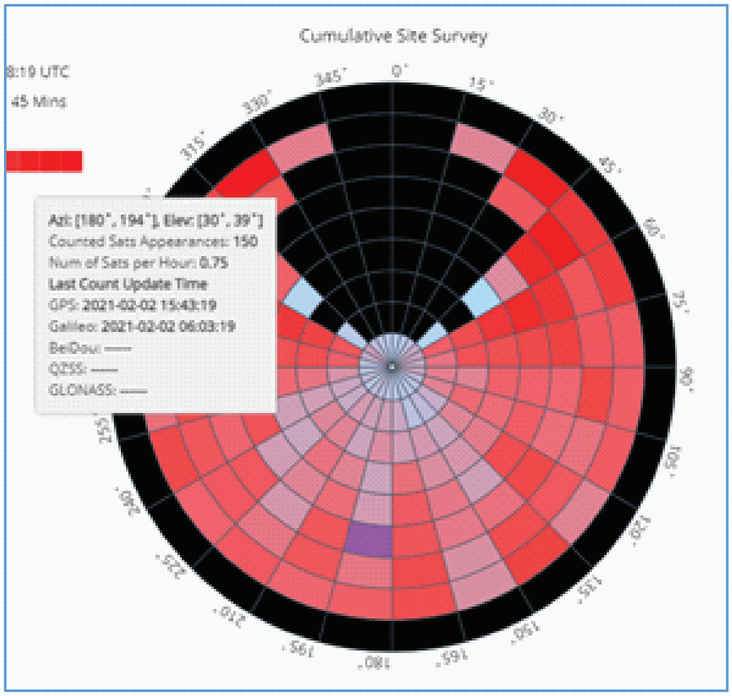
The color-coding shown in example of Figure 6-44 quickly shows a couple of things

- There is a large area to the north that never tracks any satellites. This isn't an installation issue, but just a fact of location.
- The 0-10 degree elevation black ring is due to elevation mask being set to 10 degrees.

Detail about each bin in the chart can be obtained by hovering over that bin via mouse, as shown in Figure 6-45. The grid that is referenced by the detailed data being shown is identified by the purple grid toward the bottom center portion of the chart (where the mouse was pointing when this chart was captured). As the mouse is moved, the associated grid will show this color along with the detail nearby. Reviewing the detail shown:

- Top row identifies the location of grid whose data follows
- *Counted Sats Appearances*: total number of hits in this grid (all constellations).
- *Number of sats per hour*: This is the counted sats appearances (prior row value) divided by the time the accumulation has been running. The idea is to normalize the value so if, for example, the same density is seen for one day and for one week this result would be the same (approximately) in either case.
- *Last Count Update Time:* this is a title for the remaining rows which identify the most recent update into this grid for every constellation. Here we can see that GPS updated this grid about 9 hours more recently than the last Galileo update of this bin. The "-----" indicates that there are no updates ever of this constellation into this bin. If a constellation filter is applied (see *Select Constellations row* topic) any constellations not included by the filter will show "-----".

Figure 6-45. Detail provided by mouse hover

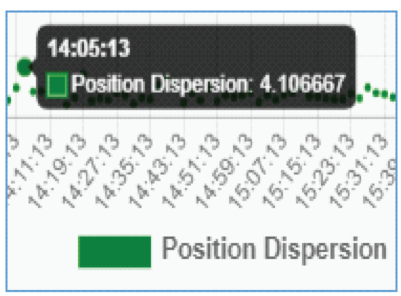


6.15.6 Position Dispersion Chart

An example is shown in Figure 6-47. The plot is simple to understand: a timeline (x-axis, with “NOW” at far right) showing history of position dispersion (y-axis) values.

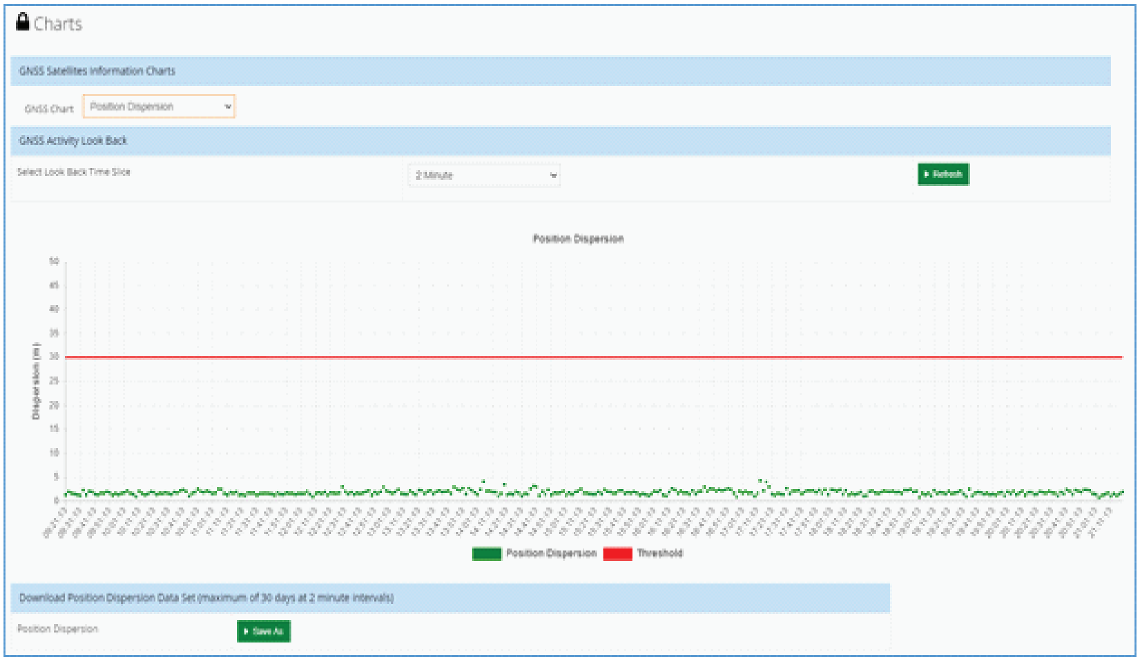
Detail for any plotted dispersion result can be seen by hovering the mouse over appropriate portion of the chart (example shown in Figure 6-46). Note how the “cartoon” box points at and enhances the size of the data value being identified.

Figure 6-46. Example mouse hover



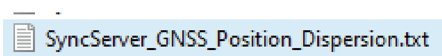
This chart shares common behavioral attributes with all other “vs. time” charts. These are covered in section titled: *Common attributes of Vs. Time Charts*.

Figure 6-47. Position Dispersion chart



6.15.6.1 Position Dispersion Save As Format

Figure 6-47 shows that position dispersion data can be saved to external storage. The saved file is given a relevant name:

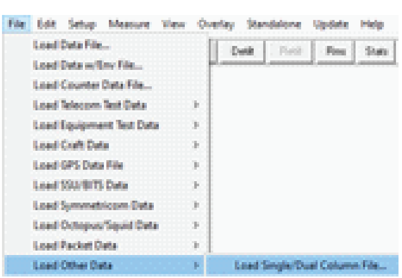


Shown below is the first portion of formatted output. The rows beginning with "#" are comments useful for chart labeling and/or description of the data meaning. Notice that:

- the sample points are 2 minutes apart
- the right-hand column is the dispersion value for the indicated time
- A full database will result in 31,200 data rows

```
#Title: GNSS Position Dispersion: Timescale = UTC
#UTC, <Dispersion Value>
2020-12-29,01:35:15, 1.517647
2020-12-29,01:37:15, 1.735294
2020-12-29,01:39:15, 1.844444
2020-12-29,01:41:15, 1.805556
2020-12-29,01:43:15, 1.738889
```

Microchip TimeMonitor Analyzer supports this format. Use this selection:

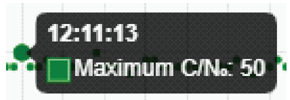


6.15.7 Maximum C/No Chart

An example is shown in Figure 6-49. The plot is simple to understand: a timeline (x-axis, with "NOW" at far right) showing history of Maximum C/No (y-axis) values.

Detail for any plotted Max C/No result is seen by hovering the mouse over appropriate portion of the chart (example shown in Figure 6-48). Note how the “cartoon” box points at and enhances the size of the data value being identified.

Figure 6-48. Example mouse hover

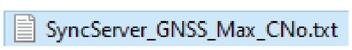


This chart shares common behavioral attributes with all other “vs. time” charts. These are covered in section titled: *Common attributes of Vs. Time Charts*.

Figure 6-49. Maximum C/No Chart

6.15.7.1 Maximum C/No Save As Format

Figure 6-49 shows that Maximum C/No data can be saved to external storage. The saved file is given a relevant name::



Shown below is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning. Notice that:

- the sample points are 2 minutes apart
- The leftmost data column is the maximum CNo for all constellations from that sample. The remaining columns are the maximum CNo for all satellites from that specific constellation.
- A full database will result in 31,200 data rows

```
#Title: GNSS Max CNo: Timescale = UTC
#UTC, <Max CNo>, <GPS CNo>, <SBAS CNo>, <Gal CNo>, <BeiDou CNo>, <QZSS CNo>, <GLONASS CNo>
2020-12-29,01:35:15, 50, 50, 42, 45, 0, 0, 0
2020-12-29,01:37:15, 50, 50, 42, 45, 0, 0, 0
2020-12-29,01:39:15, 49, 49, 42, 45, 0, 0, 0
2020-12-29,01:41:15, 50, 50, 42, 45, 0, 0, 0
2020-12-29,01:43:15, 49, 49, 42, 45, 0, 0, 0
```

6.15.8 CW Jamming Chart

An example is shown in Figure 6-51. The plot is simple to understand: a timeline (x-axis, with “NOW” at far right) shows history of CW Jamming (y-axis) values .

Detail for any plotted CW Jamming result is seen by hovering the mouse over appropriate portion of the chart (example shown in Figure 6-50). Note how the “cartoon” box points at and enhances the size of the data value being identified.

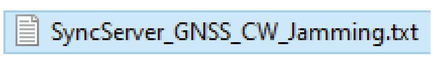
Figure 6-50. Example mouse hover

This chart shares common behavioral attributes with all other “vs. time” charts. These are covered in section titled: *Common attributes of Vs. Time Charts*.

Figure 6-51. CW Jamming chart

6.15.8.1 CW Jamming Save As Format

Figure 6-51 shows that CW Jamming data can be saved to external storage. The saved file is given a relevant name:

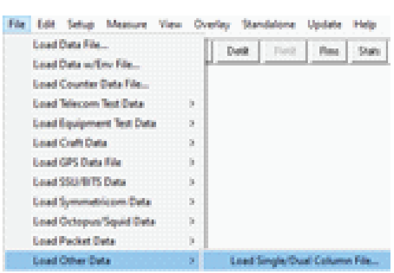


Shown below is the first portion of formatted output. The rows beginning with “#” are comments useful for chart labeling and/or description of the data meaning. Notice that:

- the sample points are 2 minutes apart
- the right-hand column is the CW jamming value for the indicated time
- A full database will result in 31,200 data rows

```
#Title: GNSS Jamming: Timescale = UTC
#UTC, <Jam value>
2020-12-29,01:37:15, 13.72
2020-12-29,01:39:15, 13.72
2020-12-29,01:41:15, 13.72
2020-12-29,01:43:15, 13.72
2020-12-29,01:45:15, 13.33
```

Microchip TimeMonitor Analyzer supports this format. Use this selection:



6.16 BlueSky Alarms

This section shows alarms directly associated with BlueSky capabilities. All BlueSky alarms are shown in Figure 6-52 and Figure 6-53. These figures are directly taken from the Admin > Alarms form. This makes the important point that all of these alarms are part of the generic S6xx alarm system and therefore support all of same capabilities as any alarm in the system.

The section titled *Alarms and associated controls* provides further detail about BlueSky-unique controls associated with these alarms.

Figure 6-52. BlueSky Alarms - Part 1

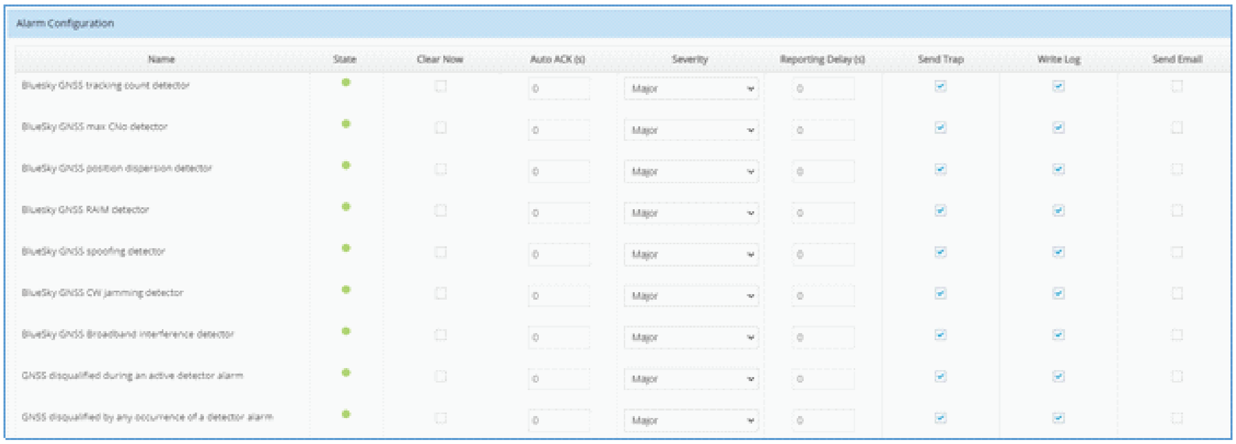
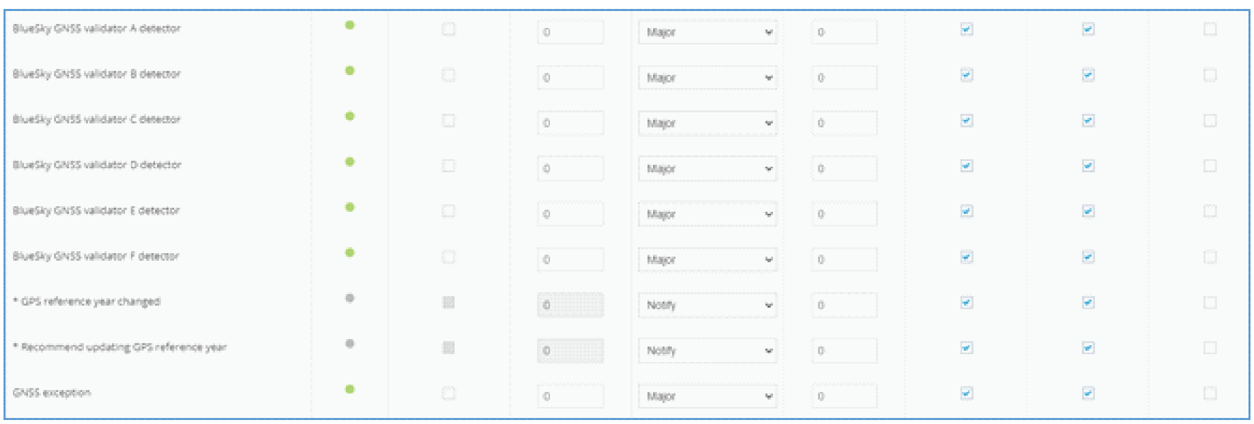


Figure 6-53. BlueSky Alarms - Part 2



7. Maintenance and Troubleshooting

7.1 Preventive Maintenance

The SyncServer S6x0 requires minimal preventive maintenance. Ensure the unit is not exposed to hazards such as direct sunlight, open windows, water, or extreme heat. See Environmental Requirements in Chapter 2, for electromagnetic compatibility conditions that may cause damage.

⚠ CAUTION To avoid electromagnetic discharge damage to the circuitry, never attempt to vacuum the SyncServer S6x0.

The following table lists preventive maintenance measures to be performed periodically. Do not disassemble components just for the purpose of inspection.

Table 7-1. Preventive Maintenance

Item	Inspection	Corrective Action	Interval
Chassis	Inspect for dirt or foreign material	Clean the exterior of chassis with a soft dry cloth	Periodically
Cables	Inspect for pinched, worn or damaged cable	Replace pinched, worn or damaged cable at the first opportunity	Periodically
Connectors	Inspect for loose or damaged connector	Tighten loose connectors. If damaged, replace the connector and/or cable at the first opportunity	Periodically

7.2 Safety Considerations

Follow your company's safety guidelines and policies when working on or around live equipment.

7.3 ESD Considerations

Maintenance personnel should wear ESD wrist straps when installing or working on all SyncServer S6x0 equipment. Plug the user-supplied wrist strap into the SyncServer S6x0.

7.4 Troubleshooting

LEDs, and System Messages can all be very helpful in troubleshooting the SyncServer S6x0. Use the Alarms page of the Web GUI to view system messages or use SNMP trap messages.

Note: The SyncServer S6x0 incorporates a system reboot function (watchdog) if any of the system's software become unresponsive. If the system's software is unresponsive for 15 minutes, then the watchdog timer will report an event in the event log (add the actual event here), and the system will reboot.

7.4.1 Diagnosing the SyncServer S6x0 − Reading LED Conditions

The following table shows the function of the LED indicators on the front panel of the unit. The table also details for the Ethernet RJ45 Port LED link activity indicators.

Table 7-2. LED Conditions

Indicator	Label	Description	Corrective Action
Clock Status	SYNC	Green - Time or Frequency clock in Normal or Bridging state	n/a
		Amber - Time or Frequency clock in Freerun or Holdover state	Use the Web GUI to view alarm IDs and descriptions, Admin > Alarms, or expand the "Alarm(s)" tab to see a summary of active alarms. See Table 8-1 in Chapter 8 System Messages for corrective actions.
Network Status	NETWOR K	Green - All configured ports are up	n/a
		Amber - Some configured ports are down (LAN2 to LAN4)	Use the Web GUI to view the configuration and status of ports, Network > Ethernet or expand the "Network" tab to see the configuration of each port. See Table 8-1 in Chapter 8 System Messages for corrective actions.
		Red - Management port (LAN1) is not configured or is down	Use the Web GUI to view the configuration and status of ports, Network > Ethernet or expand the "Network" tab to see the configuration of each port. See Table 8-1 in Chapter 8 System Messages for corrective actions.
Alarm/fault indicator	ALARM	Green - Operating Normally	n/a
		Amber - Minor Alarm(s)	Expand the Alarm(s) tab in the Web GUI dashboard to see a summary of active alarms. See Table 8-1 in Chapter 8 System Messages for corrective actions.
		Red - Major/Critical Alarm(s)	Expand the Alarm(s) tab in the Web GUI dashboard to see a summary of active alarms. See Table 8-1 in Chapter 8 System Messages for corrective actions.

...........continued

Indicator	Label	Description	Corrective Action
Ethernet RJ45 Port LEDs link/activity indicator	1 2 3 4	Left LED Amber - 100BT link Left LED Green - 1000BT link Right LED Green blinking - Activity	n/a
		Left LED Off - No link Right LED Off - No link	Use the Web GUI to view alarm IDs and descriptions, Admin > Alarms , or expand the “Alarm(s)” tab on the Dashboard to see a summary of active alarms. • Check the cable connections. • Verify that interface is enabled by using Web GUI page: Network > Ethernet. • Check that either Ethernet Auto Negotiation is enabled or that speed has been set to a compatible level with the connecting network element by using Web GUI page: Network > Ethernet. • Make sure that only full-duplex network devices are used. The SyncServer S6x0 does not support half-duplex devices, such as hubs, for NTP connections.

7.5 Repairing the SyncServer S6x0

The SyncServer S6x0 cannot be repaired in the field. There are no field-serviceable fuses in the SyncServer S6x0. If a fuse blows in a SyncServer S6x0, the unit must be returned to the factory for repair.

7.6 Upgrading the Firmware

You can upgrade the firmware using the SyncServer S6x0’s web interface and software available from Microchip. When the SyncServer S6x0 is in the firmware download mode, it prevents all other sessions from making changes to the configuration. During the upgrade process, no new sessions are allowed. Refer to SyncServer S6x0 Upgrade below for details on the upgrade process. For releases after 1.1, if the upgrade process is used to load a previous (older) version of the software, then the unit will reset the configuration to factory default values. The current firmware version can be found in the Dashboard > About window. Upon receipt of any new/repaired equipment, perform the relevant software upgrade procedure below prior to putting the shelf into service.

Caution: To avoid a possible service call, do not issue a command to the SyncServer S6x0 during an upgrade and do not remove power from the SyncServer S6x0 during an upgrade. Doing so could corrupt the flash memory, disabling the SyncServer S6x0.

7.6.1 SyncServer S6x0 Upgrade

The upgrade process is simple, but there will be Loss of Service (LOS) at reboot. The upgrade will take approximately 7 minutes to complete. The upgrade process requires an authorization file in order to proceed. This file verifies that this SyncServer unit is authorized to upgrade the selected upgrade file.

The SyncServer 6x0 does not contain a battery-backed real time clock. Therefore, it will always boot up with a default value for the system time. This time will be updated when it obtains time from a time reference such as GNSS, IRIG, or NTP. The default value for the date is the software build date. This date will be used for the first log entries when booting up the unit. The time will change to local time during the boot-up process if a time zone has been configured.

Table 7-3. Upgrading Firmware

Method	Steps	Notes
Web Interface	Admin > Upgrade 1. Navigate to the location of the authorization file and select it. 2. Navigate to the location of the upgrade file and select it. 3. Click the **Install** button.	
CLI	n/a	n/a
Front Panel	n/a	n/a

Note: If the upgrade terminates with an authorization error, then this system is not authorized to upgrade to new upgrade image, or the auth.dat file is for a different software version than the upgrade image file.

Note: If “upgrading” from revision 2.0 or higher to an older revision, then the system will set configuration to factory default values.

Note: Configuration changes made after the upgrade but before the reboot will not be available after the reboot.

Note: If the all-packets limit on LAN1 has been reduced on the Security > Packet Monitoring page, then it is recommended that the limit be temporarily increased back to the default value of 13000 packets/second. Otherwise, the file upload will be very slow and may timeout.

7.7 SyncServer S6x0 Part Numbers

The following sections provide part numbers for the system, accessories, and GNSS antenna kits.

7.7.1 System and Accessory Part Numbers

This section provides part numbers and descriptions for the system and accessories available for the SyncServer S6x0. See Table 7-4 for Quickship part numbers. See Table 7-5 for S600 Build to Order part numbers. See Table 7-6 for S600 Build to Order part numbers. See Table 7-7 for accessories.

Table 7-4. SyncServer S6x0 Quickship Part Numbers

Item	Part Number
S600 Quickship Models	
SyncServer S600	090-15200-601
SyncServer S600 + OCXO	090-15200-602
SyncServer S600 + Rubidium	090-15200-603
SyncServer S600 + Dual AC power supplies	090-15200-604
SyncServer S600 + OCXO + Dual AC power supplies	090-15200-605
SyncServer S600 + Rubidium + Dual AC power supplies	090-15200-606
S650 Quickship Models	
SyncServer S650+Timing I/O Module	090-15200-651
SyncServer S650+Timing I/O Module + Rubidium	090-15200-652

...........continued	
Item	**Part Number**
S650i Quickship Models	
SyncServer S650i+Timing I/O Module	090-15200-653
Quickship Options	
Security Protocols License Option	920-15201-002
Flex Timing Option for Timing I/O Module	920-15201-009
GNSS Option	920-15201-001
PTP Output Option	920-15201-003
PTP Input Option	920-15201-004
Measurement Option	920-15201-011
Programmable Pulse Option	920-15201-005
BlueSky GPS Spoofing Detection Option	920-15201-006

Note: The GNSS option is NOT available with the S650i.
The Flex Timing and Measurement options are only available with the Timing I/O module.

Table 7-5. SyncServer S600 Build to Order Part Numbers

Item	Part Number
S600 Build to Order	
SyncServer S600 Base Config, NO Power Supply	090-15200-600
S600 Power Supplies	
Single AC Power Supply	090-15201-001
Dual AC Power Supplies	090-15201-002
Dual DC Power Supplies	090-15201-010
S600 Oscillator Upgrades	
SyncServer OCXO Upgrade	090-15201-003
SyncServer Rubidium Upgrade	090-15201-004
S600 Software Enabled Options	
Security Protocols License Option	920-15201-102
GNSS Option	920-15201-101
PTP Master Option	920-15201-103
PTP Input Option	920-15201-104
BlueSky GPS Spoofing Detection Option	920-15201-106

Table 7-6. SyncServer S650 Build to Order Part Numbers

Item	Part Number
S650 Build to Order	
SyncServer S650 Base Config, NO Power Supply	090-15200-650

...........continued	
Item	**Part Number**
S650 Power Supplies	
Single AC Power Supply	090-15201-001
Dual AC Power Supplies	090-15201-002
Dual DC Power Supplies	090-15201-010
S650 Oscillator Upgrades	
SyncServer OCXO Upgrade	090-15201-003
SyncServer Rubidium Upgrade	090-15201-004
S650 Modules / Hardware	
SyncServer Timing I/O Module	090-15201-006
SyncServer LPN Module	090-15201-007
SyncServer ULPN Module	090-15201-008
10 GbE Card	090-15201-009
SyncServer Timing I/O Module with Telecom I/O	090-15201-011
SyncServer Timing I/O Module with HaveQuick/PTTI	090-15201-012
SyncServer Timing I/O Module with fiber optic input	090-15201-013
SyncServer Timing I/O Module with fiber optic outputs	090-15201-014
S650 Software Enabled Options	
Security Protocols License Option	920-15201-102
Flex Timing Option for Timing I/O Module	920-15201-109
PTP Master Option	920-15201-103
PTP Input Option	920-15201-104
Measurement Option	920-15201-111
GNSS Option	920-15201-101
Programmable Pulse Option	920-15201-105
BlueSky GPS Spoofing Detection Option	920-15201-106

7.7.2 GNSS Antenna Kits

Antenna cables and accessories enable versatile solutions that are easy to achieve. Inline GNSS amplifiers installed at the antenna are an easy way to extend cable runs from 225 feet to up to 900 feet, depending on cable type. Lightning arrestors provide valuable electrical protection to the SyncServer. Antenna cable splitters leverage a single antenna and cable for up to four GNSS receivers.

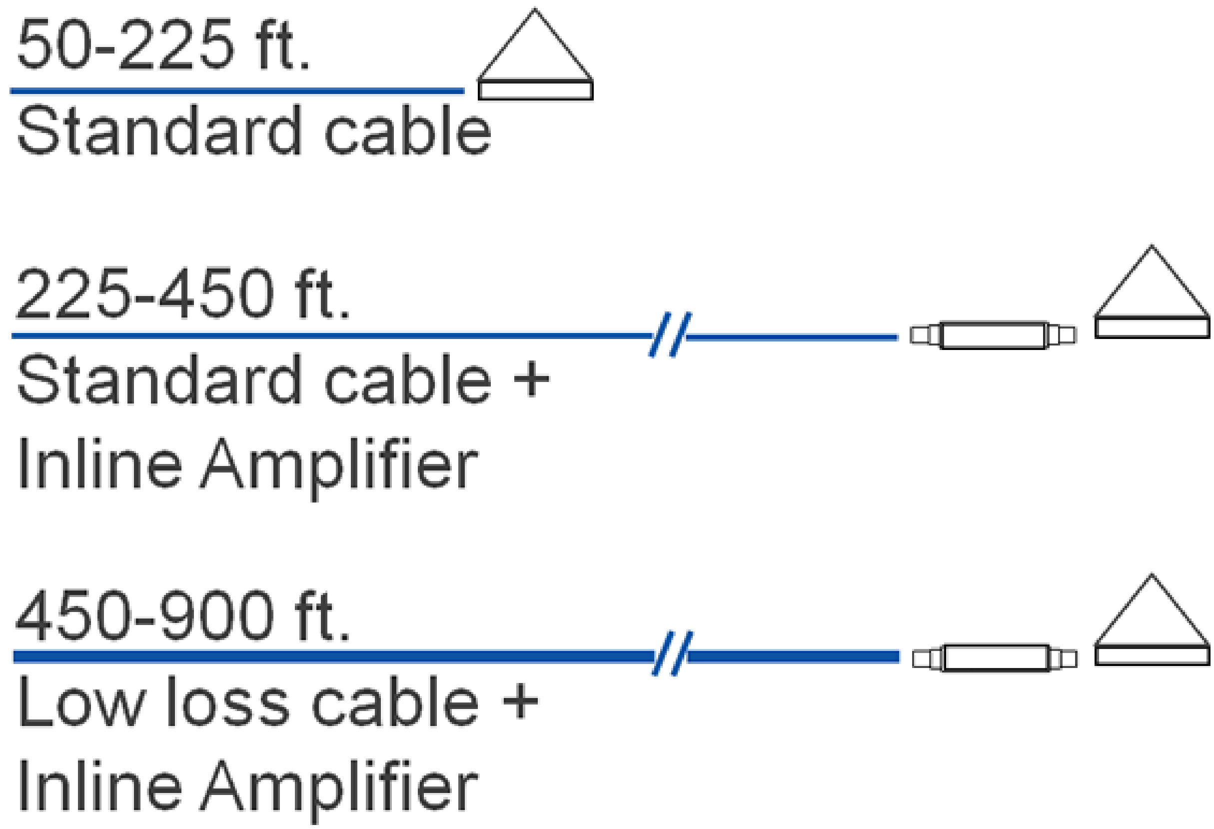
Ordering antenna components is a simple task. The most important thing the user needs to have is a rough idea of the total cable length needed between the SyncServer and the mounting location of the antenna. Any extra cable can be coiled to the side.

Preconfigured kits that include cable, antenna, and related mounting accessories are available, as shown in Table 7-7. These kits vary by total cable length, and based on whether a lightning arrestor is required or not. For long cable runs (>225 ft.), the components are assembled individually. See Figure 7-1.

To assist and simplify configuration, Microchip has an Excel-based antenna configurator that helps the user determine the exact part numbers they need for the desired cable length and accessories. See Microchip's website for the configurator:

http://www.microsemi.com/products/timing-synchronization-systems/time-frequency-distribution/network-appliances-servers/syncserver/syncserver-s650#documents.

Figure 7-1. Antenna Kits for Long Cable Runs



The antenna kit (part number 093-15202-001) includes a short SyncServer adapter cable (part number 060-00039-000) with BNC(m)-N(f) connectors. All primary antenna cables use N(m) connectors on either end. A single cable must be used between the adapter cable and the next accessory (lightning arrestor, inline amplifier, or antenna). Lightning arrestors include a 25 ft. cable to connect to the next accessory (inline amplifier or antenna).

Note: Lightning Arrest Kit includes 25 ft. cable. Total length includes the additional cable that is part of the Lightning Arrestor if selected.

Note: To receive GLONASS or BeiDou signals, the antenna system should be made of GLONASS and/or BeiDou compatible components.

.

Table 7-7. GNSS Antenna Kits & Accessories

Antenna Kit	Part Number
Kit: Total length: 50 ft, Cable: 50 ft; antenna kit (093-15202-001)	990-15202-050

...........continued

Antenna Kit	Part Number
Kit: Total length: 75 ft, Cable: 50 ft; lightning arrestor (112-43400-00-3); Cable: 25 ft; antenna kit (093-15202-001)	990-15202-075
Kit: Total length: 100 ft, Cable: 100 ft; antenna kit (093-15202-001)	990-15202-100
Kit: Total length: 125 ft, Cable: 100 ft; lightning arrestor (112-43400-00-3); Cable: 25 ft; antenna kit (093-15202-001)	990-15202-125
Kit: Total length: 150 ft, Cable: 150 ft; antenna kit (093-15202-001)	990-15202-150
Kit: Total length: 175 ft, Cable: 150 ft; lightning arrestor (112-43400-00-3); Cable: 25 ft; antenna kit (093-15202-001)	990-15202-175
Kit: Total length: 200 ft, Cable: 200 ft; antenna kit (093-15202-001)	990-15202-200
Kit: Total length: 225 ft, Cable: 200 ft; lightning arrestor (112-43400-00-3); Cable: 25 ft; antenna kit (093-15202-001)	990-15202-225
250 ft. Antenna Cable	060-15202-250
350 ft. Antenna Cable	060-15202-350
450 ft. Antenna Cable	060-15202-450
500 ft. Low Loss Antenna Cable	060-15202-500
750 ft. Low Loss Antenna Cable	060-15202-750
900 ft. Low Loss Antenna Cable	060-15202-900
Kit: • GPS/GLONASS Antenna (112-00079-000) • Mounting Bracket (193-00044-000) • Adapter cable for chassis (060-15202-004)	093-15202-001
Kit: Lightning Arrestor (112-43400-00-3) with 25 ft. cable	093-15202-002

...........continued	
Antenna Kit	**Part Number**
Kit: Lightning Arrestor (112-43400-00-3) with 25 ft. low loss cable	093-15202-003
Inline Amplifier (112-15202-001) with adapter	093-15202-005
Kit: • GPS/GLONASS/BeiDou Antenna (112-15202-003) • Mounting Bracket (193-00044-000) • Adapter cable for chassis (060-15202-004)	093-15202-006
Kit: GPS/GLONASS/BeiDou 1:4 splitter with Two (2) x 3 ft. cables	093-15202-007
Kit: • Anti-jam GPS/GLONASS/BeiDou Antenna (112-15202-004) • Mounting Bracket (158-00273-000) • Adapter cable for chassis (060-15202-004)	093-15202-010

Note: The required antenna is TALLYSMAN 32-3372-14-01, 40dB GNSS Antenna, N connector. Standard cable is LMR-240 or equivalent. Low loss cable is LMR-400 or equivalent.

7.8 Returning the SyncServer S6x0

You should return the equipment to Microchip only after you have exhausted the troubleshooting procedures described earlier in this chapter, or if Microchip FTS Services and Support has advised you to return the unit. Note: Please retain the original packaging for re-shipping the product. If the original packaging is not available, contact Microchip FTS Services and Support for assistance.

7.8.1 Repacking the Unit

Return all units in the original packaging. If the original packaging is not available, contact Microchip FTS Services and Support. Use standard packing procedures for products being returned for repair to protect the equipment during shipment. Connectors should be protected with connector covers or the equipment should be wrapped in plastic before packaging. Ensure that the display and connectivity panels are protected when packaged.

7.8.2 Equipment Return Procedure

To return equipment to Microchip for repair:

1. Call Microchip FTD Services and Support at 888-367-7966 (toll-free in USA only), 408-428-7907, or +49 700 3288 6435 in Europe, Middle East, or Africa to obtain a return material authorization number (RMA) before returning the product for service. You can request an RMA on the internet at www.microsemi.com/ftdsupport Retain the assigned RMA number for future reference.
2. Provide a description of the problem, product item number, serial number, and warranty expiration date.
3. Provide the return shipping information (customer field contact, address, telephone number, and so forth.)
4. Ship the product to Microchip, transportation prepaid and insured, with the Return Material Authorization (RMA) number and item numbers or part numbers clearly marked on the outside of the container to the address given with the RMA. Repaired equipment is returned to you with shipping costs prepaid by Microchip.

7.9 Cipher Suites

The cipher suites listed below are current as of firmware release 4.1. The list may change with subsequent firmware releases.

Ciphers used with cipher suite configuration of SSL_HIGH_ENCRYPTION:

- TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
- TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
- TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
- TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
- TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
- TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits

Ciphers used with cipher suite configuration of SSL_HIGH_AND_MEDIUM_ENCRYPTION:

- TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
- TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
- TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
- TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
- TLSv1.2 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
- TLSv1.2 256 bits AES256-GCM-SHA384
- TLSv1.2 256 bits AES256-SHA256
- TLSv1.2 256 bits AES256-SHA
- TLSv1.2 256 bits CAMELLIA256-SHA
- TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256
- TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256
- TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
- TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-AES128-SHA256 DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-SEED-SHA DHE 2048 bits
- TLSv1.2 128 bits DHE-RSA-CAMELLIA128-SHA DHE 2048 bits
- TLSv1.2 128 bits AES128-GCM-SHA256
- TLSv1.2 128 bits AES128-SHA256
- TLSv1.2 128 bits AES128-SHA
- TLSv1.2 128 bits SEED-SHA
- TLSv1.2 128 bits CAMELLIA128-SHA
- TLSv1.2 128 bits IDEA-CBC-SHA
- TLSv1.2 112 bits ECDHE-RSA-DES-CBC3-SHA Curve P-256 DHE 256
- TLSv1.2 112 bits EDH-RSA-DES-CBC3-SHA DHE 2048 bits
- TLSv1.2 112 bits DES-CBC3-SHA
- TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
- TLSv1.1 256 bits DHE-RSA-AES256-SHA DHE 2048 bits
- TLSv1.1 256 bits DHE-RSA-CAMELLIA256-SHA DHE 2048 bits
- TLSv1.1 256 bits AES256-SHA
- TLSv1.1 256 bits CAMELLIA256-SHA
- TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256
- TLSv1.1 128 bits DHE-RSA-AES128-SHA DHE 2048 bits
- TLSv1.1 128 bits DHE-RSA-SEED-SHA DHE 2048 bits
- TLSv1.1 128 bits DHE-RSA-CAMELLIA128-SHA DHE 2048 bits
- TLSv1.1 128 bits AES128-SHA
- TLSv1.1 128 bits SEED-SHA
- TLSv1.1 128 bits CAMELLIA128-SHA

- TLSv1.1 128 bits IDEA-CBC-SHA
- TLSv1.1 112 bits ECDHE-RSA-DES-CBC3-SHA Curve P-256 DHE 256
- TLSv1.1 112 bits EDH-RSA-DES-CBC3-SHA DHE 2048 bits
- TLSv1.1 112 bits DES-CBC3-SHA

7.10 User's Guide Updates

When this manual is updated the updated version will be available for downloading from Microchip's internet web site. Manuals are provided in PDF format for ease of use. After downloading, you can view the manual on a computer or print it using Adobe Acrobat Reader. Manual updates are available at: my.microsemi.com.

Note: If you are downloading a product manual for the first time, you will need to register with Microchip for a username and password. If you are currently registered, login and download the manual update.

7.11 Contacting Technical Support

To order any accessory, contact the Microchip Sales Department. If you encounter any difficulties installing or using the product, contact Microchip Frequency and Time Systems (FTS) Services and Support:

U.S.A. Call Center:

including Americas, Asia and Pacific Rim

Frequency and Time Systems (FTS)

3870 N 1st St.
San Jose, CA 95134

Toll-free in North America: 1-888-367-7966

Telephone: 408-428-7907

Fax: 408-428-7998

email: sjo-ftd.support@microchip.com

Internet: www.microsemi.com/ftdsupport

Europe, Middle East, and Africa (EMEA):

Microsemi FTS Services and Support EMEA

Altlaufstrasse 42

85635 Hoehenkirchen-Siegertsbrunn

Germany

Telephone: +49 700 3288 6435

Fax: +49 8102 8961 533

email: sjo-ftd.support@microchip.com

ftd.emea_sales@microsemi.com

8. System Messages

This section provides information about the system messages that are displayed in response to a provisioning event or to an alarm that occurs when an associated threshold or timer is outside of the provisioned setting.

8.1 Facility codes

4 Security/authorization messages

20 SyncServer S6x0 Messages (events and alarms)

21 SyncServer S6x0 Command History

22 SyncServer S6x0 Messages (events and alarms)

8.2 Message Provisioning

The SyncServer S6x0 supports logging of events using syslog defined facility and severity codes and system defined facility codes as follows: Facility codes 4 Security/authorization messages 20 SyncServer S6x0 Messages (events and alarms) 21 SyncServer S6x0 Command History 22 SyncServer S6x0 Messages (events and alarms) Severity codes 2 (critical) Critical: critical conditions 3 (major) Error: error conditions 4 (minor) Warning: warning conditions 5 (event) Notice: normal but significant condition 6 Info: Informational

Notes: Severity codes 2, 3, and 4, are also indicated by the Alarm LED(s) on the front panel.

The syslog message format is as follows: Mmm dd hh:mm:ss host_name Process-name AlarmID,Index,Severity, MsgText Where: Mmm = Month; dd = date; hh:mm:ss = system time host_name = hostname process-name = alarmd AlarmID = 000 thru Max_AlarmID Index = 0 thru 155 Severity = Notify | Minor | Major | Critical (defined by severity code) MsgText = (see tables)

8.3 Severity codes

2 (critical) Critical: critical conditions

3 (major) Error: error conditions

4 (minor) Warning: warning conditions

5 (event) Notice: normal but significant condition

6 Info: Informational

Note: Severity codes 2, 3, and 4, are also indicated by the Alarm LED(s) on the front panel.

The syslog message format is as follows:

```
Mmm dd  hh:mm:ss
host_name Process-name AlarmID,Index,Severity, MsgText
```

Where:

- Mmm = Month; dd = date; hh:mm:ss = system time
- host_name = hostname
- process-name = alarmd
- AlarmID = 000 thru Max_AlarmID
- Index = 0 thru 155
- Severity = Notify | Minor | Major | Critical (defined by severity code)
- MsgText = (see tables)

8.4 System Notification Messages

The following table provides a list of system notification messages. These messages are logged and sent to a remote syslog server if configured. These messages can also be sent via email . Alarms can also generate an SNMP trap.

Note: Transitory Events represent transitions that have no “Set and Clear” behavior, such as when the first lock occurs after power-up (see “first normal-track since powerup” alarm).

Table 8-1. System Notification Messages

Description	Event ID	Msg Level	Trans-itory	MsgText	Corrective Action
Enter/exit time/freq warmup	1	Minor	No	Entered time/frequency warm-up state Transitioned out of time/ frequency warm-up state	No action required No action required
Enter/exit time/freq freerun	2	Minor	No	Entered time/frequency free-run state Transitioned out of time/ frequency free-run state	No action required No action required
Enter/exit time/freq fast-track	3	Notify	No	Entered time/frequency fast-track state Transitioned out of time/ frequency fast-track state	No action required No action required
Enter/exit time/freq normal	4	Notify	No	Entered time/frequency normal state Transitioned out of time/ frequency normal state	No action required No action required
Enter/exit time/freq bridging	5	Notify	No	Entered time/frequency bridging state Transitioned out of time/ frequency bridging state	No action required No action required
Entered time/ frequency holdover	6	Minor	No	Entered time/frequency holdover state Transitioned out of holdover state	• Check input references • Check configuration for correct reference selection • Check reference status • Check ref configuration for Priority values. No action required
Entered time/ frequency holdover recovery	8	Minor	No	Entered time/frequency holdover recovery state Transitioned out of holdover recovery state	No action required No action required
First normal-track since power-up	9	Notify	Yes	First normal-track since Power-Up	No action required

...........continued

Description	Event ID	Msg Level	Trans-itory	MsgText	Corrective Action
Input ref poor quality	21	Minor	No	GNSS | NTP | J1A | J2A | J2A | J2B Input Poor Quality GNSS | NTP | J1A | J2A | J2A | J2B Input poor quality cleared	• If this persists for > 1hr check input reference. • For GNSS check signal quality. No action required
Time input selected	24	Notify	Yes	GNSS | NTP | J1A | J2A | J2A | J2B input selected as time reference	No action required
Freq input selected	25	Notify	Yes	GNSS | J1A | J2A | J2A | J2B input selected as frequency reference	No action required
Input Alarm indication signal (AIS)	27	Minor	No	T1E1-[1 | 2] Input Alarm Indication Signal T1E1-[1 | 2] Input Alarm Indication Signal cleared	Correct input signal. N/A
Input out of frame	28	Minor	No	T1E1-[1 | 2] Input out of frame T1E1-[1 | 2] Input out of frame cleared	Correct input signal. N/A
Input CRC Error	29	Minor	No	T1E1-[1 | 2] Input CRC Error T1E1-[1 | 2] Input CRC Error cleared	Correct input signal. N/A
Input BPV	30	Minor	No	T1E1-[1 | 2] Input Bipolar Violation T1E1-[1 | 2] Input Bipolar Violation cleared	Correct input signal. N/A
GNSS Time Qualified	33	Notify	No	GNSS input time qualified Exit Input Time qualified cleared	No action required No action required
NTP Time Qualified	34	Notify	No	NTP input time qualified Exit NTP Input Time qualified cleared	No action required No action required
PTP Time Qualified	35	Notify	No	PTP input time qualified Exit PTP input time qualified	No action required No action required
J1A Time Qualified	36	Notify	No	J1A input time qualified Exit J1A Input Time qualified cleared	No action required No action required
J1B Time Qualified	37	Notify	No	J1B input time qualified Exit J1B Input Time qualified cleared	No action required No action required

...........continued					
Description	**Event ID**	**Msg Level**	**Trans-itory**	**MsgText**	**Corrective Action**
GNSS Freq Qualified	40	Notify	No	GNSS input freq qualified Exit Input Freq qualified cleared	No action required No action required
NTP Freq Qualified	41	Notify	No	Reserved - event will never be reported	Reserved - event will never be reported
PTP Freq Qualified	42	Notify	No	PTP input frequency qualified Exit PTP input frequency qualified	No action required No action required
J1A Freq Qualified	43	Notify	No	J1A input freq qualified Exit J1A Input Freq qualified cleared	No action required No action required
J1B Freq Qualified	44	Notify	No	J1B input freq qualified Exit J1B Input Freq qualified cleared	No action required No action required
J2A Freq Qualified	45	Notify	No	J2A input freq qualified Exit J2A Input Freq qualified cleared	No action required No action required
J2B Freq Qualified	46	Notify	No	J2B input freq qualified Exit J2B Input Freq qualified cleared	No action required No action required
J7A Freq Qualified	47	Notify	No	J7A input freq qualified Exit J7A Input Freq qualified cleared	No action required No action required
J7B Freq Qualified	48	Notify	No	J7B input frequency qualified Exit J7B Input frequency qualified cleared	No action required No action required
PTP Input Change	52	Notify	Yes	PTP input lost PTP input lost cleared	No action required (PTP parent dataset changed) No action required
PTP master switch	53	Notify	Yes	PTP master switched or being re-qualified	No action required
PTP input not time/ freq traceable	54	Notify	No	PTP input time | freq not traceable PTP input time | freq not traceable cleared	No action required No action required
PCP client dropped	72	Notify	Yes	PTP client x dropped from LANx client list	No action required
PTP client added	73	Notify	Yes	PTP client x added to LANx client list	No action required
PTP client list refreshed	74	Notify	Yes	PTP client list on LANx refreshed	No action required

...........continued

Description	Event ID	Msg Level	Trans-itory	MsgText	Corrective Action
PTP state change to disabled	75	Notify	Yes	PTP state changed to disabled on LANx	No action required
PTP state change to listening	76	Notify	Yes	PTP state changed to listening on LANx	No action required
PTP state change to master	77	Notify	Yes	PTP state changed to master on LANx	No action required
PTP state change to passive	78	Notify	Yes	PTP state changed to passive on LANx	No action required
GNSS receiver comms failed	91	Major	No	GNSS receiver communications failed GNSS receiver communications failure cleared	• Reboot • If problem persists call SGS for support. No action required
GNSS receiver not tracking satellites	92	Minor	No	GNSS receiver not tracking satellites GNSS receiver not tracking satellites cleared	• Check Antenna installation • Check if Antenna cable is connected properly. • Installation should conform to the guidelines as described in Chapter 10. No action required
GNSS Signal Low(1)	93	Minor	No	GNSS signal low GNSS signal normal	Improve antenna gain • Add amplifier • Reduce cable length • Or use low loss cable No action required
GNSS ant short-circuit	96	Minor	No	GNSS antenna short-circuit GNSS antenna short-circuit cleared	Check for short circuit in the antenna cable. If shorted antenna, then out-of-range and short-circuit alarms will be generated. No action required
GNSS ant open-circuit	97	Minor	No	GNSS antenna open-circuit GNSS antenna open-circuit cleared	Check for Antenna not connected or AC coupled splitter. If using a splitter you must at least draw 10mA of current from the SyncServer S6x0. This can be achieved by adding a 50 ohm termination. If no antenna, then open-circuit and out-of-range alarms both will be generated No action required

...........continued					
Description	**Event ID**	**Msg Level**	**Trans-itory**	**MsgText**	**Corrective Action**
GNSS PPS failure	98	Major	No	Reserved - event will never be reported	Reserved - event will never be reported
J1A Input LOS (LOSS OF SIGNAL)(5)	99	Notify	No	J1A Input LOS J1A Input LOS cleared	• Check if cable is securely connected. • Check signal source is present and configured properly. No action required
J1B Input LOS (LOSS OF SIGNAL)(5)	100	Notify	No	J1B Input LOS J1B Input LOS cleared	• Check if cable is securely connected. • Check signal source is present and configured properly. No action required
J2A Input LOS (LOSS OF SIGNAL)	101	Notify	No	J2A Input LOS J2A Input LOS cleared	• Check if cable is securely connected. • Check signal source is present and configured properly. No action required
J2B Input LOS (LOSS OF SIGNAL)	102	Notify	No	J2B Input LOS J2B Input LOS cleared	• Check if cable is securely connected. • Check signal source is present and configured properly. No action required
J7A Input LOS (LOSS OF SIGNAL)	103	Notify	No	J7A Input LOS J7A Input LOS cleared	• Check if cable is securely connected. • Check signal source is present and configured properly. No action required
J7B Input LOS (LOSS OF SIGNAL)	104	Notify	No	J7B Input LOS J7B Input LOS cleared	• Check if cable is securely connected. • Check signal source is present and configured properly. No action required
Excessive traffic on port (2)	112	Minor	No	Excessive traffic on PORT [1 | 2 | 3 | 4 | 5 6] Excessive traffic on PORT [1 | 2 | 3 | 4 | 5 6]	• Check traffic level on network • Check for intrusion attempts. • Check broadcast traffic. (See Footnote 1) No action required
RESERVED	113				•

...........continued

Description	Event ID	Msg Level	Trans- itory	MsgText	Corrective Action
Ethernet Port1 link down	115	Minor	No	LAN1 port link down LAN1 port link down cleared	• Check cable. • Check the box the interface is connected to. • Check Auto- negotiation. No action required
Ethernet Port2 Port link down	116	Minor	No	LAN2 port link down LAN2 port link down cleared	• Check cable. • Check the box the interface is connected to. • Check Auto- negotiation. No action required
Ethernet Port3 Port link down	117	Minor	No	LAN3 port link down LAN3 port link down cleared	• Check cable. • Check the box the interface is connected to. • Check Auto- negotiation. No action required
Ethernet Port4 Port link down	118	Minor	No	LAN4 port link down LAN4 port link down cleared	• Check cable. • Check the box the interface is connected to. • Check Auto- negotiation. No action required
Ethernet Port 5 link down	119	Minor	No	LAN5 port link down LAN5 port link down	• Check cable • Check the box the interface is connected to No action required
Ethernet Port 6 link down	120	Minor	No	LAN6 port link down LAN6 port link down	• Check cable • Check the box the interface is connected to No action required
Service load limit exceeded[3]	130	Minor	No	Service load limit exceeded on PORTx Service load limit exceeded on PORTx cleared	Reduce service traffic on specified LAN port or increase service packet limit value. If using PTP unicast profile, reduce the number of PTP clients requesting service. (see Footnote) No action required

...........continued

Description	Event ID	Msg Level	Trans-itory	MsgText	Corrective Action
Power Out of Range	131	Major	No	`[ +13.2 | +5 | OSC +5 | +3.3 | +2.5 | +1.5 | +1.1 | +1.0 | osc current | 3.8V | 1.2V | -5V]` out of range ____ out of range cleared	• If alarm persists power cycle/reboot • Call SGS support if it persists after reboot/ power cycle. n/a
Operational Failure:	132	Major	No	Operational failure: <name of item failing> Operational failure cleared	• If alarm persists power cycle/reboot • Call SGS support if it persists after reboot/ power cycle. No action required
Synth unlock	137	Major	No	Synth unlock Synth unlock cleared	• If alarm persists power cycle/reboot • Call SGS support if it persists after reboot/ power cycle. No action required
Rubidium unlock	138	Major	No	Rubidium unlock Rubidium unlock cleared	• If alarm persists power cycle/reboot • Call SGS support if it persists after reboot/ power cycle. No action required
Temperature out of range	139	Minor	No	Temperature out of range Temperature out of range cleared	Check your operating environment. No action required
Fan Failure	140	Minor	No	Fan failed - [A | B] Fan failure cleared	• If alarm persists power cycle/reboot • Call SGS support if it persists after reboot/ power cycle. No action required
Timeline has been changed	152	Notify	Yes	Timeline has been changed n/a	n/a
Phase has been aligned	153	Notify	Yes	Phase has been aligned n/a	n/a
System Reboot	155	Notify	Yes	System reboot n/a	No action required. n/a
RESERVED	156				
Timing Quality > 1e^{-6}	157	Minor	No	Timing Quality> 1e^{-6} set Timing Quality > 1e^{-6} cleared	n/a

...........continued

Description	Event ID	Msg Level	Trans- itory	MsgText	Corrective Action
Timing Quality > $1e^{-5}$	158	Minor	No	Timing Quality> $1e^{-5}$ set Timing Quality > $1e^{-5}$ cleared	n/a
Timing Quality > $1e^{-4}$	159	Minor	No	Timing Quality> $1e^{-4}$ set Timing Quality > $1e^{-4}$ cleared	n/a
Timing Quality > $1e^{-3}$	160	Minor	No	Timing Quality> $1e^{-3}$ set Timing Quality > $1e^{-3}$ cleared	n/a
NTP System Peer Changed	161	Notify	Yes	NTP System Peer Changed to < > n/a	No action required. n/a
NTP Stratum Changed	162	Notify	Yes	NTP System Peer Changed to < > n/a	No action required. n/a
NTP Leap Indicator Changed	163	Notify	Yes	NTP Leap Indicator Changed n/a	No action required. n/a
System Upgrade Available	164	Notify	No	System upgrade available n/a	Upgrade unit software. n/a
J1A IRIG Input Protocol Fault	170	Minor	No	J1A IRIG Input protocol fault J1A IRIG Input protocol fault cleared	Verify IRIG configuration matches source configuration. No action required
J1B IRIG Input Protocol Fault	171	Minor	No	J1B IRIG Input protocol fault J1B IRIG Input protocol fault cleared	Verify IRIG configuration matches source configuration. No action required
Holdover Exceeded	172	Minor	Yes	Holdover time error threshold exceeded Holdover time error threshold cleared	Same as for entering holdover No action required
Leap event pending	173	Notify	Yes	Leap event pending Leap event pending cleared	No action required
Excessive Frequency Adjustment	174	Major	Yes	Excessive frequency adjustment Excessive frequency adjustment cleared	n/a
Input power not present	175	Minor	No	No power detected on [AC1 | AC2 | DC1 | DC2] No power detected on [AC1 | AC2 | DC1 | DC2] cleared	Connect other power input to AC power (if dual power version) Verify backup supply is operational n/a
Full system configuration occurred	176	Notify	Yes	Reserved - event will never be reported	Reserved - event will never be reported

...........continued

Description	Event ID	Msg Level	Trans- itory	MsgText	Corrective Action
Configuration Change	177	Notify	Yes	Configuration changed n/a	No action required. n/a
LPN oscillator unlock[(4)]	179	Minor	No	LPN oscillator unlock LPN oscillator unlock cleared	• If alarm persists, power-cycle • Call support if it persists after power-cycle No action required
Manual Time Entry Mode Enabled	180	Minor	No	Entered Manual Time Entry Mode Transitioned out of Manual Time Entry Mode	No action required
LPN oscillator lock state changed	181	Notify	No	LPN Oscillator lock status changed to xx LPN Oscillator lock status changed to xx cleared	No action required No action required
NTP reflector state changed to passive	182	Notify	Yes	NTPr state changed to passive on port x	No action required
NTP reflector state change to server	183	Notify	Yes	NTPr state changed to Server on port x	No action required
Event Overflow	184	Notify	No	Event Overflow at Slot [A | B] J1 Event Overflow at Slot [A | B] J1 cleared	Reduce frequency or bursts of J1 input signal N/A
User password will expire	185	Notify	Yes	Password for user <username> will expire in <value> days	Update user password
BlueSky GNSS Track Count	186	Minor	No	Bluesky GNSS tracking count detector Exit bluesky GNSS tracking count detector	Check antenna installation or possible jamming No action required
BlueSky GNSS Max C/No	187	Minor	No	BlueSky GNSS max CNo detector Exit BlueSky GNSS max CNo detector	Check for possible spoofer No action required
BlueSky GNSS Position Dispersion	188	Major	No	BlueSky GNSS position dispersion detector Exit BlueSky GNSS position dispersion detector	Check for possible spoofer No action required
BlueSky GNSS RAIM	189	Notify	No	BlueSky GNSS RAIM detector Exit BlueSky GNSS RAIM detector	Check for possible spoofer No action required

...........continued

Description	Event ID	Msg Level	Trans-itory	MsgText	Corrective Action
BlueSky GNSS Spoofing	190	Major	No	BlueSky GNSS spoofing detector Exit BlueSky GNSS spoofing detector	Check for possible spoofer No action required
BlueSky GNSS CW Jamming	191	Major	No	BlueSky GNSS CW jamming detector Exit BlueSky GNSS CW jamming detector	Check for possible jammer No action required
BlueSky GNSS Broadband Interference	192	Major	No	BlueSky GNSS Broadband interference detector Exit BlueSky GNSS Broadband interference detector	Check for possible jammer No action required
GNSS disqualified during detector alarm	193	Major	No	GNSS disqualified during an active detector alarm Exit GNSS disqualified during an active detector alarm	Check detector alarm No action required
GNSS disqualified by any occurrence of a detector alarm	194	Major	No	GNSS disqualified by occurrence of <detector> detector alarm Exit GNSS disqualified by occurrence of <detector> detector alarm	When ready, disable alarm to allow qualification of GNSS No action required
BlueSky GNSS Validator A	195	Major	No	BlueSky GNSS validator B <value> detector Exit BlueSky GNSS validator B <value> detector	Check for possible spoofer No action required
BlueSky GNSS Validator B	196	Major	No	BlueSky GNSS validator B <value> detector Exit BlueSky GNSS validator B <value> detector	Check for possible spoofer No action required
BlueSky GNSS Validator C	197	Major	No	BlueSky GNSS validator C <value> detector Exit BlueSky GNSS validator C <value> detector	Check for possible spoofer No action required
BlueSky GNSS Validator D	198	Major	No	BlueSky GNSS validator D <value> detector Exit BlueSky GNSS validator D <value> detector	Check for possible spoofer No action required
BlueSky GNSS Validator E	199	Notify	No	BlueSky GNSS validator E <value> detector Exit BlueSky GNSS validator E <value> detector	No action required No action required

...........continued					
Description	**Event ID**	**Msg Level**	**Trans- itory**	**MsgText**	**Corrective Action**
BlueSky GNSS Validator F	200	Notify	No	BlueSky GNSS validator F <value> detector Exit BlueSky GNSS validator F <value> detector	No action required No action required
GPS Reference Year Changed	201	Notify	Yes	GPS reference year changed	RESERVED: event not used
Recommend Updating GPS Reference Year	202	Notify	Yes	Recommend updating GPS reference year	RESERVED: event not used
GNSS Exception	203	Minor	No	GNSS exception: <exception description> GNSS exception cleared: <exception description>	No action required No action required

(1) The ”GNSS signal low” alarm is created if the unit has achieved a position solution, but is not tracking at least 4 satellites with a C/No value greater than 37 for several minutes.
(2) The excessive traffic alarm is set if the count of Ethernet packets received in one second exceeds the user-settable “All Packets” threshold on the Security > Packet Monitoring form (license required). With no license the detection level is a fixed 13000 packets per second. All traffic received by the SyncServer S6x0 Ethernet ports, and not handled by the PTP GM or NTP reflector, is counted, such as ARP, ICMP, IGMP. The all-packets limit is set to a fixed 3000 packets/second if a timing service is configured on the port -- NTP reflector or PTP.

(3) The service load limit alarm is set if the count of Ethernet packets received by the timing service (NTP reflector or PTP master) in one second exceeds the user-settable threshold on the Security > Packet Monitoring form (license required).

(4) When S6xx is recovering from holdover (shows “Recovering” on Dashboard) a temporary setting of the “LPN oscillator unlock” alarm may occur. This is an indication that LPN 10MHz output adjustments are being limited from changing too fast in order to maintain optimal 10MHz output phase noise performance.

(5) Input LOS alarms could be generated if the input is slower than 1PPS. Microchip recommends disabling the LOS alarm actions on the Admin->Alarms page under this condition.

9. Specifications

This chapter provides mechanical and electrical specifications and factory defaults for the SyncServer S6x0.

9.1 Specifications

This section provides the specifications for the SyncServer S6x0 input and output signals.

9.1.1 Mechanical

Table 9-1. SyncServer S6x0 Mechanical Specifications

Parameter	Description
Mounting	19 in. or 23 in. Rack
Rack Mounting	See Figure 2-2 for drawings with detailed chassis dimensions.
Width	17.24 in. / 438 mm
Height	1.73 in. / 44 mm; 1 RU
Depth	15.00 in. / 381 mm 15.88 in. / 403 mm - including connectors on rear panel
Weight Unit Shipping Package	12.5 lb. / 5.7 kg 16.3 lb. / 7.4 kg

9.1.2 Environmental

Table 9-2. SyncServer S6x0 Environmental Specifications

Parameter	Description
Operating Temperature	• 20° to 65° C, -4° to 149° F − Standard or OCXO [startup > -20°C (-4°F)] • 5° to 55° C, 23° to 131° F − Rubidium oscillator
Storage Temperature	• 40° to 85° C, -40° to 185° F
Operating Humidity	5% to 95% RH, maximum, non-condensing
Operating Altitude	25,000 feet, maximum
Storage Altitude	25,000 feet, maximum

9.1.3 Power

Table 9-3. SyncServer S6x0 AC Power Specifications

Parameter	Description
Input Voltage Range	110/220 VAC (90 VAC to 250 VAC), 50/60 Hz
AC Power - Operating	50 W, 417 mA @ 120V

Table 9-4. SyncServer S6x0 Dual DC Power Specifications

Parameter	Description
Input Voltage Range	20 VDC to 75 VDC

...........continued	
Parameter	**Description**
DC Power - Operating	50 W
Cable connector parts	Housing - Molex 03-12-1036, Terminals - 0018121222 (16-18 AWG tin plated)

9.1.4 Compliance & Certifications

Table 9-5. SyncServer S6x0 Compliance Specifications

Parameter	Description
Safety Certifications	• UL1950 • UL60950-1/CSA C22.2 No. 60950-1, Second Edition
EMC Immunity	
Radiated Emissions	• FCC Part 15, Class A • EN 55011 • CISPR 22, Class A • EN55014
Conducted Emissions	• FCC Part 15, Class A • EN 55011 • CISPR 22, Class A • EN55014
Immunity Radiated	ENV50140 RF immunity, 10V/m, 80 – 1000MHz, 80% modulation; 900 MHz pulsed at 200 Hz
Immunity Conducted	• ENV50140 RF common mode immunity, 0.15 - 80 MHz, 10V, 80% modulation • EN61000-4-8 Magnetic Field immunity, 50Hz, 40A/m continuous, 1000A/m for 1 sec
Environmental & Physical	
Environmental Compliance	• FCC Part 15, Class A, • CISPR 22, Class A, • UL/CSA • 60950-1 • IEC 60950-1 • EN 60950-1 • PSE • VCCI • RoHS (6 of 6)
Shock and Vibration Operational Storage Transportation - Bounce Transportation - Vibration Transportation - Package Drop Seismic	ETSI EN-300 019-2-3, Mil-STD-810G IEC 60068-2-6 Fc (sinusoidal vib), Mil-Std-810G, figure 514.6C-3 IEC 60068-2-27Ea (shock 18g) IEC 60068-2-64Fh (random vib) IEC 60068-2-31 Ec EN300 019-2-3, NEBS GR-63-CORE

...........continued	
Parameter	**Description**
Storage Temperature and Humidity Criteria	IEC 60068-2-1Ab (low temp soak), IEC 60068-2-2Bb (hi-temp soak) IEC 60068-2-14Nb (change of temp) IEC 60068-2-78Cb (humidity storage), IEC 60068-2-30Db (humidity condensation)
Operational Humidity Criteria	IEC 60068-2-78Cb, IEC 60068-2-30Db
General	
	• NTP (v3 - RFC1305, v4 - RFC5905) • NTP Unicast, Autokey, • MD5 (RFC1321) • SNTP (RFC4330) • SNMP v2c (RFC1441-1452), v3 (RFC3411-3418) • Custom MIB • DHCP (RFC2131) • DHCPv6 (RFC3315) • TACACS+ (RFC1492) • LDAPv3 (RFC4510-4521) • RADIUS (RFC2865) • HTTPS/SSL (RFC2616),high encryption cipher suite • SMTP Forwarding • SSHv2 • IPv4/IPv6 • Syslog 1 to 8 servers • Key management protocols can be individually disabled. • PORT 1: Management & Time protocols • PORT 2, 3 & 4: Time protocols only.

VCCI

9.1.5 Serial Port

Table 9-6. SyncServer S6x0 Console Serial Port Specifications

Item	Description
Connector Type	9-pin, female D connector
Connector Label	CONSOLE
Interface	RS-232, data terminal equipment (DTE)
Baud Rate	57.6 Kbps
Data Bits	8
Parity Bit	None
Stop Bits	1
Flow Control	None

9.1.6 Input Signals

9.1.6.1 GNSS

Table 9-7. SyncServer S6x0 GNSS Input Signal Specifications

Parameter	Specification
Signal Type	GNSS L1
Gain	Between 15 dB and 30 dB including gain of antenna and loss of cable
Frequency	GPS: 1575.42 MHz center frequency
Impedance	50 ohms
Coupling	DC (center pin provides DC power to the GNSS antenna or in-line amplifier)
Output to Antenna voltage current	9.7 VDC 100 mA (max)
Connector Type	BNC connector, female
Connector Label	GNSS

9.1.6.2 IRIG Input

IRIG inputs are available with the Optional Timing I/O Module.

Table 9-8. SyncServer S6x0 IRIG Input Signal Specifications

Parameter	Specification
Impedance	50 Ω or high impedance (> 50 k Ω)
Connector Type	BNC
Connector Label	J1
Signal Level	AM: Ratio 2:1 to 3.5:1 Amp: 1 V to 8 V p-p, into 50 Ω DCLS: <0.8 V for logic 0, >2 V for logic 1

IRIG inputs are also available with the Optional Timing I/O Module with fiber optic input (090-15201-013).

Table 9-9. SyncServer S6x0 Fiber IRIG Input Signal Specifications

Parameter	Specification
Connector Type	ST, fiber optic
Connector Label	J1
Wavelength	820 nm
Fiber	Multimode
Maximum Length	1000m using 62.5/125 um fiber

9.1.6.3 NTP Input

Table 9-10. SyncServer S6x0 NTP Input Signal Specifications

Parameter	Specification
Connector Type	RJ45

...........continued	
Parameter	**Specification**
Connector Label	1, 2, 3, 4

9.1.6.4 PPS Input

1PPS input is available with the Optional Timing I/O Module (090-15201-006).

Table 9-11. SyncServer S6x0 PPS Input Signal Specifications

Parameter	Specification
Signal Type	TTL, rising edge active
Impedance	50 Ω or high impedance (> 50 k Ω)
Connector Type	BNC
Connector Label	J1

1PPS input is also available with the Optional Timing I/O Module with fiber optic input (090-15201-013).

Table 9-12. SyncServer S6x0 Fiber PPS Input Signal Specifications

Parameter	Specification
Signal Type	Optical, rising edge active
Connector Type	ST, fiber optic
Connector Label	J1
Wavelength	820 nm
Fiber	Multimode
Maximum Length	1000m using 62.5/125 um fiber

9.1.6.5 10M PPS Input

10M PPS input is available with the Optional Timing I/O Module.

Table 9-13. SyncServer S6x0 PPS Input Signal Specifications

Parameter	Specification
Signal Type	< 0.8 V for logic 0, > 2 V for logic 1
Impedance	50 Ω or high impedance (> 50 k Ω)
Connector Type	BNC
Connector Label	J1

9.1.6.6 10MHz, 5MHz, 1MHz Input

The 10MHz, 5MHz, and 1MHz inputs are available with the Optional Timing I/O Module.

Table 9-14. SyncServer S6x0 10/5/1 MHz Input Signal Specifications

Parameter	Specification
Signal Type	Sine Wave
Amplitude	1 Vpp to 8 Vpp
Impedance	50 Ω

...........continued	
Parameter	**Specification**
Connector Type	BNC
Connector Label	J2

9.1.6.7 T1, E1 Input

The T1 and E1 inputs are available with the Optional Timing I/O Module with Telecom I/O (090-15201-011).

Table 9-15. SyncServer S6x0 T1, E1 Input Signal Specifications

Parameter	Specification
Signal Type	T1: ANTSI T1.403. G.703 Section 5 Framed T1 Format: D4, ESF, 1544 kHz E1: G.703 Section 9 Framed E1, CAS or CCS, CRC4 enable/disable; or G.703 Section 13 2048 kHz Composite Clock (CC): 50/50 or 5/8 duty cycle Japanese Composite Clock (JCC): with or without 400 Hz Japanese Sine Wave (JSW): 6.312 MHz
Amplitude	0.2 Vpp to 6.5 Vpp
Impedance	110 Ω
Connector Type	RJ-48C, balanced pair
Connector Label	J7

9.1.6.8 HaveQuick Input

The J1 input is available as a HaveQuick input with the Optional Timing I/O Module with HaveQuick/PTTI (090-15201-012). J2 is used for the HaveQuick 1PPS input.

Table 9-16. SyncServer S6x0 HaveQuick Input Signal Specifications

Parameter	Specification
Signal Type	HaveQuick HaveQuick 1PPS
Amplitude	5V or TTL
Impedance	50 Ω
Connector Type	BNC
Connector Label	J1 for HaveQuick J2 for HaveQuick 1PPS (only available if J1 used for HaveQuick input.

9.1.6.9 Timing Accuracy for Inputs

The following table lists the expected timing accuracy when using different input references.

Table 9-17. Timing Accuracy to Reference

Reference	Timing Accuracy to Reference	Comments
GPS	15 ns rms to UTC (USNO)	
IRIG AM		
A13x	± 5 μs	10 kHz

...........continued		
Reference	**Timing Accuracy to Reference**	**Comments**
B12x	± 10 µs	1 kHz
E11x	± 1 ms	100 Hz
E12x	± 10 µs	1 kHz
G14x	± 5 µs	100 kHz
NASA 36 AM	± 10 µs	1 kHz
XR3 AM	± 10 µs	250 Hz
2137 AM	± 10 µs	1 kHz
IRIG DCLS		
A00x	± 100 ns	
B00x	± 100 ns	
E00x	± 100 ns	
G00x	± 100 ns	
NASA 36	± 100 ns	
XR3	± 100 ns	
2137	± 100 ns	
PTP client	± 1 µs, typical	
NTP client	± 100 µs, typical	Server on same subnet

9.1.7 Output Signals

9.1.7.1 NTP Output

Table 9-18. SyncServer S6x0 NTPOutput Signal Specifications

Parameter	Specification
Connector Type	RJ45
Connector Label	Ports 1, 2, 3, 4

The timestamps have been compensated for 1000BT. For 100BT, the NTP packets will have a bias of up to 1 microsecond.

9.1.7.2 PTP Master Output

PTP outputs are available with the PTP License option.

Table 9-19. SyncServer S6x0 PTP Output Signal Specifications

Parameter	Specification
Connector Type	RJ45, 100/1000 Base-T
Connector Label	Ports 1, 2, 3, 4
PTP Profile	Enterprise

9.1.7.3 IRIG Output

IRIG outputs are available with the Timing Input/Output Module (090-15201-006). They are also available on ports J3-J6 on the Telecom module (090-15201-011) and the HaveQuick/PTTI module (000-15201-012). It is available on ports J3-J8 on the Fiber input module (090-15201-14), and ports J4, J6, and J8 on the Fiber output module (090-15201-013).

Table 9-20. SyncServer S6x0 IRIG Output Signal Specifications

Parameter	Specification
Signal Type	IRIG B
Connector Type	BNC
Connector Label	J3, J4, J5, J6, J7, J8
Impedance	50 Ω
Signal Level	AM: Ratio 10:3 ± 10% Amp: 3.5 ± 0.5 Vpp, DCLS: <0.8 V for logic 0, >2.4 V for logic 1

IRIG outputs are also available with the Optional Timing I/O Module with fiber optic outputs (090-15201-014). Only DCLS signals are available on the fiber outputs.

Table 9-21. SyncServer S6x0 Fiber IRIG Output Signal Specifications

Parameter	Specification
Connector Type	ST, fiber optic
Connector Label	J3, J5, J7
Wavelength	820 nm
Fiber	Multimode
Maximum Length	1000m using 62.5/125 um fiber

9.1.7.4 T1, E1 Output

The T1 and E1 outputs are available with the Optional Timing I/O Module with Telecom I/O (090-15201-011)..

Table 9-22. SyncServer S6x0 T1, E1 Output Signal Specifications

Parameter	Specification
Signal Type	T1: ANTSI T1.403. G.703 Section 5 Framed T1 Format: D4, ESF, 1544 kHz E1: G.703 Section 9 Framed E1, CAS or CCS, CRC4 enable/disable; or G.703 Section 13 2048 kHz Composite Clock (CC): 50/50 or 5/8 duty cycle Japanese Composite Clock (JCC): with or without 400 Hz Japanese Sine Wave (JSW): 6.312 MHz
T1 Amplitude	2.4 Vpk to 3. 6 Vpk, 100 Ω
E1 Amplitude	3 V +- 0.3V, 120 Ω
CC Amplitude	3 Vpk +- 0.4 V
JCC Amplitude	1 Vpk +- 01V, nominal
JSW Amplitude	0 DBm +- 3dB, 120 Ω

...........continued	
Parameter	**Specification**
1.054 or 2.048 MHz squarewave Amplitude	3 Vpp +- 0.3V
Connector Type	RJ-48C, balanced pair
Connector Label	J7, J8

9.1.7.5 HaveQuick Outputs

The J3 - J6 outputs are available as a HaveQuick outputs with the Optional Timing I/O Module with HaveQuick/PTTI (090-15201-012). These ports can also be configured as 1PPS or 1PPM outputs..

Table 9-23. SyncServer S6x0 HaveQuick Output Signal Specifications

Parameter	Specification
Signal Type	HaveQuick TTL HaveQuick 5V
Amplitude	5V or TTL
Impedance	50 Ω
Connector Type	BNC
Connector Label	J3 - J6

.

Table 9-24. SyncServer S6x0 1PPS/1PPM Output Signal Specifications on Timing I/O Module with HaveQuick/PTTI

Parameter	Specification
Signal Type	1PPS 1PPM
Amplitude	5V or 10V
Impedance	50 Ω
Connector Type	BNC
Connector Label	J3 - J6

9.1.7.6 PTTI Outputs

The J7 and J8 outputs are available as PTTI outputs with the Optional Timing I/O Module with HaveQuick/PTTI (090-15201-012)..

Table 9-25. SyncServer S6x0 PTTI Output Signal Specifications

Parameter	Specification
Signal Type	PTTI BCD time code is a 50 bit (full) or 24 (bit) abbreviated) message defining the UTC time of day, day of year, and TFOM Transmitted at 50 bps.
Amplitude	+-2 V min to 100 Ω, +-3 V typical
Impedance	110 Ω
Connector Type	RJ-48C, balanced pair
Connector Label	J7 - J8

9.1.7.7 TOD Output

Table 9-26. SyncServer S6x0 1PPS+TOD Output Signal Specifications

Parameter	Specification
Connector Type	9-pin, female D connector
Connector Label	DATA/TIMING
Signal Level	RS-232
Timing Relationship between 1PPS and TOD	Transmission of a TOD message starts 10 ms (default) after the rising edge of 1PPS signal, and the transmission is completed within 500 ms, as shown in Figure 9-1. This TOD message indicates the time of the current 1 PPS rising edge, and is sent at a rate of once per second.
TOD Frame	TOD messages use whole 8-bit bytes for transmission, with check sum protection. Message type and message ID are used to clarify messages. Follows Big Endian convention when a field is longer than one byte, where bit 0 represents the least significant bit (LSB), and bit 0 of each byte is transmitted first.
TOD Transmission Parameters Table 9-15. SyncServer S6x0 1PPS+TOD Output Signal Specifications	Baud Rate: 9600 Parity Check: None Start Bit: 1 (low level) Stop Bit: 1 (high level) Idle Frame: High level Data Bits: 8
TOD Message Encoding	Binary

9.1.7.8 PPS Output

Table 9-27. SyncServer S6x0 1PPS+TOD Output Signal Specifications

Parameter	Specification
Connector Type	BNC female connector
Connector Label	1PPS
Impedence	50
Signal Level	3.25V, typical
Timing Relationship between 1PPS and TOD	Transmission of a TOD message starts 10 ms (default) after the rising edge of 1PPS signal, and the transmission is completed within 20 us, as shown in Figure 9-1. This TOD message indicates the time of the current 1 PPS rising edge, and is sent at a rate of once per second.
Rise Time - 1PPS Pulse	1.5 ns, typical
Pulse Width	20 µs
Active Edge	Rising

9.1.7.9 10 / 5 / 1 MHz Output

The 10/5/1 MHz outputs are available with the Optional Timing I/O Module (090-15201-006). They are also available on ports J3-J6 on the Telecom module (090-15201-011) and the HaveQuick/PTTI module (000-15201-012). It is available on ports J3-J8 on the Fiber input module (090-15201-14), and ports J4, J6, and J8 on the Fiber output module (090-15201-013).

Table 9-28. SyncServer S6x0 10 MHz Output Signal Specifications

Parameter	Specification
Signal type	Sine wave
Connector type	BNC male
Connector Label	J3 - J8
Impedance	50 Ω
Signal Level	2 - 3 Vpp

9.1.7.10 1PPS x N Output Signal Specifications

The 1PPS x N outputs are available with the Optional Timing I/O Module (090-15201-006). They are also available on ports J3-J6 on the Telecom module (090-15201-011) and the HaveQuick/PTTI module (000-15201-012). It is available on ports J3-J8 on the Fiber input module (090-15201-14), and on the Fiber output module (090-15201-013).

Table 9-29. SyncServer S6x0 1PPS Output Signal Specifications

Parameter	Specification
Signal type	Rising edge on-time TTL or optical
Settings - Fixed Rate	• 10/5/1MPPS • 100/10/1/kPPS • 100/10/1/0.5PPS • 1PPM
Settings - Programmable Period	100 ns to 86400 seconds, step size of 10 ns
Pulse Width	• 50% for programmable pulse • 20µs for fixed-rate pulse periods of PPM, PP2S, and PPS • 50% for other periods of fixed-rate pulse
Connector type	BNC male, or ST for fiber
Connector Label	J3 - J8
Impedance	50 Ω for electrical

9.1.7.11 LPN Module Output Signal Specifications

The LPN outputs are available with the Optional LPN Module.

Table 9-30. SyncServer S6x0 LPN Module Output Signal Specifications

Parameter	Specification
Phase Noise 1 Hz 10 Hz 100 Hz 1 kHz 10 kHz 100 kHz	– 95 dBc/Hz –125 dBc/Hz –145 dBc/Hz –150 dBc/Hz –155 dBc/Hz –155 dBc/Hz

...........continued

Parameter	Specification
Allan Deviation 1 s 10 s	$<3.0 \times 10^{-12}$ $<4.5 \times 10^{-12}$
Output Level	13 dBm ± 1.5 dB
Channel-to-Channel Isolation	100 dB at 10 MHz
Connector type	BNC male
Connector Label	J1 - J8
Impedance	50 Ω

9.1.7.12 ULPN Module Output Signal Specifications

The ULPN outputs are available with the Optional ULPN Module.

Table 9-31. SyncServer S6x0 ULPN Module Output Signal Specifications

Parameter	Specification
Phase Noise 1 Hz 10 Hz 100 Hz 1 kHz 10 kHz 100 kHz	–112 dBc/Hz –135 dBc/Hz –150 dBc/Hz –158 dBc/Hz –160 dBc/Hz –160 dBc/Hz
Allan Deviation 1 s 10 s	$<4.5 \times 10^{-13}$ $<2.0 \times 10^{-12}$
Output Level	13 dBm ± 1 dB
Channel Isolation	100 dB at 10 MHz
Connector type	BNC male
Connector Label	J1 - J8
Impedance	50 Ω

Table 9-32. Holdover Performance

Oscillator	Holdover - 24 Hour (µsec)
Standard	400
OCXO	25
Rubidium	<1

Note: Holdover values are approximate and assume operation at constant temperature, no initial frequency or phase offset, and that the unit has been powered on for 2 weeks and locked to GNSS for three consecutive days.

9.2 GNSS Antenna Kits Specifications

The basic antenna kit (093-15202-001) consists of the following

- GNSS Antenna (112-00079-000) with internal LNA
- Mounting Bracket (193-00044-000)
- Adapter cable for chassis (060-15202-004). This cable has an N-connector on one end and a BNC-connector on the other end.

Other components available in kits or separately include the following:

- Lightning arrestor (112-43400-00-3)
- Inline Amplifier (112-15202-001)

See Table 7-7 for antenna kit part numbers.

9.2.1 GNSS Antennas with Internal LNA Specifications

The following table provides specifications for the GNSS antenna with internal LNA.

Table 9-33. GNSS Antenna with Internal Low-Noise Amplifier Specifications

Characteristic	Specification
Mechanical	
Diameter	66.5 mm
Height	21 mm
Weight	150 grams
Environmental	
Operating Temperature	• 40 to +85 °C
Environmental	IP67, CE, REACH, and RoHS compliant
Salt Fog / Spray	MIL-STD-810F Section 509.4
Electrical	
1 dB Bandwidth	31 MHz
10 dB Return Loss Bandwidth	45 MHz
Antenna Gain	4.5 dBic
Axial Ratio	<4 dB @ 1590 MHz, 8 dB typical at band-edges
Filtered LNA Frequency	1575 to 1606 MHz
Gain	40 dB minimum

...........continued

Characteristic	Specification
Gain	flatness ± 2 dB, 1575 to 1606 MHz
Out-of-Band Rejection <1550 MHz >1640 MHz	>50 dB >70 dB
VSWR (at LNA output)	<1.5:1
Noise Figure	2.5 dB typical
Supply Voltage Range	+2.5 to 16 VDC nominal (12 VDC recommended maximum)
Supply Current	20 mA maximum at 85°C

9.2.2 Wideband GNSS Antennas with Internal LNA Specifications

The following table provides specifications for the GNSS antenna with internal LNA

This wide-band antenna is a precision high gain GNSS antenna covering the BeiDou B1, Galileo E1, GPS L1, GLONASS L1, and SBAS (WAAS, EGNOS, QZSS, and MSAS) frequency band (1557 MHz to 1606 MHz). It provides very circular polarized signal reception through the entire bandwidth of the antenna, thereby providing superior multipath signal rejection. The antenna has a three stage low noise amplifier, comprised of one input LNA per feed, a mid section SAW to filter the combined output, and a final output gain stage. An additional pre-filter provides extra strong protection from near frequency and strong harmonic signals. An L-bracket for pole mounting and 3-foot BNC(m) to N(f) cable is also included.

Table 9-34. Wideband GNSS Antenna with Internal Low-Noise Amplifier Specifications

Characteristic	Specification
Mechanical	
Diameter	66.5 mm
Height	21 mm
Weight	150 grams
Environmental	
Operating Temperature	• 40 to +85 °C
Environmental	IP67, CE, REACH, and RoHS compliant
Salt Fog / Spray	MIL-STD-810F Section 509.4
Electrical	
2 dB Bandwidth	47 MHz
Antenna Gain (with 100 mm ground plane)	4.25 dBic
Axial Ratio	<2 dB typical, 3 dB max
Filtered LNA Frequency	1559 to 1606 MHz
Gain	40 dB minimum

...........continued

Characteristic	Specification
Out-of-Band Rejection <1500 MHz >1640 MHz	>50 dB >70 dB
VSWR (at LNA output)	<1.5:1
Noise Figure	3 dB typical
Supply Voltage Range	+2.5 to 16 VDC nominal (12 VDC recommended maximum)
Supply Current	19 mA maximum at 85°C

9.2.3 GNSS Lightning Arrestor Specifications

Table 9-35. Lightning Arrestor Specifications

Characteristic	Specification
Type	DC Pass
Mount Type	Bulkhead Mount
PIM Rated	N
Standards	CE Compliant, RoHS Compliant
Connector	N
Surge Side Connector	Bi-Directional N
Protected Side Connector	Bi-Directional N
Frequency Range	dc to 5 GHz
Turn On Voltage	150 Vdc (spark over)
RF Power	25 W
VSWR	<1.2 dB to 1
Insertion Loss	<0.1 dB
Protocol/Application	Gas tube, DC pass RF coaxial protection for dc to 5 GHz

9.2.4 GNSS L1 Inline Amplifier Specifications

The GNSS L1 Inline Amplifier (112-00076-000) option boosts the signal from the antenna. Use this amplifier on longer cable runs to maintain sufficient gain; it receives power from the GNSS radio receiver through the antenna coaxial cable connections. The following table provides mechanical and electrical specifications for the amplifier.

Table 9-36. GNSS L1 Inline Amplifier Specifications

Characteristic	Specification
Mechanical	
Connectors, (In/Out)	N-Type
Dimensions, includes connectors	Length: 2.32 in (59 mm)
Operating Temp.	• 40 to +85 °C

...........continued	
Characteristic	**Specification**
Environmental	RoHS, REACH, and IP67
Electrical	
Nominal Gain	25 dB +4/-0 dB typical
Pass Band Ripple	± 2 dB
Impedance	50 Ohms
Noise Figure	2 dB typical
Bandwidth	1.2 to 1.8 GHz
Input VSWR	1.5 typical / 2 maximum
Output VSWR	1.5 typical / 2 maximum
Reverse Isolation	>35 dB
Output 1 dB	• 10 dB
Output 3 dB	+5 dBm

9.2.5 GPS/GLONASS/BeiDou 1:4 Active Splitter Specifications

The GPS/GLONASS/BeiDou 1:4 active splitter option splits the signal from the antenna. The following table provides mechanical and electrical specifications for the high isolation active splitter.

This L band frequency, RoHS compliant 4:1 active splitter makes it possible to use a single GNSS referencing antenna and cable arrangement for multiple synchronization systems. The antenna DC bias select circuit allows for the active antenna DC input to be applied to any or all RF outputs. One DC voltage will be chosen to power the antenna while other inputs will be switched to DC loads. If the selected DC bias input should fail, the DC bias will automatically switch to another DC input to ensure an uninterrupted supply to the active antenna.

Table 9-37. GNSS L1 1:4 Active Splitter Specifications

Characteristic	Specification
Number of Output Ports	4
Input/output impedance	50 ohms
Frequency Range	1 GHz to 2 GHz
Noise Figure	2 dB max
Port-to-port isolation	30 - 40 dB
DC power	+3.3 to +12 V DC
Operating current	18 to 20 mA
Pass through current	250 mA
Group delay, L1	5 ns
RF connectors	Female N-type
RoHS 6/6	Compliant

9.2.6 GPS Antenna Coaxial Cable Specifications

Other cable types are available. The following table provides antenna cable specifications. Before using additional cables, verify that the total antenna system gain is acceptable.

Table 9-38. Antenna Cable Specifications

Cable Type	Loss (@1.575 GHz dB per foot)	DC Resistance (Ω per foot)	Type Center Conductor	Flammability
RG213/U (Belden 8267)	0.093 dB	0.0030	Stranded 13 AWG	U/L CSA
RG213/U (Belden 8267)	0.093 dB	0.0030	Stranded 2.62 mm^2	U/L CSA
UHF/VHF (Belden 9913)	0.058 dB	0.0027	Solid 10 AWG	
UHF/VHF (Belden 9913)	0.058 dB	0.0027	5.26 mm^2	
UHF/VHF (Belden 89913)	0.089 dB	0.0027	Solid 10 AWG	Plenum U/L CSA
UHF/VHF (Belden 89913)	0.089 dB	0.0027	5.26 mm^2	Plenum U/L CSA
LMR-400	0.051 dB	Shield – 0.00165 Center – 0.00139	0.109 inch Solid	
LMR-400	0.051 dB	Shield – 0.00165 Center – 0.00139	0.27686 cm^2 Solid	
LMR/CNT 240	0.101 dB	Inner Conductor – 0.0032 Outer Conductor – 0.00389	.056 inch diameter Solid BC	
LMR/CNT 600	0.034 dB	Inner Conductor – 0.00053 Outer Conductor – 0.0012	.176 inch diameter Solid BCCAI	

9.3 Factory Defaults

9.3.1 Network

Table 9-39. Network > Ethernet Parameters

Description	Default Value	Value Range
Speed	Auto	Auto | Full_100 | Full_1000

...........continued		
Description	**Default Value**	**Value Range**
IPv4	IPv4 uncheck/static	IPv4 uncheck | IPv4 check/DHCP | IPv4 check/Static
IP6v	IPv6 uncheck/ autoconfig /static	IPv6 uncheck | IPv6 check/ Autoconfig uncheck/static | IPv6 check/Autoconfig uncheck /DHCP | IPv6 check/Autoconfig check/static | IPv6 check/Autoconfig check/DHCP
Address (IPv4)	Blank (no value)	[<ipv4_address>]
Subnet (IPv4)	Blank (no value)	[<ipv4_address>]
Gateway (IPv4)	Blank (no value)	[<ipv4_address>]
Address (IPv6)	Blank (no value)	[<ipv6_address>]
Subnet (IPv6)	Blank (no value)	[<ipv6_address>]
Gateway (IPv6)	Blank (no value)	[<ipv6_address>]

Table 9-40. Network > SNMP Parameters

Description	Default Value	Value Range
sysLocation	unknown	[<printable ASCII>], 1 - 49 chars
Read Community	microcommr	[<printable ASCII>], 1 - 49 chars
SysName	SyncServer	[<printable ASCII>], 1 - 49 chars
Write Community	microcommw	[<printable ASCII>], 1 - 49 chars
sysContact	admin@ localhost	[<printable ASCII>], 1 - 49 chars
Name (v3 User)	Blank (no val	[<printable ASCII>], 1 - 49 chars
Priv Phrase (v3 User)	Blank (no val	[<printable ASCII>], 1 - 49 chars
Auth Phrase (v3 User)	Blank (no val	[<printable ASCII>], 1 - 49 chars
Min Priv (v3 User)	Authentication	Authentication | Authentication & Privacy
Auth Crypt (v3 User)	Blank (no value)	MD5 | SHA

Table 9-41. Network > SNMP Traps Parameters

Description	Default Value	Value Range
IP Address	Blank (no value)	<IPv4_address> | <IPv6_address>
v2c and v3	No Select	No Select | v2c | v3
User / Community	Blank (no value)	[<printable ASCII>], 1 - 32 chars
Send as Inform	uncheck	uncheck | check
Auth Phrase (v3)	Blank (no value)	[<printable ASCII>], 1 - 99 chars
MD5 / SHA (v3)	No check	If v3 check then [<MD5 check> | <SHA check>]
Priv Phrase (v3)	Blank (no value)	[<printable ASCII>], 1 - 99 chars

9.3.2 NTP

Table 9-42. NTP > NTP Configuration Parameters

Description	Default Value	Value Range
Role	Server	Server | Peer | Broadcast
Address	Blank (no value)	[<IPv4_address> | <IPv6_address> | <dns_name>]
Port	Default	LAN1 | LAN2 | LAN3 | LAN4
Prefer	uncheck	uncheck | check
Burst	N/A	N/A | Burst | iBurst | Both
MinPoll	Default	Power-of-2 times in seconds range: default | 16 | 32 | 64 | … | 65536 MinPoll cannot be > MaxPoll
MaxPoll	Default	Power-of-2 times in seconds range: default | 16 | 32 | 64 | … | 65536 MaxPoll cannot be < MinPoll
Symmetric	None	None | Auto | 1 | 2 | … | 17 | 18 | 19 | 20
TTL	7	1 to 7

9.3.3 PTP

Table 9-43. PTP > PTP Configuration Parameters for Enterprise Profile

Description	Default Value	Value Range
Domain	0	0 to 127
Two-Step	Disabled	Disabled | Enabled
Priority 1	128	0 to 255
Priority 2	128	0 to 255
Announce Interval	0	0 (fixed)
Sync Interval	0	• 7 to 7
Delay Interval	3	• 7 to 7
Announce Timeout	3	3 (fixed)
Client Timeout	300	10 to 3600
Diffserv Code	0	0 to 63
Offset Scaled Log Variance Override	Not checked	Not checked or checked
Offset Scaled Log Variance	0x4e5d	0x0 to 0xffff
Time To Live (TTL)	16	1 to 255

Table 9-44. PTP > PTP Master Configuration Parameters for Default Profile

Description	Default Value	Value Range
Domain	0	0 to 127
Two-Step	Disabled	Disabled | Enabled

...........continued		
Description	**Default Value**	**Value Range**
Priority 1	128	0 to 255
Priority 2	128	0 to 255
Announce Interval	0	• 3 to 3
Sync Interval	0	• 7 to 7
Delay Interval	3	• 7 to 7
Announce Timeout	3	2 to 10
Client Timeout	300	10 to 3600
Diffserv Code	0	0 to 63
Offset Scaled Log Variance Override	Not checked	Not checked or checked
Offset Scaled Log Variance	0x4e5d	0x0 to 0xffff
Time To Live (TTL)	16	1 to 255

Table 9-45. PTP > PTP Master Configuration Parameters for Telecom 2008 Profile

Description	Default Value	Value Range
Domain	0	0 to 127
Two-Step	Disabled	Disabled | Enabled
Priority 1	128	0 to 255
Priority 2	128	0 to 255
Unicast negotiation	Enable	Disable | Enable
Diffserv Code	0	0 to 63
Offset Scaled Log Variance Override	Not checked	Not checked or checked
Offset Scaled Log Variance	0x4e5d	0x0 to 0xffff
Time To Live (TTL)	16	1 to 255

Table 9-46. PTP > PTP Master Configuration Parameters for Power IEC-61850-2016 Profile

Description	Default Value	Value Range
Domain	0	0 to 255
Two-Step	Disable	Disable | Enable
Priority 1	128	0 to 255
Priority 2	128	0 to 255
Announce Interval	0	• 4 to 4
Sync Interval	0	• 7 to 7
Pdelay Resp Followup	Disable	Disable | Enable
Announce Timeout	3	2 to 10
Client Timeout	300	10 to 3600 seconds

...........continued		
Description	**Default Value**	**Value Range**
VLAN	Disable	Disable | Enable
VLAN ID	0	0 to 4094
VLAN Priority	4	0 to 7

Table 9-47. PTP > PTP Master Configuration Parameters for Power C37-238-2017 Profile

Description	Default Value	Value Range
Domain	254	0 to 127, 254
Two-Step	Disable	Disable | Enable
Priority 1	128	0 to 255
Priority 2	128	0 to 255
Announce Interval	0	• 4 to 4
Sync Interval	0	• 7 to 7
Pdelay Resp Followup	Disable	Disable | Enable
Announce Timeout	3	2 to 10
Client Timeout	300	10 to 3600 seconds
VLAN	Disable	Disable | Enable
VLAN ID	0	0 to 4094
VLAN Priority	4	0 to 7
C37.238 TLV - Grandmaster ID	0	0 to 65535
Alternate Time Offset Indicator TLV		
State	Enable	Disable | Enable
Current Offset	0	
Time of Next Jump	0	
Key	0	0 to 255
Jump Seconds	0	
Display Name		10 characters, maximum

Table 9-48. PTP > PTP Master Configuration Parameters for Power C37-238-2011 Profile

Description	Default Value	Value Range
Domain	0	0 to 127
Two-Step	Disable	Disable | Enable
Priority 1	128	0 to 255
Priority 2	128	0 to 255
Announce Interval	0	• 4 to 4
Sync Interval	0	• 7 to 7

...........continued		
Description	**Default Value**	**Value Range**
Pdelay Resp Followup	Disable	Disable | Enable
Announce Timeout	3	2 to 10
Client Timeout	300	10 to 3600 seconds
VLAN	Enable	Disable | Enable
VLAN ID	0	0 to 4094
VLAN Priority	4	0 to 7
C37.238 TLV - Grandmaster ID	3	3 to 254
Alternate Time Offset Indicator TLV		
State	Enable	Disable | Enable
Current Offset	0	
Time of Next Jump	0	
Key	0	0 to 255
Jump Seconds	0	
Display Name		10 characters, maximum

Table 9-49. PTP > PTP Master Configuration Parameters for SMPTE Profile - Hybrid

Description	Default Value	Value Range
Delay mechanism	E2E	E2E
Domain	127	0 to 127
Two step	Disable	Enable / Disable
Priority 1	128	0 to 255
Priority 2	128	0 to 255
PTP state	Enable	Enable / Disable
Announce Interval	-2	-3 to1
Sync Interval	-3	-7 to 1
Delay Pdelay Interval	-3	-7 to 4
Announce Timeout	3	2 to 10
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255

...........continued

Description	Default Value	Value Range
Default system frame rate	60/1	24/1 25/1 30/1 50/1 60/1 24000/1001 30000/1001 60000/1001
Time address flag - Bit 0	Non-drop frame	Non-drop frame Drop frame
Time address flag - Bit 1	Not in use	Not in use In use
Daily Jam	None	None Local Time: Hour 0 – 23, Minute 0, 10, 20, 30, 40, 50

Table 9-50. PTP > PTP Master Configuration Parameters for SMPTE Profile - Multicast

Description	Default Value	Value Range
Delay mechanism	E2E	E2E P2P
Domain	127	0 to 127
Two step	Disable	Enable / Disable
Priority 1	128	0 to 255
Priority 2	128	0 to 255
PTP state	Enable	Enable / Disable
Announce Interval	-2	-3 to1
Sync Interval	-3	-7 to 1
Delay Pdelay Interval	-3	-7 to 4
Announce Timeout	3	2 to 10
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255

...........continued		
Description	**Default Value**	**Value Range**
Default system frame rate	60/1	24/1 25/1 30/1 50/1 60/1 24000/1001 30000/1001 60000/1001
Time address flag - Bit 0	Non-drop frame	Non-drop frame Drop frame
Time address flag - Bit 1	Not in use	Not in use In use
Daily Jam	None	None Local Time: Hour 0 – 23, Minute 0, 10, 20, 30, 40, 50

Table 9-51. PTP > PTP Master Configuration Parameters for SMPTE Profile - Unicast

Description	Default Value	Value Range
Delay mechanism	E2E	E2E
Domain	127	0 to 127
Two step	Disable	Enable / Disable
Priority 1	128	0 to 255
Priority 2	128	0 to 255
PTP state	Enable	Enable / Disable
Announce Interval	n/a	n/a
Sync Interval	n/a	n/a
Delay Pdelay Interval	n/a	n/a
Announce Timeout	3	2 to 10
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255

...........continued		
Description	**Default Value**	**Value Range**
Default system frame rate	60/1	24/1 25/1 30/1 50/1 60/1 24000/1001 30000/1001 60000/1001
Time address flag - Bit 0	Non-drop frame	Non-drop frame Drop frame
Time address flag - Bit 1	Not in use	Not in use In use
Daily Jam	None	None Local Time: Hour 0 – 23, Minute 0, 10, 20, 30, 40, 50

Table 9-52. PTP > PTP Client Configuration Parameters for Telecom 2008 Profile

Description	Default Value	Value Range
Domain	0	0 to 255
Lease Duration	300	60 to 1000
Master 1		Valid IP address
Master 2		Valid IP address
Announce Interval	1	3 to1
Sync Interval	6	6 to -4
Delay Request Interval	6	6 to -4
Announce Timeout	3	2 to 10
Unicast negotiation	Enable	Disable | Enable
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255
FPP Cluster Width 1	10000	1000 to 10000000
FPP Cluster Width 2	10000	1000 to 10000000

Note: The SMPTE client standard of 5-second synchronization time is not applicable to the SyncServer S6x0.

Table 9-53. PTP > PTP Client Configuration Parameters for SMPTE Profile - Hybrid

Description	Default Value	Value Range
Delay mechanism	E2E	E2E
Domain	127	0 to 127
Lease Duration	n/a	n/a
Master 1	n/a	n/a
Master 2	n/a	n/a
PTP state	Enable	Enable / Disable
Announce Interval	n/a	n/a
Sync Interval	n/a	n/a
Delay Request Interval	-3	-6 to -3
Announce Timeout	3	2 to 10
Unicast negotiation	n/a	n/a
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255
FPP Cluster Width 1	10000	1000 to 10000000
FPP Cluster Width 2	10000	1000 to 10000000

Note: The SMPTE client standard of 5-second synchronization time is not applicable to the SyncServer S6x0.

Table 9-54. PTP > PTP Client Configuration Parameters for SMPTE Profile - Multicast

Description	Default Value	Value Range
Delay mechanism	E2E	E2E P2P
Domain	127	0 to 127
Lease Duration	n/a	n/a
Master 1	n/a	n/a
Master 2	n/a	n/a
PTP state	Enable	Enable / Disable
Announce Interval	n/a	n/a
Sync Interval	n/a	n/a
Delay Request Interval	• -3	• -6 to -3
Announce Timeout	3	2 to 10
Unicast negotiation	n/a	n/a
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255
FPP Cluster Width 1	10000	1000 to 10000000
FPP Cluster Width 2	10000	1000 to 10000000

Note: The SMPTE client standard of 5-second synchronization time is not applicable to the SyncServer S6x0.

Table 9-55. PTP > PTP Client Configuration Parameters for SMPTE Profile - Unicast

Description	Default Value	Value Range
Delay mechanism	E2E	E2E
Domain	127	0 to 127
Lease Duration	180	60 - 1000
Master 1		Valid IP address
Master 2		Valid IP address
PTP state	Enable	Enable / Disable
Announce Interval	-2	-3 to 1
Sync Interval	-3	-6 to -3
Delay Request Interval	-3	-6 to -3
Announce Timeout	3	2 to 10
Unicast negotiation	Enable	Enable / Disable
Diffserv Code	0	0 to 63
Time To Live (TTL)	64	1 to 255
FPP Cluster Width 1	10000	1000 to 10000000
FPP Cluster Width 2	10000	1000 to 10000000

9.3.4 Timing

Table 9-56. Timing > Holdover Configuration Parameters

Description	Default Value	Value Range
Time Error Limit	Computed from Holdover Duration default, result depends on oscillator type.	0.000100 ms to 100 ms
Holdover Duration	1 day	0.001 days to 200.00 days

Table 9-57. Timing > Serial Parameters

Description	Default Value	Value Range
Output	Off	Off | NMEA | NENA | Legacy
NMEA Detail	All Off	Any combination of the following allowed: ZDA on/off, GGA on/off, GSV on/off, RMV on/off
NENA Detail	DDD…	DDD… | WWW … | YYYY …

9.3.5 References

Table 9-58. References > GNSS Configuration Parameters

Description	Default Value	Value Range
GNSS Constellation	GPS	{GPS, Galileo, QZSS}, GLONASS, BeiDou (up to 2 groups)
SBAS Enable	Not checked	Checked or Not checked
Elevation Mask	10	5 to 60 degrees Step size is 1 deg
Mode	Survey	Survey | Position Hold | Dynamic
Latitude (for Position Hold)	N 0:0:0.000	Ndd:mm:ss.ss or Sdd:mm:ss.sss 0 to 90 degrees
Longitude (for Position Hold)	W 0:0:0.000	Eddd:mm:ss.ss or Wddd:mm:ss.sss 0 to 180 degrees
Altitude (for Position Hold)	0.0 m	• 1000.0 to +12000.0 m
Antenna Cable Delay	0	0 to 10000 ns
GNSS Receiver Reset	unchecked	checked | unchecked

9.3.6 Security

Table 9-59. Security > Users > Password Policy

Description	Default Value	Value Range
Maximum Number	6	6 to 100
Uppercase letter required	checked	not checked | checked
Lower case letter required	checked	not checked | checked
Number required	checked	not checked | checked
Special character required	checked	not checked | checked

Table 9-60. Security > Users > Password Expiration

Description	Default Value	Value Range
Password expiry	Enable	Enable / Disable
Number of days	365	1 to 365

Table 9-61. Security > Users Parameters

Description	Default Value	Value Range
User	new user	new user | list of existing users
Delete Selected User	not checked	not checked | checked

...........continued

Description	Default Value	Value Range
New Username	Blank (no value) Only admin user is retained.	a-z, 0-9, _, 1 – 32 chars, First character must be a lowercase alpha character (not underscore or number)
New Password	Blank (no value)	[<printable ASCII>, 1 – 64 chars Passwords must contain at least 8 characters, including uppercase, lowercase letters, numbers and special characters. The following characters are not allowed for the password: (', “, <, >, &,), $
Retype New Password	Blank (no value)	This is same as “New Password”
Recovery Question	No selection	[Birth City? | Mother’s Maiden Name? | Favorite pet’s name? | Custom] <printable ASCII> , 1 – 34 chars
Answer	Blank (no value)	<printable ASCII>, 1 – 34 chars
Email Address	Blank (no value)	<printable ASCII>, 1 – 34 chars
SMTP Gateway	Blank (no value)	<printable ASCII>, 1 – 34 chars
Send Test Email	not checked	not checked | checked

Table 9-62. Security > Services State Parameters

Description	Default Value	Value Range
Webserver	Checked	Checked | Not Checked
SNMP	Checked	Checked | Not Checked
SSH	Checked	Checked | Not Checked
TOD	Checked	Checked | Not Checked
Telnet	Not Checked	Checked | Not Checked

Table 9-63. Security > HTTPS Web Server Parameters

Description	Default Value	Value Range
Protocols	TLS 1.2	TLS 1.1 | TLS 1.2
Cipher Suites	SSL_HIGH_ ENCRYPTION	SSL_HIGH_ENCRYPTION | SSL_HIGH_AND_MEDIUM_ENCRYPTION
SSL Timeout	10 Minutes	5 to 1440 Minutes

Table 9-64. Security > LDAP Settings

Description	Default Value	Value Range
Port - Server Binding	389	1 to 65535
Time Limit for Searching	300	120 to 65535 seconds
Time Limit for binding	300	120 to 65535 seconds

...........continued

Description	Default Value	Value Range
LDAP Protocol version	LDAPv3	LDAPv2 | LDAPv3
Scope to search server	sub	base | one | sub

9.3.7 Admin

Table 9-65. Admin > General Parameters

Description	Default Value	Value Range
Hostname	SyncServer	
Web Session Timeout	10 min	5 | 10 | 15 | 30 | 60 minutes
Check for Software Upgrades	checked	not checked | checked
Enable Lockout for Failed Login Attempts	checked	not checked | checked
Allowed Number of Failed Login Attempts	3	3 to 6

Table 9-66. Admin > Alarm Relay Parameters

Description	Default Value	Value Range
Top Selection	Off	Any Major Alarm | Any Major or Minor Alarm | Off
System Restart Delay	0	0, 1, 2,..., 60 minutes

Table 9-67. Admin > Alarms Parameters

Description	Default Value	Value Range
Name	N/A	Cannot be set by user. See Table 8-1 for name of each alarm
State	Strictly condition driven	• Green = condition not set or has been acknowledged • Blue = condition set at Notify severity (and has not been user cleared or acknowledged) • Orange = condition set at Minor severity (and has not been user cleared or acknowledged) • Red = condition set at Major severity (and has not been user cleared or acknowledged) • Gray = this is a transient alarm
Clear Now	not checked (all rows)	not checked | checked
Auto ACK (s)	0 (all rows)	0, 1, ..., 999, 1000
Severity	See Table 8-1 for default severity for each alarm	Notify | Minor | Major
Reporting Delay (s)	0 (all rows)	0, 1, ..., 999, 1000

...........continued		
Description	**Default Value**	**Value Range**
Send Trap	checked (all rows)	not checked | checked
Write Log	checked (all rows)	not checked | checked
Send Email	not checked (all rows)	not checked | checked

Table 9-68. Admin > Serial Port Config Parameters - Serial/Data Port

Description	Default Value	Value Range
Baud Rate	9600	4800 | 9600 | 19.2k | 38.4k | 57.6k | 115.2k
Data Bits	8	7 | 8
Parity	none	none | even | odd
Stop Bits	1	1 | 2

Table 9-69. Admin > Serial Port Config Parameters - Console Port

Description	Default Value	Value Range
Baud Rate	115.2k	4800 | 9600 | 19.2k | 38.4k | 57.6k | 115.2k
Data Bits	8	8 (fixed)
Parity	none	none (fixed)
Stop Bits	1	1 (fixed)

9.3.8 Timing I/O Modules

Table 9-70. Timing I/O Module Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-71. Timing I/O Module - Telecom E1/T1 Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns

...........continued	
Description	**Value Range**
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	T1 output; ESF
J8	E1 output; CCS; SSMbit 4; CRC enable; zero suppress on

Table 9-72. Timing I/O Module - HaveQuick/PTTI Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-73. Timing I/O Module - Fiber Input Default Parameters

Description	Value Range
J1	Pulse; Fixed rate; 1PPS; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-74. Timing I/O Module - Fiber Output Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B1344 DCLS; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns

...........continued	
Description	Value Range
J7	Off
J8	Off

9.3.8.1 Timing I/O Modules

Table 9-75. Timing I/O Module Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-76. Timing I/O Module - Telecom E1/T1 Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	T1 output; ESF
J8	E1 output; CCS; SSMbit 4; CRC enable; zero suppress on

Table 9-77. Timing I/O Module - HaveQuick/PTTI Default Parameters

Description	Value Range
J1	Timecode; IRIG B; 1kHz, with year; 50 ohm; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-78. Timing I/O Module - Fiber Input Default Parameters

Description	Value Range
J1	Pulse; Fixed rate; 1PPS; cable delay of 0 ns
J2	Sine; 10 MHz
J3	Timecode; IRIG B; no local time; B124; squelch never; phase offset of 0 ns
J4	Sine; 10 MHz; squelch never
J5	Timecode; IRIG B; no local time; B004; squelch never; phase offset of 0 ns
J6	Pulse; Fixed rate; 1PPS; squelch never; phase offset of 0 ns
J7	Off
J8	Off

Table 9-79. Timing I/O Module - LPN/ULPN Default Parameters

Description	Default	Value Range
10 MHz to 1PPS Coherency	Disable	Enable | Disable

9.3.9 BlueSky-Related Factory Default Configuration

This section lists factory presets for all user-settable parameters related to the BlueSky capabilities. These are the settings that a new unit will have upon arrival from factory but also can accomplished at any time via the Admin > Config Backup/Restore form. All settings are retained through power-cycle.

Table 9-80. Bluesky Related Factory Defaults

Parameter	Factory Default Configurations	Details
Tracking group action, *Spoofing group* action, *validator anomalies group* action, *RF Health group* action	Stopped. Action column will appear as for each, indicating that it can be started.	Configured with BlueSky GNSS Detector Summary form See Figure 6-34.
GNSS Site Survey action	Stopped. Action column will appear as for each, indicating that it can be started.	Configured with BlueSky GNSS Detector Summary form See Figure 6-34.
Tracked satellites detector threshold	4 satellites	Set with BlueSky Configuration form See Figure 6-35.
Max C/No detector threshold	60	Set with BlueSky Configuration form See Figure 6-35.
Position dispersion threshold	100 meters	Set with BlueSky Configuration form See Figure 6-35.
CW Jamming threshold	50%	Set with BlueSky Configuration form See Figure 6-35.
Alarm Enable checkbox (applies to all detectors on configuration form)	NOT checked (alarm function is disabled)	Set with BlueSky Configuration form See Figure 6-35.
GNSS Action on alarm (applies to all detectors on configuration form)	None (no GNSS action taken on alarm)	Set with BlueSky Configuration form See Figure 6-35.

Table 9-81. Bluesky Alarms - Generic Alarm Factory Presets

Parameter	Factory Default Configurations	Details
Severity	*Major* Applies to all BlueSky alarms other than those listed below in Minor and Notify categories *Minor* Applies to BlueSky GNSS tracking count detector and BlueSky GNSS Max C/No detector *Notify* Applies to BlueSky GNSS RAIM detector, BlueSky GNSS Validator E detector, and BlueSky GNSS Validator F detector	
Clear Now	*Not checked* (applies to all BlueSky alarms)	
Auto ACK	0 seconds (applies to all BlueSky alarms)	
Reporting Delay	0 seconds (applies to all BlueSky alarms)	
Send Trap	Checked (enabled) (applies to all BlueSky alarms)	
Write Log	Checked (message log will be written to) (applies to all BlueSky alarms)	
Send Email	*Not checked* (email will NOT be sent) (applies to all BlueSky alarms)	
GNSS Action on alarm (applies to all detectors on configuration form)	None (no GNSS action taken on alarm)	

10. Installing GNSS Antennas

The GNSS L1 Reference Antenna is one component of a complete line of GNSS accessories for your GNSS antenna system provided by Microchip. These accessories are designed to deliver precise GNSS signals over a wide temperature range and in harsh environmental conditions.

10.1 Antenna Kits Overview

Deciding on which of the available antenna kits meets your needs, the key factor is the distance between the GNSS antenna and the SyncServer S6x0. There are several coaxial cable lengths available to assist in receiving proper gains from the GNSS antenna. Microchip offers eight antenna kits for the SyncServer S6x0, plus separate GNSS antenna accessory parts including the antenna, cable, amplifier, lightning arrestor, and splitter.

10.1.1 Considerations for Antenna Installation

The GNSS engine requires a net gain at the antenna connector input of the chassis to be between 15 to 30 dB. All antenna kits include the GNSS L1 antenna, mounting bracket and a BNC cable adapter. The antennas, in-line amplifiers and the lightning arrestor have N connectors. All antenna kits supplied use a LMR-240 or LMR-400, or equivalent, low-loss coaxial cable. The L1 signal loss of LMR-400 is 0.173 dB/meter. The L1 signal loss of LMR-240 is 0.33 dB/meter. The L1 signal loss of a lightning arrestor is typically less than 0.25 dB. See Antenna Coaxial Cable.

10.1.1.1 GNSS Antennas with Low Noise Amplifiers

The antenna used with the SyncServer S600/S650 is a high-gain (40dB) GNSS antenna covering the GPS L1, GLONASS L1, and SBAS (WAAS, EGNOS and MSAS) frequency band (1575 to 1606 MHz). The antenna has a three stage low-noise amplifier, with a mid-section SAW with a tight pre-filter to protect against saturation by high level sub-harmonics and L-Band signals making it excellent for timing applications. An L-bracket for pole mounting and 3-foot BNC(m) to N(f) cable is also included.

Figure 10-1. GNSS Antenna

Accuracy of the antenna position determined using receiver survey depends on providing RF gain to the GNSS receiver within a required range of 15 to 30 dB and locating the antenna with an unobstructed field of view in a low multipath environment. If these conditions are not met, the receiver survey will either require longer than 20 minutes to complete or will not complete, preventing the GNSS input from being used by the system as a reference. Also, timing stability will not be optimized if these conditions are not met.

10.2 Antenna Kits Accessories

10.2.1 Lightning Arrestor

Microchip offers the lightning arrestor for installations that require antenna coaxial lead-in protection. The lightning arrestor passes DC power and frequencies in the 1.5 GHz range with L1 GNSS antennas. In most installations, the lightning arrestor mounts near the point at which the antenna lead enters the facility. See the GNSS Lightning Arrestor Specifications, for specifications.

Lightning does not have to strike the antenna to significantly damage the antenna or the GNSS receiver. Damage is often due to the effects of a lightning strike on a nearby structure, not a direct strike on the antenna itself. Since lightning strikes may induce damaging voltages in the antenna system when striking nearby objects, attempt to locate the antenna away from lightning rods, towers, and other structures that attract lightning. Also, locate the GNSS antenna lower than any nearby structures that are likely to attract a strike. See the following image.

Figure 10-2. GNSS Lightning Arrestor

10.2.2 GNSS L1 In-line Amplifier

The GNSS L1 in-line amplifier (093-15202-005) option boosts the signal from the antenna with total cable lengths of 150 and 230 meters. See the GNSS L1 Inline Amplifier Specifications for specifications.

Cable length is a common cause for signal loss between the GNSS antenna and the GNSS receiver. As with any electromagnetic radio wave, GNSS signals become attenuated as they pass through an electrical cable. The amount of signal loss depends on the length and type of cable used. The inline amplifier attaches inline between the antenna and the antenna cable. It uses the same power as the antenna and does not require extra wiring. The inline amplifier supports a total cable length up to 900 feet depending on the cable type. See the following image.

Figure 10-3. Inline Amplifier

10.2.3 GPS L1 1:4 Active Splitter

The active splitter features four output ports, as shown in the following image. See the GPS L1 1:4 Active Splitter Specifications for specifications.This high isolation device can be cascaded without adding separate amplifiers and bias-tees between splitters. The splitter delivers precise GPS signals over a wide temperature range and in harsh environmental conditions. It eliminates feedback and interaction between any GPS system connected to it.

Figure 10-4. GPS L1 1:4 Active Splitter

10.2.4 GPS/GLONASS/BeiDou Splitter

This L band frequency, RoHS compliant 4:1 active splitter makes it possible to use a single GPS referencing antenna and cable arrangement for multiple synchronization systems. The antenna DC bias select circuit allows for the active antenna DC input to be applied to any or all RF outputs. One DC voltage will be chosen to power the antenna while other inputs will be switched to DC loads. If the selected DC bias input should fail, the DC bias will automatically switch to another DC input to ensure an uninterrupted supply to the active antenna.

Figure 10-5. GPS/GLONASS/BeiDou Splitter

10.3 Antenna Coaxial Cable

Microchip provides coaxial cables with N-type connectors on both ends. The following table lists the part numbers for the cables and its crimp kit. Also see GPS Antenna Coaxial Cable Specifications,.

Table 10-1. LMR-400 Antenna Coaxial Cable Accessories

Part Number	Description
121-32212-00-2	Type N (male) connector for LMR-400 cable
12813080-000-0	Crimp Kit for LMR-400 or equivalent (10 ea. N-Type connector, crimp tool, weatherproof tape)
Contact your sales office for available cable lengths and specific cable item number.	

10.4 SyncServer Down/Up Converter

For very long antenna runs, down/up converters can be used. There are both coaxial and fiber-optic variations.

Microchip has sold the 142-6150 family of down/up converters, which supports the L1 frequency. Therefore it only supports GPS, Galileo, QZSS, and SBAS for GPS. This system uses a coaxial cable between the converters. The upconverter is inserted between the end of the coaxial cable and the SyncServer. The upconverter is powered by an external power supply.

The upconverter was designed to also operate from power supplied on the RF connector. However, the SyncServer S6x0 does not have sufficient power output to power the upconverter.

The upconverter may not operate correctly if the SyncServer S6x0 is powered up before the upconverter's external power supply.

Microchip recommends that users install a DC-block between the upconverter and the SyncServer S6x0.

Microchip also sells a GNSS-RF-over-fiber extension kit, the 093-15203-001.

10.5 GNSS Antenna Installation

This section provides information about planning and installing a GNSS antenna.

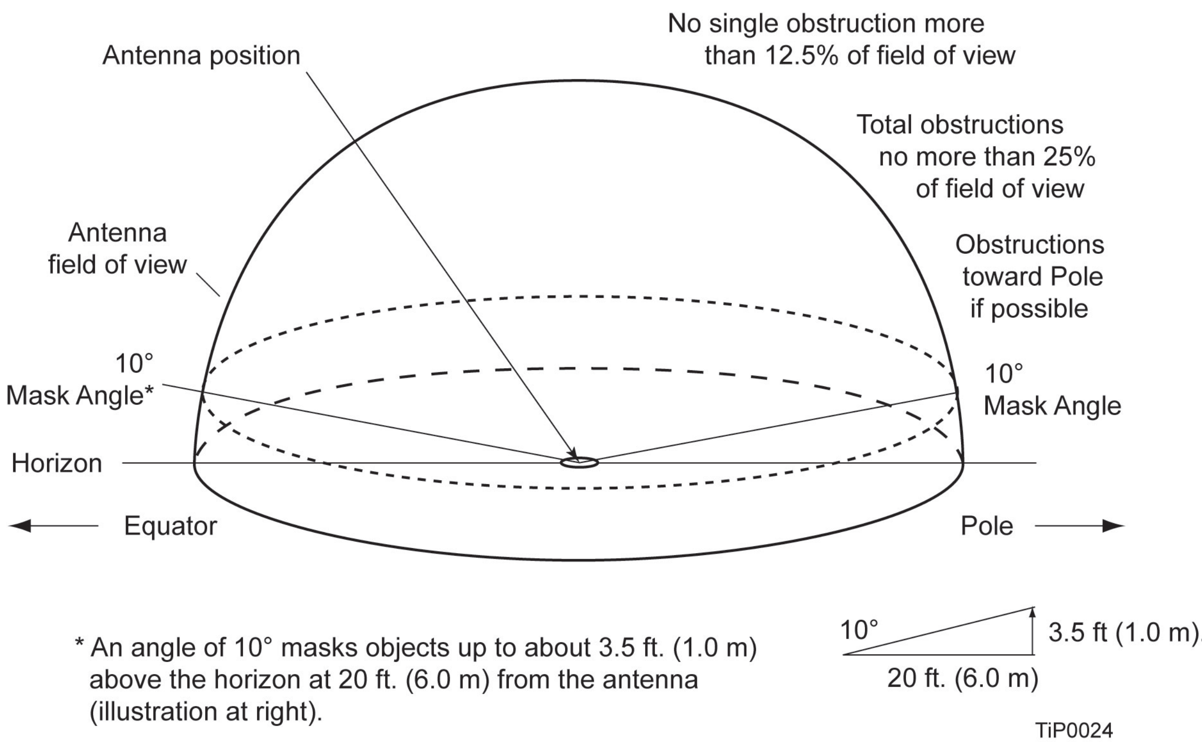
10.5.1 Planning the Antenna Location

Prior to installing the antenna, you should plan the site, antenna location, grounding scheme, cable route, and all other details.

10.5.2 Locating the Antenna

Use the following image as a guide to locate the antenna.

Figure 10-6. Locating the GNSS Antenna



⚠WARNING The SyncServer S6x0 GNSS interface uses the electrical current it supplies to power a GNSS antenna to determine whether or not the antenna is properly connected and functional. If the SyncServer S6x0 does not detect any current, it will assume a failed GNSS antenna and will consequently generate an alarm and switch to another timing (non-GNSS) source.
Some GNSS splitters can block the DC current, and if used with SyncServer S6x0, will cause the alarm condition described above. Usage of such GNSS splitters with the SyncServer S6x0 will require the installation of a 50 OHM load so that the SyncServer S6x0 GNSS interface is able to detect current and operate normally.

⚠ CAUTION To avoid damage to the GNSS antenna, do not place the antenna where high-power radio signals are beamed directly at the unit. Such signals can damage the preamplifier of the GNSS antenna.

⚠WARNING To avoid serious injury to personnel or damage to equipment, exercise caution when working near high voltage lines. In particular:

- Use extreme caution when installing the GNSS antenna near, under, or around high voltage lines.
- Follow local building electrical codes for grounding using the frame ground lugs on the shelf.
- The in-line amplifier receives DC power from the GNSS receiver, and is supplied on the center conductor of the coaxial cable.
- Microchip does not recommend cutting the antenna cables provided in the GNSS Antenna Kit.

Tip: Microchip recommends that you consider the following location and environment influences before installing the GNSS antenna:

- If possible, provide the antenna with an unobstructed 360-degree view of the sky from the horizon.
- In general, do not allow obstructions that obscure the horizon (as viewed from the antenna) by more than 10 degrees, as shown in the above image.
- Locate the antenna well away from, and preferably in a plane above electrical equipment such as elevators, air conditioners, or other machinery.
- To reduce the risk of lightning damage, do not place the antenna at the highest point of the building.
- Locate the GNSS antenna at least 3.7 m (12 ft.) from metallic objects, if possible.
- Locate the antenna high enough to avoid drifted snow.
- Locate the lightning arrestor in a protected area to avoid contact with standing water.
- Locate the antenna within 9.1 m (30 ft.) of the point at which the antenna cable enters the building.
- Allow at least 3.0 m (10 ft.) of separation distance between GNSS antennas.
- Surfaces above the plane of the unit that are between the antenna and the horizon can produce reflected (multi-path) signals, which can degrade the performance of the GNSS receiver.

10.5.3 Developing a Grounding Scheme

In addition to determining where to locate and mount the antenna and cabling, you should develop a grounding scheme. The purpose of the grounding scheme is to provide some protection against voltage surges and static discharge. If lightning arrestors are used, they also need to be connected to the perimeter ground system or to the bulkhead entrance panel that is connected to the perimeter ground system.

⚠ CAUTION To ensure proper grounding, observe these precautions when installing the antenna:

- Allow no sharp bends in the ground conductors. The ground conductor must have a 9.1 m (30-ft.) radius for any bends made.
- Ensure that no painted surface insulates the lightning arrestor or grounding clamps.
- Ensure that ground conductors are bonded to the metal enclosure box (if used) and do not enter through an access hole.
- Do not use soldered connections for grounding purposes.
- Secure all grounding connections with mechanical clamp type connectors.

- In general, follow local building codes when selecting a grounding scheme, wire size, and installation. Use #6 AWG (16 mm^2) copper ground wire or larger, depending on the distance to the earth ground electrode. Refer to your local electrical codes for specific details. In most cases, #1/0 AWG (50 mm^2) ground wire will maintain 1/10 the resistance of the coaxial shield.

  Note: Larger ground conductors provide better transient elimination; that is, the larger the ground conductor, the less likely the chance of transients.
- Connect lightning arrestors, if part of the grounding scheme, to earth ground through a conductor.
  Note: Do not connect the outside lightning arrestor ground to the inside equipment rack ground. Doing so can defeat the protection afforded by the lightning arrestor.
- Never connect antenna systems to the same earth ground connector as heating and cooling systems, elevator or pump motors, or other motors or machinery which can induce noise in the antenna system.

10.5.4 Antenna Installation Tools and Materials

These standard tools and materials are not supplied in the antenna kit, but may be required for installing the GNSS antenna.

- Extra cable ties or acceptable cable clamps
- #6 AWG (16 mm^2) copper ground wire (minimum)
- Eight-foot (2.9 m) ground electrode
- Custom mounting plates, U-bolts, PVC pipes, masonry bolt, etc. as needed for mounting to a tower, roof, or wall of a building
- A cable puller may be required for installing the antenna coaxial cable
- Digital multivoltmeter (DVM)

⚠ CAUTION To avoid damage to the connectors, do not use the connectors to pull the cable. If at all possible, avoid bundling the coaxial cable with other cables (and possible noise sources). Use appropriate cable-pulling devices when pulling the coaxial cable through conduit or a weather head.

10.5.5 Cutting Antenna Cables

Microchip recommends that you coil excess cable to avoid gain mismatch between the GNSS antenna and the GNSS receiver. Coiling the excess cable also allows you to use the factory-installed crimped connector.

Microchip does not recommend cutting the antenna cables provided in the GNSS Antenna Kits. If you must cut the cables, please ensure that the following requirements are met.

Cable Requirements – The total cable length from the GNSS receiver to the antenna must not be shorter than the minimum cable lengths indicated in the GNSS Antenna Kits (see Table 10-1).

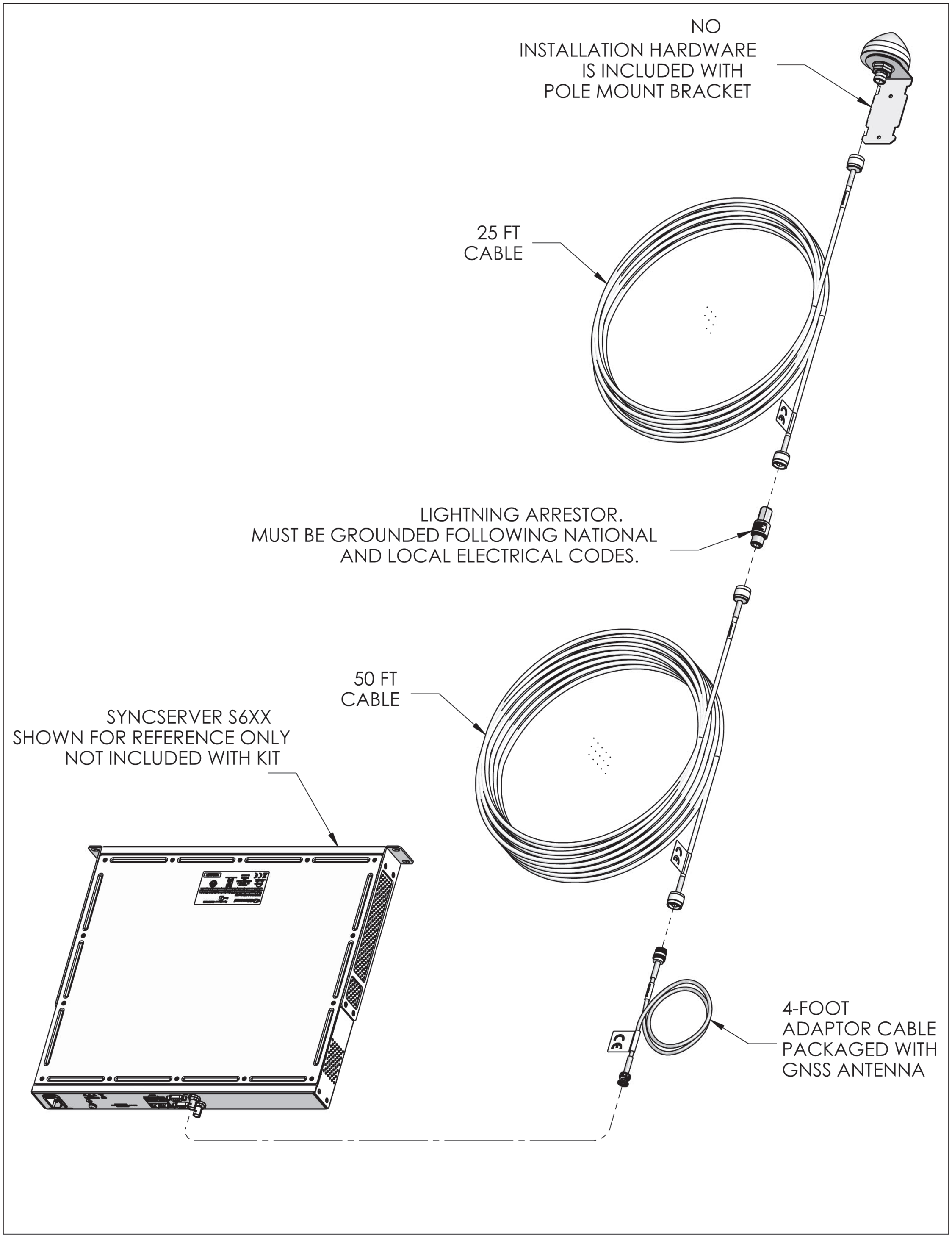
Connector Requirements – The cables provided with the GNSS antenna kit have factory installed crimped connectors. If you cut these cables, you must supply and add a connector. Microchip recommends that you use only crimp-style N-type connectors.

10.5.6 Installing the Antenna

This section provides procedures for installing the GNSS antenna (see the following image).

1. Insert the antenna into the right-angle mounting bracket and tighten it using the antenna nuts.
2. Mount the right-angle bracket to the mast using for example, U-bolts.
3. To secure the coaxial cable to the mast, use 8-inch cable ties or appropriate cable clamps.
4. Adhere to local building codes to determine the type and number of fasteners, screws, bolts, etc. that may be required.
   Note: Follow local building electrical codes when installing the GNSS antenna.

Figure 10-7. GNSS Antenna Installation



10.5.7 Connecting the Cable to the Antenna

This section describes how to connect the coaxial cable to the mounted antenna. See the Figure 10-1.

1. Connect the 25 ft. cable to the antenna..

⚠ CAUTION To avoid damage to the connectors, do not use the connectors to pull the cable. If at all possible, avoid bundling the coaxial cable with other cables (and possible noise sources). Use appropriate cable-pulling devices when pulling the coaxial cable through conduit or a weather head.

2. Connect the other end of the 25 ft. cable to the lightning arrestor.
3. Connect the lightning arrestor to the long cable.
4. Connect the other end of the long cable with the 4 ft. BNC-N adapter cable.

⚠ CAUTION To avoid damage to internal solder connections, do not over-tighten the connector.

10.5.8 Installing the Lightning Arrestor

Lightning arrestors should be installed in accordance with your antenna system grounding scheme. To install a lightning arrestor, follow these steps:

1. Mount the lightning arrestor within 30 ft. (9 m) of the GNSS antenna.
2. Connect the ground wire between the lightning arrestor and the proper grounding zone (building ground, master ground bar, or other) for the mounting location.

Tip: Microchip does not recommend soldered connections for grounding purposes. All grounding connections should be secured with mechanical clamp connectors.

3. Wrap the connectors with weatherproof tape for added protection.
4. Verify that the antenna coaxial cable center conductor is not shorted to the shield of the cable.

10.5.9 Connecting the GNSS Antenna

You should install the antenna cable from the lightning arrestor to the SyncServer S6x0 using the shortest route possible. Follow all applicable building and electrical codes to ensure a water-tight and fire-resistant installation.

⚠ CAUTION To avoid damage to the connectors, do not use the connectors to pull the cable. If at all possible, avoid bundling the cable with other cables (and possible noise sources). Use appropriate cable-pulling devices when pulling the cable through conduit or a weather head.

To connect the GNSS antenna, perform the following steps:

1. Using a DVM, Verify that the center conductor is not shorted to the shield.
   If the reading shows a short or open, you may have a shorted or open cable or lightning arrestor. Therefore, apply the same measurements directly to the GNSS antenna. This requires disconnecting the antenna cable at the antenna.

   Note: The open-circuit range of an individual ohmmeter can cause readings to vary among meters.
2. Secure the free end of the antenna cable to the BNC (f) antenna connector on the rear panel of the SyncServer S6x0.

Tip: Microchip recommends coiling excess cable to avoid gain mismatch between the GNSS antenna and the SyncServer S6x0. Coiling the excess cable also allows you to use the factory-installed crimped connector.

10.5.10 Antenna Installation Completeness Checklist

To verify that antenna installation is complete:

- Verify that all power and ground wires are installed correctly and securely fastened.
- Verify that all input and output cables are properly installed.
- Verify that all antenna connectors are secure, tight, and weatherproofed.
- Microchip does not generally recommend the use of GNSS splitters. However, if one is used, Microchip recommends the use of GPS L1 1:4 Active Splitter.

11. Software Licenses

This product contains licensed third party software, including software available under the GPL licensing scheme. You can obtain these licenses and the open-source software by contacting Microchip Technical support at the following numbers:

- Worldwide (Main Number): 1-408-428-7907
- USA, Canada, Latin America including Caribbean, Pacific Rim including Asia, Australia and New Zealand: 1-408-428-7907
- USA toll-free: 1-888-367-7966
- Europe, Middle East & Africa: 49 700 32886435

An administrative fee may be charged to obtain the source code.

By using the SyncServer S6x0, the user agrees to the terms of these licenses.

The licenses can be obtained using the following URLs:

- www.gnu.org/licenses
- www.apache.org/licenses
- www.boost.org/users/license.html
- opensource.org/licenses/BSD-3-Clause
- opensource.org/licenses/BSD-2-Clause
- opensource.org/licenses/MIT
- opensource.org/licenses/Python-2.0
- spdx.org/licenses/bzip2-1.0.6.html
- spdx.org/licenses/AFL-2.1.html
- www.opensource.org/licenses/ISC
- www.openssl.org/source/license.html
- www.openldap.org/software/release/license.html
- www.opensource.org/licenses/Artistic-1.0
- www.zlib.net/zlib_license.html
- opensource.org/licenses/PHP-3.0

11.1 Third-Party Software

The following is a list of third-party software applications provided with the SyncServer S6x0.

- PACKAGE NAME: adduser
  PACKAGE VERSION: 3.115

  RECIPE NAME: adduser

  LICENSE: GPLv2
- PACKAGE NAME: apache2

  PACKAGE VERSION: 2.4.34

  RECIPE NAME: apache2

  LICENSE: Apache-2.0
- PACKAGE NAME: apr

  PACKAGE VERSION: 1.5.2

  RECIPE NAME: apr

  LICENSE: Apache-2.0
- PACKAGE NAME: apr-util

  PACKAGE VERSION: 1.5.4

RECIPE NAME: apr-util

LICENSE: Apache-2.0

- PACKAGE NAME: autoconf

  PACKAGE VERSION: 2.69

  RECIPE NAME: autoconf

  LICENSE: GPLv2 GPLv3
- PACKAGE NAME: base-files

  PACKAGE VERSION: 3.0.14

  RECIPE NAME: base-files

  LICENSE: GPLv2
- PACKAGE NAME: base-passwd

  PACKAGE VERSION: 3.5.29

  RECIPE NAME: base-passwd

  LICENSE: GPLv2+
- PACKAGE NAME: bash

  PACKAGE VERSION: 4.3.30

  RECIPE NAME: bash

  LICENSE: GPLv3+
- PACKAGE NAME: binutils

  PACKAGE VERSION: 2.26

  RECIPE NAME: binutils

  LICENSE: GPLv3
- PACKAGE NAME: boost

  PACKAGE VERSION: 1.60.0

  RECIPE NAME: boost

  LICENSE: BSL-1.0 & MIT & Python-2.0
- PACKAGE NAME: busybox

  PACKAGE VERSION: 1.24.1

  RECIPE NAME: busybox

  LICENSE: GPLv2 & bzip2
- PACKAGE NAME: ca-certificates

  PACKAGE VERSION: 20160104

  RECIPE NAME: ca-certificates

  LICENSE: GPL-2.0+ & MPL-2.0
- PACKAGE NAME: conntrack-tools

  PACKAGE VERSION: 1.4.0

  RECIPE NAME: conntrack-tools

  LICENSE: GPLv2+
- PACKAGE NAME: coreutils

  PACKAGE VERSION: 8.25

  RECIPE NAME: coreutils

LICENSE: GPLv3+

- PACKAGE NAME: cronie

  PACKAGE VERSION: 1.5.0

  RECIPE NAME: cronie

  LICENSE: ISC & BSD-3-Clause & BSD-2-Clause & GPLv2+
- PACKAGE NAME:dbus

  PACKAGE VERSION: 1.10.6

  RECIPE NAME:dbus

  LICENSE: AFL-2 | GPLv2+
- PACKAGE NAME: dhcp-client

  PACKAGE VERSION: 4.3.0

  RECIPE NAME: dhcp

  LICENSE: ISC
- PACKAGE NAME: diffutils

  PACKAGE VERSION: 3.3

  RECIPE NAME: diffutils

  LICENSE: GPLv3+
- PACKAGE NAME: directc

  PACKAGE VERSION: 0.1

  RECIPE NAME: directc

  LICENSE: GPLv2
- PACKAGE NAME: dosfstools

  PACKAGE VERSION: 3.0.28

  RECIPE NAME: dosfstools

  LICENSE: GPLv3
- PACKAGE NAME: drivertestprogs

  PACKAGE VERSION: 0.1

  RECIPE NAME: drivertestprogs

  LICENSE: GPLv2
- PACKAGE NAME: dtc

  PACKAGE VERSION: 1.4.1+gitAUTOINC+302fca9f4c

  RECIPE NAME: dtc

  LICENSE: GPLv2 BSD
- PACKAGE NAME: e2fsprogs

  PACKAGE VERSION: 1.42.99+1.43+gitAUTOINC+0f26747167

  RECIPE NAME: e2fsprogs

  LICENSE: GPLv2 LGPLv2 BSD MIT
- PACKAGE NAME: elfutils

  PACKAGE VERSION: 0.164

  RECIPE NAME: elfutils

  LICENSE: GPLv3+ Elfutils-Exception
- PACKAGE NAME: ethtool

PACKAGE VERSION: 4.2

RECIPE NAME: ethtool

LICENSE: GPLv2+

- PACKAGE NAME: expat

  PACKAGE VERSION: 2.1.0

  RECIPE NAME: expat

  LICENSE: MIT
- PACKAGE NAME: expect

  PACKAGE VERSION: 5.45

  RECIPE NAME: expect

  LICENSE: PD
- PACKAGE NAME: factorycfg

  PACKAGE VERSION: 1.0

  RECIPE NAME: factorycfg

  LICENSE: BSD
- PACKAGE NAME: fuse

  PACKAGE VERSION: 2.9.3

  RECIPE NAME: fuse

  LICENSE: GPLv2 & LGPLv2
- PACKAGE NAME: gator

  PACKAGE VERSION: 5.21.1+gitAUTOINC+f0ddf6b40e

  RECIPE NAME: gator

  LICENSE: GPLv2
- PACKAGE NAME: gawk

  PACKAGE VERSION: 4.1.3

  RECIPE NAME: gawk

  LICENSE: GPLv3
- PACKAGE NAME: gdb

  PACKAGE VERSION: 7.10.1

  RECIPE NAME: gdb

  LICENSE: GPLv2 GPLv3 LGPLv2 LGPLv3
- PACKAGE NAME: glib-2.0

  PACKAGE VERSION: 2.46.2

  RECIPE NAME: glib-2.0

  LICENSE: LGPLv2+ & BSD & PD
- PACKAGE NAME: glibc

  PACKAGE VERSION: 2.23

  RECIPE NAME: glibc

  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: gmp

  PACKAGE VERSION: 6.1.0

RECIPE NAME: gmp

LICENSE: GPLv2+ | LGPLv3+

- PACKAGE NAME: gnu-config

  PACKAGE VERSION: 20150728+gitAUTOINC+b576fa87c1

  RECIPE NAME: gnu-config

  LICENSE: GPL-3.0-with-autoconf-exception
- PACKAGE NAME: grep

  PACKAGE VERSION: 2.23

  RECIPE NAME: grep

  LICENSE: GPLv3
- PACKAGE NAME: inetutils-telnetd

  PACKAGE VERSION: 1.9.4

  RECIPE NAME: inetutils

  LICENSE: GPLv3
- PACKAGE NAME: initscripts

  PACKAGE VERSION: 1.0

  RECIPE NAME: initscripts

  LICENSE: GPLv2
- PACKAGE NAME: initscripts-microsemi

  PACKAGE VERSION: 1.0

  RECIPE NAME: initscripts-microsemi

  LICENSE: BSD
- PACKAGE NAME: ipdynaddrd

  PACKAGE VERSION: 1.1

  RECIPE NAME: ipdynaddrd

  LICENSE: BSD
- PACKAGE NAME: iperf

  PACKAGE VERSION: 2.0.5

  RECIPE NAME: iperf

  LICENSE: BSD-2-Clause
- PACKAGE NAME: iproute2

  PACKAGE VERSION: 4.4.0

  RECIPE NAME: iproute2

  LICENSE: GPLv2+
- PACKAGE NAME: iptables

  PACKAGE VERSION: 1.6.0

  RECIPE NAME: iptables

  LICENSE: GPLv2+
- PACKAGE NAME: iputils

  PACKAGE VERSION: s20151218

  RECIPE NAME: iputils

LICENSE: BSD GPLv2+
- PACKAGE NAME: kbd

  PACKAGE VERSION: 2.0.3

  RECIPE NAME: kbd

  LICENSE: GPLv2+
- PACKAGE NAME: kernel

  PACKAGE VERSION: 4.1.22+git999

  LICENSE: GPLv2
- PACKAGE NAME: kmod

  PACKAGE VERSION: 22+gitAUTOINC+42f32b8ae4

  RECIPE NAME: kmod

  LICENSE: GPL-2.0+ LGPL-2.1+
- PACKAGE NAME: ldd

  PACKAGE VERSION: 2.23

  RECIPE NAME: glibc

  LICENSE: GPLv2 LGPLv2.1
- PACKAGE NAME: libacl

  PACKAGE VERSION: 2.2.52

  RECIPE NAME: acl

  LICENSE: LGPLv2.1+
- PACKAGE NAME: libattr

  PACKAGE VERSION: 2.4.47

  RECIPE NAME: attr

  LICENSE: LGPLv2.1+ GPLv2+
- PACKAGE NAME: libbz2

  PACKAGE VERSION: 1.0.6

  RECIPE NAME: bzip2

  LICENSE: bzip2
- PACKAGE NAME: libcap

  PACKAGE VERSION: 2.24

  RECIPE NAME: libcap

  LICENSE: BSD GPLv2
- PACKAGE NAME: libcomerr

  PACKAGE VERSION: 1.42.99+1.43+gitAUTOINC+0f26747167

  RECIPE NAME: e2fsprogs

  LICENSE: GPLv2 LGPLv2 BSD MIT
- PACKAGE NAME: libcrypto

  PACKAGE VERSION: 1.0.2h

  RECIPE NAME: openssl

  LICENSE: openssl
- PACKAGE NAME: libdw

  PACKAGE VERSION: 0.164

RECIPE NAME: elfutils

LICENSE: GPL-2+ Elfutils-Exception

- PACKAGE NAME: libe2p2

  PACKAGE VERSION: 1.42.99+1.43+gitAUTOINC+0f26747167

  RECIPE NAME: e2fsprogs

  LICENSE: GPLv2 LGPLv2 BSD MIT
- PACKAGE NAME: libelf

  PACKAGE VERSION: 0.164

  RECIPE NAME: elfutils

  LICENSE: GPL-3+ Elfutils-Exception
- PACKAGE NAME: libevent

  PACKAGE VERSION: 2.0.22

  RECIPE NAME: libevent

  LICENSE: BSD
- PACKAGE NAME: libext2fs2

  PACKAGE VERSION: 1.42.99+1.43+gitAUTOINC+0f26747167

  RECIPE NAME: e2fsprogs

  LICENSE: GPLv2 LGPLv2 BSD MIT
- PACKAGE NAME: libffi

  PACKAGE VERSION: 3.2.1

  RECIPE NAME: libffi

  LICENSE: MIT
- PACKAGE NAME: libgcc

  PACKAGE VERSION: linaro-5.2

  RECIPE NAME: libgcc

  LICENSE: GPL-3.0-with-GCC-exception
- PACKAGE NAME: libgcrypt

  PACKAGE VERSION: 1.6.5

  RECIPE NAME: libgcrypt

  LICENSE: LGPLv2.1+
- PACKAGE NAME: libgpg-error

  PACKAGE VERSION: 1.21

  RECIPE NAME: libgpg-error

  LICENSE: GPLv2+ LGPLv2.1+
- PACKAGE NAME: libidn

  PACKAGE VERSION: 1.32

  RECIPE NAME: libidn

  LICENSE: (LGPLv2.1+ | LGPLv3) & GPLv3+
- PACKAGE NAME: libkmod

  PACKAGE VERSION: 22+gitAUTOINC+42f32b8ae4

  RECIPE NAME: kmod

LICENSE: LGPL-2.1+

- PACKAGE NAME: libltdl

  PACKAGE VERSION: 2.4.6

  RECIPE NAME: libtool

  LICENSE: GPLv2 LGPLv2.1
- PACKAGE NAME: liblzma

  PACKAGE VERSION: 5.2.2

  RECIPE NAME: xz

  LICENSE: PD
- PACKAGE NAME: libmcrypt

  PACKAGE VERSION: 2.5.8

  RECIPE NAME: libmcrypt

  LICENSE: LGPLv2.1
- PACKAGE NAME: libmnl

  PACKAGE VERSION: 1.0.3

  RECIPE NAME: libmnl

  LICENSE: LGPLv2.1+
- PACKAGE NAME: libmysqlclient

  PACKAGE VERSION: 5.5.52

  RECIPE NAME: mariadb

  LICENSE: GPLv2
- PACKAGE NAME: libnetfilter-conntrack

  PACKAGE VERSION: 1.0.2

  RECIPE NAME: libnetfilter-conntrack

  LICENSE: GPLv2+
- PACKAGE NAME: libnetfilter-cthelper

  PACKAGE VERSION: 1.0.0

  RECIPE NAME: libnetfilter-cthelper

  LICENSE: GPLv2+
- PACKAGE NAME: libnetfilter-cttimeout

  PACKAGE VERSION: 1.0.0

  RECIPE NAME: libnetfilter-cttimeout

  LICENSE: GPLv2+
- PACKAGE NAME: libnetfilter-queue

  PACKAGE VERSION: 1.0.2

  RECIPE NAME: libnetfilter-queue

  LICENSE: GPLv2+
- PACKAGE NAME: libnfnetlink

  PACKAGE VERSION: 1.0.1

  RECIPE NAME: libnfnetlink

  LICENSE: GPLv2+
- PACKAGE NAME: libnfsidmap

PACKAGE VERSION: 0.25

RECIPE NAME: libnfsidmap

LICENSE: BSD

- PACKAGE NAME: libpam

  PACKAGE VERSION: 1.2.1

  RECIPE NAME: libpam

  LICENSE: GPLv2+ BSD
- PACKAGE NAME: libpcap

  PACKAGE VERSION: 1.7.4

  RECIPE NAME: libpcap

  LICENSE: BSD
- PACKAGE NAME: libpci

  PACKAGE VERSION: 3.4.1

  RECIPE NAME: pciutils

  LICENSE: GPLv2+
- PACKAGE NAME: libpcre

  PACKAGE VERSION: 8.38

  RECIPE NAME: libpcre

  LICENSE: BSD
- PACKAGE NAME: libpq

  PACKAGE VERSION: 9.2.4

  RECIPE NAME: postgresql

  LICENSE: BSD
- PACKAGE NAME:libpython2

  PACKAGE VERSION: 2.7.11

  RECIPE NAME: python

  LICENSE: PSFv2
- PACKAGE NAME: libsqlite3

  PACKAGE VERSION: 3.13.0

  RECIPE NAME: sqlite3

  LICENSE: PD
- PACKAGE NAME: libss

  PACKAGE VERSION: 1.42.99+1.43+gitAUTOINC+0f26747167

  RECIPE NAME: e2fsprogs

  LICENSE: GPLv2 LGPLv2 BSD MIT
- PACKAGE NAME: libssl

  PACKAGE VERSION: 1.0.2h

  RECIPE NAME: openssl

  LICENSE: openssl
- PACKAGE NAME: libstdc++

  PACKAGE VERSION: linaro-5.2

RECIPE NAME: gcc-runtime

LICENSE: GPL-3.0-with-GCC-exception

- PACKAGE NAME: libsysfs

  PACKAGE VERSION: 2.1.0

  RECIPE NAME: sysfsutils

  LICENSE: LGPLv2.1
- PACKAGE NAME: libsystemd

  PACKAGE VERSION: 229+gitAUTOINC+714c62b463

  RECIPE NAME: systemd

  LICENSE: GPLv2 LGPLv2.1 MIT
- PACKAGE NAME: libtirpc

  PACKAGE VERSION: 1.0.1

  RECIPE NAME: libtirpc

  LICENSE: BSD
- PACKAGE NAME: libudev

  PACKAGE VERSION: 229+gitAUTOINC+714c62b463

  RECIPE NAME: systemd

  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: libusb-1

  PACKAGE VERSION: 1.0.20

  RECIPE NAME: libusb1

  LICENSE: LGPLv2.1+
- PACKAGE NAME: libwrap

  PACKAGE VERSION: 7.6

  RECIPE NAME: tcp-wrappers

  LICENSE: BSD
- PACKAGE NAME: libxerces-c

  PACKAGE VERSION: 3.1.1

  RECIPE NAME: xerces-c

  LICENSE: Apache-2.0
- PACKAGE NAME: libxml2

  PACKAGE VERSION: 2.9.4

  RECIPE NAME: libxml2

  LICENSE: MIT
- PACKAGE NAME: logrotate

  PACKAGE VERSION: 3.9.1

  RECIPE NAME: logrotate

  LICENSE: GPLv2
- PACKAGE NAME: ltrace

  PACKAGE VERSION: 7.3+gitAUTOINC+01b10e191e

  RECIPE NAME: ltrace

LICENSE: GPLv2

- PACKAGE NAME: m4

  PACKAGE VERSION: 1.4.17

  RECIPE NAME: m4

  LICENSE: GPLv3
- PACKAGE NAME: make

  PACKAGE VERSION: 4.1

  RECIPE NAME: make

  LICENSE: GPLv3 LGPLv2
- PACKAGE NAME: microsemi-app

  PACKAGE VERSION: 1.0

  RECIPE NAME: microsemi-app

  LICENSE: BSD
- PACKAGE NAME: microsemi-misc

  PACKAGE VERSION: 1.0

  RECIPE NAME: microsemi-misc

  LICENSE: GPLv2
- PACKAGE NAME: minicom

  PACKAGE VERSION: 2.7

  RECIPE NAME: minicom

  LICENSE: GPLv2+
- PACKAGE NAME: msmtp

  PACKAGE VERSION: 1.6.6

  LICENSE: GPL v3
- PACKAGE NAME: mtd-utils

  PACKAGE VERSION: 1.5.2

  RECIPE NAME: mtd-utils

  LICENSE: GPLv2+
- PACKAGE NAME: ncurses

  PACKAGE VERSION: 6.0+20160213

  RECIPE NAME: ncurses

  LICENSE: MIT
- PACKAGE NAME: net-snmp

  PACKAGE VERSION: 5.7.1

  LICENSE: BSD
- PACKAGE NAME: nettle

  PACKAGE VERSION: 3.2

  RECIPE NAME: nettle

  LICENSE: LGPLv3+ | GPLv2+
- PACKAGE NAME: net-tools

  PACKAGE VERSION: 1.60-26

  RECIPE NAME: net-tools

LICENSE: GPLv2+

- PACKAGE NAME: netbase

  PACKAGE VERSION: 5.3

  RECIPE NAME: netbase

  LICENSE: GPLv2
- PACKAGE NAME: network-scripts

  PACKAGE VERSION: 1.0

  RECIPE NAME: network-scripts

  LICENSE: BSD
- PACKAGE NAME: nfs-utils

  PACKAGE VERSION: 1.3.3

  RECIPE NAME: nfs-utils

  LICENSE: MIT GPLv2+ BSD
- PACKAGE NAME: NTP

  PACKAGE VERSION: 4.2.8p14

  LICENSE: BSD like
- PACKAGE NAME: openldap

  PACKAGE VERSION: 2.4.39

  RECIPE NAME: openldap

  LICENSE: OpenLDAP
- PACKAGE NAME: openssh

  PACKAGE VERSION: 7.4p1

  RECIPE NAME: openssh

  LICENSE: BSD
- PACKAGE NAME: openssl

  PACKAGE VERSION: 1.0.2h

  RECIPE NAME: openssl

  LICENSE: openssl
- PACKAGE NAME: oprofile

  PACKAGE VERSION: 1.1.0

  RECIPE NAME: oprofile

  LICENSE: LGPLv2.1+ GPLv2
- PACKAGE NAME: os-release

  PACKAGE VERSION: 1.0

  RECIPE NAME: os-release

  LICENSE: MIT
- PACKAGE NAME: packagegroup-core-boot

  PACKAGE VERSION: 1.0

  RECIPE NAME: packagegroup-core-boot

  LICENSE: MIT
- PACKAGE NAME: pam-plugin

  PACKAGE VERSION: 1.2.1

RECIPE NAME: libpam

LICENSE: GPLv2+ BSD

- PACKAGE NAME: pam_ldap

  PACKAGE VERSION: 186

  LICENSE: GPL v2
- PACKAGE NAME: pam_radius

  PACKAGE VERSION: 1.3.17

  LICENSE: GPL v2
- PACKAGE NAME: pam_tacplus

  PACKAGE VERSION: 1.3.8

  LICENSE: GPL v2
- PACKAGE NAME: parted

  PACKAGE VERSION: 3.2

  RECIPE NAME: parted

  LICENSE: GPLv3+
- PACKAGE NAME: pciutils

  PACKAGE VERSION: 3.4.1

  RECIPE NAME: pciutils

  LICENSE: GPLv2+
- PACKAGE NAME: perl

  PACKAGE VERSION: 5.22.1

  RECIPE NAME: perl

  LICENSE: Artistic-1.0 GPL-1.0
- PACKAGE NAME: php

  PACKAGE VERSION: 5.6.33

  RECIPE NAME: php

  LICENSE: PHP-3.0
- PACKAGE NAME: popt

  PACKAGE VERSION: 1.16

  RECIPE NAME: popt

  LICENSE: MIT
- PACKAGE NAME: portmap

  PACKAGE VERSION: 6.0

  RECIPE NAME: portmap

  LICENSE: BSD
- PACKAGE NAME: postgresql

  PACKAGE VERSION: 9.2.4

  RECIPE NAME: postgresql

  LICENSE: BSD
- PACKAGE NAME: procps

  PACKAGE VERSION: 3.3.11

  RECIPE NAME: procps

LICENSE: GPLv2+ LGPLv2+

- PACKAGE NAME: python-xxx (many)

  PACKAGE VERSION: 2.7.11

  RECIPE NAME: python

  LICENSE: PSFv2
- PACKAGE NAME:readline

  PACKAGE VERSION: 6.3

  RECIPE NAME: readline

  LICENSE: GPLv3+
- PACKAGE NAME: rpcbind

  PACKAGE VERSION: 0.2.3

  RECIPE NAME: rpcbind

  LICENSE: BSD
- PACKAGE NAME: run-postinsts

  PACKAGE VERSION: 1.0

  RECIPE NAME: run-postinsts

  LICENSE: MIT
- PACKAGE NAME: rwi-mod

  PACKAGE VERSION: 0.1

  RECIPE NAME: rwi-mod

  LICENSE: GPLv2
- PACKAGE NAME: sed

  PACKAGE VERSION: 4.2.2

  RECIPE NAME: sed

  LICENSE: GPLv3+
- PACKAGE NAME: setserial

  PACKAGE VERSION: 2.17

  RECIPE NAME: setserial

  LICENSE: GPLv2.0
- PACKAGE NAME: shadow

  PACKAGE VERSION: 4.2.1

  RECIPE NAME: shadow

  LICENSE: BSD Artistic-1.0
- PACKAGE NAME: sipcalc

  PACKAGE VERSION: 1.1.6

  RECIPE NAME: sipcalc

  LICENSE: BSD
- PACKAGE NAME: smarty

  PACKAGE VERSION: 3.1.17

  RECIPE NAME: smarty

  LICENSE: GPL
- PACKAGE NAME: sqlite3

PACKAGE VERSION: 3.13.0

RECIPE NAME: sqlite3

LICENSE: PD

- PACKAGE NAME: sshfs-fuse

  PACKAGE VERSION: 2.5

  RECIPE NAME: sshfs-fuse

  LICENSE: GPLv2
- PACKAGE NAME: strace

  PACKAGE VERSION: 4.11

  RECIPE NAME: strace

  LICENSE: BSD
- PACKAGE NAME: sudo

  PACKAGE VERSION: 1.8.15

  RECIPE NAME: sudo

  LICENSE: ISC BSD Zlib
- PACKAGE NAME: sysfsutils

  PACKAGE VERSION: 2.1.0

  RECIPE NAME: sysfsutils

  LICENSE: GPLv2
- PACKAGE NAME: sysklogd

  PACKAGE VERSION: 1.5.1

  RECIPE NAME: sysklogd

  LICENSE: GPLv2+ BSD
- PACKAGE NAME: systemd

  PACKAGE VERSION: 229+gitAUTOINC+714c62b463

  RECIPE NAME: systemd

  LICENSE: GPLv2 LGPLv2.1 MIT
- PACKAGE NAME: systemd-compat-units

  PACKAGE VERSION: 1.0

  RECIPE NAME: systemd-compat-units

  LICENSE: MIT
- PACKAGE NAME: systemd-serialgetty

  PACKAGE VERSION: 1.0

  RECIPE NAME: systemd-serialgetty

  LICENSE: GPLv2+
- PACKAGE NAME: tar

  PACKAGE VERSION: 1.28

  RECIPE NAME: tar

  LICENSE: GPLv3
- PACKAGE NAME: tcl

  PACKAGE VERSION: 8.6.4

RECIPE NAME: tcl

LICENSE: BSD-3-Clause

- PACKAGE NAME: tcpdump

  PACKAGE VERSION: 4.6.1

  RECIPE NAME: tcpdump

  LICENSE: BSD
- PACKAGE NAME: tzcode

  PACKAGE VERSION: 2.2.3

  RECIPE NAME: tzcode

  LICENSE: PD BSD
- PACKAGE NAME: tzdata

  PACKAGE VERSION: 2019c

  RECIPE NAME: tzdata

  LICENSE: PD BSD
- PACKAGE NAME: udev

  PACKAGE VERSION: 229+gitAUTOINC+714c62b463

  RECIPE NAME: systemd

  LICENSE: GPLv2 LGPLv2.1 MIT
- PACKAGE NAME: update-alternatives-opkg

  PACKAGE VERSION: 0.1.8+gitAUTOINC+53274f0875

  RECIPE NAME: opkg-utils

  LICENSE: GPLv2+
- PACKAGE NAME: update-rc.d

  PACKAGE VERSION: 0.7

  RECIPE NAME: update-rc.d

  LICENSE: GPLv2+
- PACKAGE NAME: usbutils

  PACKAGE VERSION: 008

  RECIPE NAME: usbutils

  LICENSE: GPLv2+
- PACKAGE NAME: util-linux

  PACKAGE VERSION: 2.27.1

  RECIPE NAME: util-linux

  LICENSE: GPLv2+ LGPLv2.1+ BSD
- PACKAGE NAME: valgrind

  PACKAGE VERSION: 3.11.0

  RECIPE NAME: valgrind

  LICENSE: GPLv2 GPLv2+ BSD
- PACKAGE NAME: volatile-binds

  PACKAGE VERSION: 1.0

  RECIPE NAME: volatile-binds

LICENSE: MIT

- PACKAGE NAME: wget

  PACKAGE VERSION: 1.20.3

  RECIPE NAME: wget

  LICENSE: GPLv3
- PACKAGE NAME: xerces-c

  PACKAGE VERSION: 3.1.1

  RECIPE NAME: xerces-c

  LICENSE: Apache-2.0
- PACKAGE NAME: xinetd

  PACKAGE VERSION: 2.3.15

  RECIPE NAME: xinetd

  LICENSE: BSD
- PACKAGE NAME: yp-tools

  PACKAGE VERSION: 2.14

  RECIPE NAME: yp-tools

  LICENSE: GPL-2.0
- PACKAGE NAME: ypbind-mt

  PACKAGE VERSION: 1.38

  RECIPE NAME: ypbind-mt

  LICENSE: GPL-2.0
- PACKAGE NAME: zlib

  PACKAGE VERSION: 1.2.8

  RECIPE NAME: zlib

  LICENSE: Zlib

12. Port Details

12.1 Ethernet Port Electrical

By design, the SyncServer network ports are galvanically isolated.

12.2 Ethernet Port Isolation

The SyncServer S600 Series Network Time Servers have four Ethernet ports. These independent ports allow the SyncServer to connect to distinct Ethernet subnets. There is only one CPU in the SyncServer, so all of the Ethernet traffic, with the exception of the NTP Reflector and PTP server traffic, is ultimately handled by the protocol stack of the operating system.

The SyncServer uses the operating system IP packet filtering facilities to secure the SyncServer from unwanted access. The SyncServer also creates rules to filter IP packets based on the pre-assigned role of each Ethernet port. The SyncServer assigns different roles to the Ethernet ports. The LAN1 port serves the distinction of being the management port. The other ports serve as timing ports only. Each role is defined as the set of supported protocols allowed for that Ethernet port. By default, the SyncServer is configured to reject all TCP/UDP IP packets.

12.3 Management Port Rules

The management port allows the following types of IP packets:

- HTTP: inbound and outbound TCP packets on port 80
- HTTPS: inbound and outbound TCP packets on port 443
- SNMP: inbound and outbound UDP packets on port 161
- SSH: inbound and outbound packets TCP on port 22
- NTP: inbound and outbound UDP packets on port 123

The management port uses the following types of IP packets, but the ports do not show as open on a port scanner:

- Telnet: inbound packets TCP on port 23 (if telnet is enabled)
- SMTP: inbound and outbound TCP packets on port 25
- DNS: inbound and outbound UDP and TCP packets on port 53
- DHCP: inbound and outbound UDP packets on port 67 and 68
- SNMPTRAP: inbound and outbound UDP packets on port 162
- syslog: outbound UDP packets on port 514
- RADIUS: inbound and outbound UDP packets, outbound on port 1812 or 1645
- TACACS+: inbound and outbound TCP/UDP packets, outbound on port 49
- LDAP: inbound and outbound TCP/UDP packets, outbound on port 389

Note that the rules allow inbound packets only, outbound packets that are part of the session are allowed to go out of the port.

12.4 Timing Port Rules

The three timing ports allow the following types of IP packets.

- NTP: inbound and outbound UDP packets on port 123
- PTP: inbound and outbound UDP packets on ports 319 and 320

The timing ports use the following types of IP packets, but the ports do not show as open on a port scanner:

- DHCP: inbound and outbound UDP packets on port 67 and 68

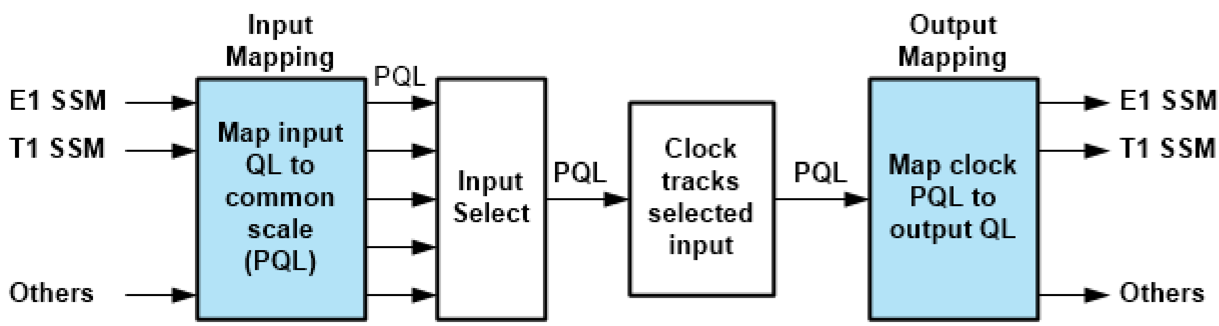
13. PQL Mapping

13.1 Purpose of Input and Output Mapping Tables

When the SyncServer S6x0 has 1 or 2 Timing I/O Modules with Telecom I/O Connections (090-15201-011) the topic of Synchronization Status Messaging (SSM) becomes relevant. In this context, SSM provides a frequency quality measure that can be passed between equipment to identify “how good” the frequency “on the wire” is. E1 and T1 frequency references have a long history of support for SSM, but since they don't use the same quality scales a mechanism is needed to merge the scales to allow inter-operability of these signal types. The telecom module supports E1 and T1 input (J7 connection) as well as E1 and T1 output (J7 and J8 connections), so the inter-operability case is possible. For example, J7 can be configured to use an SSM-capable T1 as input frequency reference while J8 is providing an SSM-capable E1 output. This section addresses the question that arises in these cases: what is the input-to-output mapping of SSM? The following image shows the overall end-to-end process.

Reference inputs may use different scales for quality level. At the input, these different scales of quality level are mapped to a common scale called PQL (priority quality level). The PQL scale is a number from 1 to 16, with 1 being the highest quality and 16 being the lowest. Once all input quality levels are mapped to PQL, internal processing will only use PQL as the quality indicator. See PQL Input Mapping for PQL mapping of frequency inputs.

Figure 13-1. PQL Input and Output Mapping



13.1.1 E1 and T1 Signals That Embed SSM

For E1 configurations, they all support embedded SSM except for these: CAS or CCS frame types with CRC state disabled, 2.048 MHz SquareWave.

For T1 configurations, only the ESF frame type supports embedded SSM.

For the cases when one of these SSM-capable signals is configured as a frequency input to the S6xx, the SSM content will be expected and processed as described here. Note that T1 and E1 inputs can only be configured on J7 connection. As with all system references, to use any input it must be enabled on the Timing > Input Control form.

Figure 13-2. Enabling J7 Telecom Input

Here's a summary of how SSM-capable inputs are processed:

1. The SSM value is extracted from the input.
   If it is an E1 signal, the legal SSM encodings are shown in left column of Table 13-4. Each of these have a mapping to an internal-use-only PQL value, shown in the rightmost column. For example if 0x4 is decoded on the input, it will result in PQL = 6. As will be seen, the purpose of PQL is to provide a common scale for merging E1 and T1 signals onto a single quality comparison scale. PQL never actually appears on any signals, it is an internal comparison scale.

   If the input is a T1 ESF-framed signal, the legal SSM encodings are shown in the left column of Table 13-5. The legal SSM encodings are shown in the left column and associated PQL value in rightmost column.

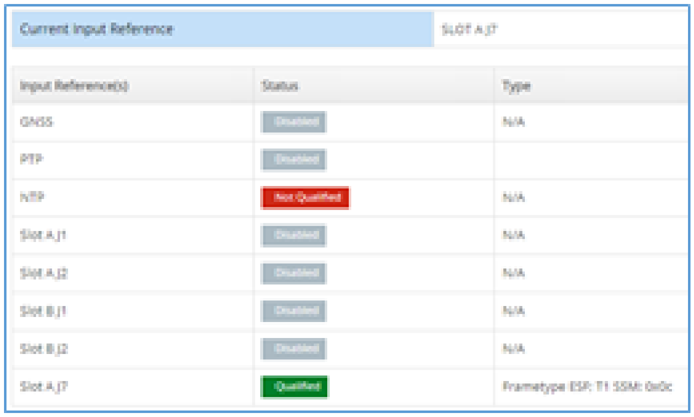
   For any of these signals, if an illegal SSM code is read (anything not in the associated table) then the input will not be qualified for use (it would remain in red on Dashboard > Timing, Frequency References row).
2. Assuming an SSM code is actually being read from the input, that value is shown on the References > Status form. Look for the row labeled Slot A J7 (or Slot B J7), the Type column will summarize the input signal configuration and show the SSM value. If J7 has been configured as an output that will also be shown here to help with troubleshooting.
   Using the mapping to PQL covered in step 1, this value is compared with a PQL value that is assigned to the internal reference oscillator in this S6xx. These assignments are shown in Table 13-1. The type of oscillator in the unit can be observed on Help > About. Using the PQL mapping of the input and the appropriate value from 13-1 a very simple decision is made: If the input PQL is a larger number than the internal oscillator PQL then the input will NOT be used (the larger the PQL, the worse the frequency performance). The purpose of this comparison test and possible rejection of the input is based the following basic concepts:

   – The reference oscillator in the S6xx is also a frequency reference, it just happens to be embedded inside the product.
   – If the candidate externally-supplied frequency reference (the signal with the embedded SSM information) is indicating worse quality than the quality of S6xx internal reference, then it is better to just use the internal reference and reject the candidate reference.
   If the candidate input is rejected due to failure of this comparison test, it will remain red on Dashboard > Timing frequency references row, indicating that it is not qualified for use.

   Keep in mind that the input SSM is continually being read, so if the SSM value from the candidate improves, this reference could become qualified. The process is dynamic.
3. Assuming the candidate reference is not rejected by the prior step, then it can become qualified (it will be shown in green on Dashboard > Timing frequency references row). For simplicity of this explanation, assume that the T1 or E1 SSM-capable reference is the only external candidate reference being provided. In this case, it will not only be qualified for use (meaning that it could be selected from the pool of qualified candidates), it will actually be selected as the frequency reference for the S6xx.
4. To follow the complete SSM input-to-output path we'll use an example. In this case the unit has a telecom module in Slot A which has been configured as a reference input, specifically a T1 ESF-framed signal. A valid T1 ESF signal is provided containing a known SSM value (taken from another Microchip product).

From the References > Status form (shown below) we can see the configuration of the J7 input as well as the current SSM value that is being read: 0x0C. Using table 13-5 (used for T1 SSM inputs) we find that 0x0C maps to PQL = 4. This form also shows at the top that J7 connection is the current input reference for this S650. This means that the PQL=4 value is sourcing SSM for any T1 and E1 outputs that might be configured.

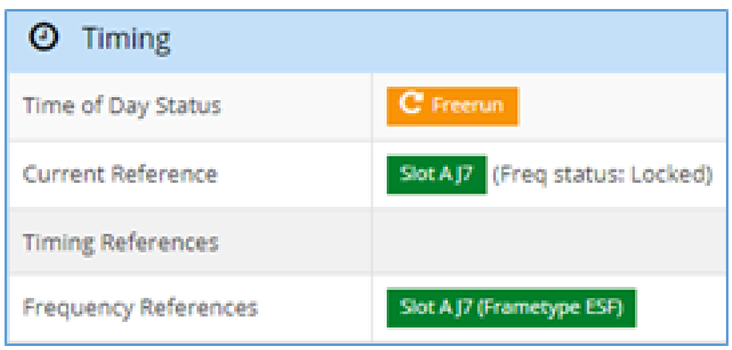
Figure 13-3. SSM input values shown in Type column on References ' Status form



- The form will not self-update this status. To ensure that current value is being shown, refresh the form.
- The format of the SSM values is not correctly shown, but the content is correct. Ignore the trailing “FF” for E1 values.

Another view of the overall system status can be seen on Dashboard > System Timing. The Current Reference row shows that the input at AJ7 is the selected reference for the system. It also shows that the system is frequency locked. Note that since there is no time-reference into the system, the Time of Day Status remains in freerun.

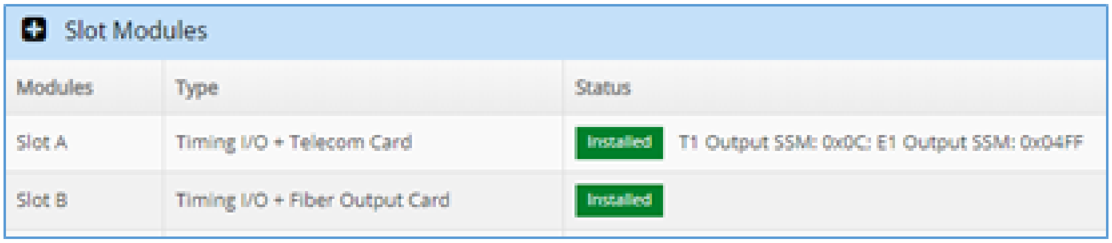
Figure 13-4. S6xx Frequency Locked to T1 ESF Input on Slot A J7



We can use Tables 13-6 and 13-7 to identify the SSM values that will be encoded onto E1 or T1 outputs (if they are capable of encoding SSM). Since we already identified that the PQL level of the current reference is 4, then we just look up the corresponding output SSM for each signal type. Table 13-6 shows that a PQL of 4 maps to output E1 SSM of 0x4 (it is SSM that will be encoded on any SSM-capable E1 output). Similarly, Table 13-7 shows the mapping for a T1 ESF signal. The PQL of 4 maps to SSM of 0x0CFF.

The S6xx performs this conversion automatically and displays these values on the Dashboard > Slot Modules form. As shown, whenever the S6xx contains a telecom module, the T1 and E1 current output SSM values will always be shown here, even if there are currently no actual outputs of this type being generated. As can be seen, the values match what was determined from the tables (note the T1 should have the appended “FF”, not the E1 on the form shown, but the actual outputs will be encoded correctly).

Figure 13-5. Dashboard > Slot Modules always shows T1 and E1 output SSM encodings

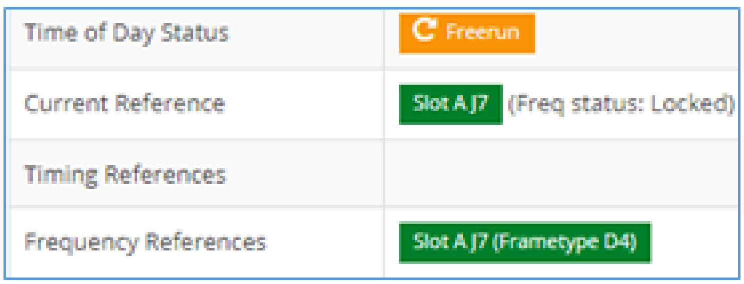


13.1.2 Frequency References That Don't Provide SSM

The prior section covered SSM processing for input frequency reference configurations that are SSM capable. All other frequency inputs on S6xx are not SSM-capable, so there is nothing to decode. However, since it is always possible to have SSM-capable outputs (regardless of selected input reference) there must be an input-to-output mapping process for these cases.

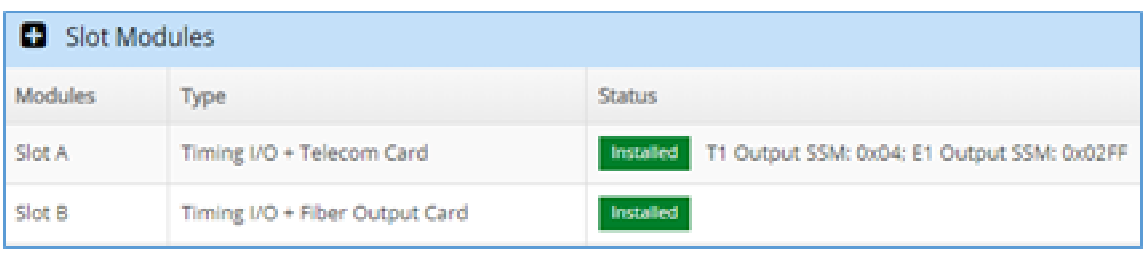
This category is handled just the same as the prior section except, for these non-SSM inputs, the PQL value is always assigned the value 1, which is equivalent to saying this is the best possible frequency quality. From there the mapping process is identical. Here's an example where the J7 input has been changed to T1 frametype D4, which is NOT SSM capable and therefore PQL is assigned the value 1.

Figure 13-6. Using a non-SSM capable input PQL is always assigned value of 1



Use tables F-6 and F-7 to see the values that will be encoded onto SSM-capable outputs. From F-6 (E1 encodings) it is seen that PQL = 1 will encode SSM 0x2. From F-7 (T1 encodings) it is seen that PQL = 1 will encode SSM 0x04FF.

As always, this information is provided on the Dashboard > Slot Modules form, in the row associated with the telecom module (note the T1 should have the appended “FF”, not the E1 on the form shown, but the actual outputs will be encoded correctly).



The current set of frequency inputs that are NOT capable of encoding SSM include:

- Any E1 signal with CRC disabled, E1 2.048 MHz
- T1 framed D4, T1 1.544 MHz
- Frequency inputs on J2 (1 MHz, 5 MHz, 10 MHz)
- Frequency inputs on J1 (1PPS, 10MPPS)

Any of these, when selected as the system frequency reference will set PQL = 1.

13.1.3 Selection of Frequency References

The selection of which frequency reference to use in a situation where there are multiple candidates is fundamentally unchanged by the addition of SSM-capable input references. Here are the key points:

- Use the priority control (see Timing > Input Control, Frequency Reference Priority group) to define the preferred order of frequency input selection. When there are multiple qualified candidates the one with highest priority will be selected.
- While the SSM value for use on T1 or E1 outputs (that can encode SSM) will be based on the PQL of the selected frequency reference (process covered in prior sections), the PQL is not used to modify the selection criteria for frequency inputs. In other words, if the PQL of a higher priority reference is worse than the PQL of a lower priority reference, it will not affect the selection decision: the highest priority qualified reference always gets selected.
- The one situation where SSM can impact frequency reference selection is if the decoded SSM maps to a PQL that is worse than the static PQL of the internal reference. When that occurs, the reference become disqualified and therefore can't be selected (regardless of its priority).

Table 13-1. Oscillator PQL Values

OSCILLATOR	PQL
Rubidium	4
OCXO	6
Standard	12

13.1.4 Quality Levels Defined by ITU-T

The mapping between PQL and various frequency synchronization quality level scales conforms to the frequency synchronization quality levels defined in ITU-T G.781 (for SSM) and ITU-T G.8265.1 (SSM).

G.781 defines five valid QL and SSM values for Option I network (2048 kbps hierarchy), as shown in Table 13-2.

Table 13-2. G.781 QL and SSM values for Option I Network (2048 kbps hierarchy)

QL	SSM	Clock Quality Definition
PRC	0x2	G.811
SSU-A	0x4	G.812 type I or V
SSU-B	0x8	G.812 type VI
SEC	0xB	G.813, or G.8262 option I
DNU	0xF	Should not be used for synchronization

G.781 defines nine valid QL and SSM values for Option II network (1544 kbps hierarchy), as shown in Table 13-3.

Table 13-3. G.781 QL and SSM values for Option II Network (1544 kbps hierarchy)

QL	SSM	Clock Quality Definition
PRS	04FF	G.811
STU	08FF	Synchronized - traceability unknown
ST2	0CFF	G.812 type II
TNC	78FF	G.812 type V
ST3E	7CFF	G.812 type III
ST3	10FF	G.812 type IV
SMC	22FF	G.813, or G.8262 option I
PROV	40FF	Provisionable by network operator
DUS	30FF	Should not be used for synchronization

13.2 PQL Input Mapping

Table 13--4 shows PQL values converted from SSM for Option I Network frequency references. Table 13-5 shows PQL values converted from SSM for Option II Network frequency references.

Table 13-1 shows PQL values associated with clock types for rubidium and quartz oscillators. Table 13-8 shows PQL values associated with various clock states for rubidium and quartz oscillators.

Table 13-4. PQL Input Mapping for Option I Network - Converted from SSM

Input E1 SSM	Input QL	To Input PQL
0x2	QL-PRC	3
0x4	QL-SSU-A	6
0x8	QL-SSU-B	9
0xB	QL-SEC/EEC1	13
0xF invalid_SSM	QL-DNU	16

Table 13-5. PQL Input Mapping for Option II Network - Converted from SSM

Input T1 SSM	Input QL	To Input PQL
04FF	QL-PRS	1
08FF	QL-STU	2
0CFF	QL-ST2	4
78FF	QL-TNC	6
7CFF	QL-ST3E	11
10FF	QL-ST3	12
22FF	QL-SMC/EEC2	14
40FF	QL-PROV	15
30FF invalid SSM	QL-DUS	16

13.3 PQL Output Mapping

Output signal quality level is determined by the quality level of the internal clock. When the internal clock is tracking a reference, the quality level (PQL value) of the internal clock is the PQL of the selected reference. At the outputs, the frequency PQL is converted to the appropriate quality levels for different output signal types, as shown in Figure 13-1. See Table 13-6 below for PQL output mapping for Option I networks. See Table 13-7 below for PQL output mapping for Option II networks.

When the internal clock is not tracking a reference, the quality level of the internal clock is determined by its clock state and its oscillator quality. Table 13-8 shows the internal clock quality level for different oscillator types and clock states.

Table 13-6. PQL Output Mapping for Option I Network - Converted to SSM

From Output PQL	Output E1 SSM	Output QL
1	0x2	QL-PRC
2		
3		
4	0x4	QL-SSU-A
5		
6		
7	0x8	QL-SSU-B
8		
9		
10		
11		
12	0xB	QL-SEC/EEC1
13		
14		
15	0xF	QL-DNU
16		

Table 13-7. PQL Output Mapping for Option II Network - Converted to SSM

From Output PQL	Output T1 SSM	Output QL
1	04FF	QL-PRS
2	08FF	QL-STU
3	04FF	QL-PRS
4	0CFF	QL-ST2
5	78FF	QL-TNC
6		
7	7CFF	QL-ST3E
8		
9		
10		
11		
12	10FF	QL-ST3
13	22FF	QL-SMC/EEC2
14		
15	40FF	QL-PROV

...........continued

From Output PQL	Output T1 SSM	Output QL
16	30FF invalid SSM	QL-DUS

Table 13-8. PQL Values for Clock States

CLOCK STATE	Rb	OCXO	Standard
Warmup	16	16	16
Freerun	4	6	12
Locking	4	6	12
Locked	Freq PQL for Selected Ref.	Freq PQL for Selected Ref.	Freq PQL for Selected Ref.
Bridging	Freq PQL for Selected Ref.	Freq PQL for Selected Ref.	Freq PQL for Selected Ref.
Holdover	4	6	12
Extended Holdover	4	6	12
Relocking	4	6	12

14. Configuring Remote Auth Servers in the SyncServer S600/S650

14.1 Install and configure RADIUS server

Microchip uses the widely available open source RADIUS server software FreeRADIUS. The FreeRADIUS binaries exist for different platforms. This note describes how to download, build and install the FreeRADIUS server from source on a 64bit Ubuntu 14.04/16.04. The instructions are the same for both Ubuntu 14.04/16.04.

14.1.1 Download FreeRADIUS

Use the http://freeradius.org/releases/ to download the latest stable release source. As of this writing, the stable version is 3.0.15.

14.1.2 Download and Install 'talloc'

The FreeRADIUS has a dependency on the talloc package which is not installed on either Ubuntu 14.04 or Ubuntu 16.04. In fact, apt-get install fails to find the talloc package. Use https://www.samba.org/ftp/talloc/ to download talloc source code. As of this writing, the 2.1.10 release is the latest.

```
tar xfz talloc-2.1.10.tar.gz
cd talloc-2.1.10
./configure
make
sudo make install
```

14.1.3 Install FreeRADIUS

```
tar xfz freeradius-server-3.0.15.tar.gz
cd freeradius-server-3.0.15
./configure
make
sudo make install
```

14.1.4 Configure FreeRADIUS

The configuration files are under /usr/local/etc/raddb directory. You want to 'su' to be 'root' before making edits since all the files and directories under /usr/local/etc/raddb are owned by 'root'.

```
su -
cd /usr/local/etc/raddb
```

Note that we assume you enabled 'root' on the Ubuntu installation. If not, you want to add 'sudo' to commands you run that requires 'root' privilege.

14.1.4.1 Run FreeRADIUS with OpenSSL vulnerability

By default, the FreeRADIUS exits immediately if the OpenSSL it uses has known vulnerabilities. For our testing purposes, we want to disable this check. Open the radiusd.conf. Search for the security section, starting with

```
security {
......
}
```

Comment out the line 'allow_vulnerable_openssl = no' (before the '}') and add a line below that line 'allow_vulnerable_openssl = yes'

```
    #allow_vulnerable_openssl = no
    allow_vulnerable_openssl = yes
```

14.1.4.2 Configure clients

Open clients.conf, at the top of file immediately below the comment line “Define RADIUS clients (usually a NAS, Access Point, etc.).”, add

```
client k2 {
        ipaddr = *
        proto = *
        secret = myk2secret
}
```

Note that 'ipaddr = *' is to allow any RADIUS client (IPv4 or IPv6) to be authenticated. You can use individual IPs or subnets to restrict the clients the server is going to authenticate. The secret 'myk2secret' is to be configured on the SyncServer's RADIUS page and they must match.

14.1.4.3 Configure listening on legacy port 1645

Open sites-enabled/default, after the 'listen { …… }' section, add

```
listen {
        type = auth
        ipaddr = *
        port = 1645
        limit {
              max_connections = 16
              lifetime = 0
              idle_timeout = 30
        }
}
```

14.1.4.4 Configure users

Open mods-config/files/authorize, below the top comment section, add

```
admin Cleartext-Password := "myrad-passwd"
testk2user01 Cleartext-Password := "mscck2userpass01"
```

You have added two users 'admin' and 'testk2user01' to the RADIUS server.

14.1.4.5 Run the RADIUS server

If you are now 'su' as the 'root', enter

```
# radiusd
```

Otherwise, enter

```
% sudo radiusd
```

On the console, you can watch all the RADIUS client requests and server responses information.

14.1.4.6 Run the RADIUS server in debug

```
# radiusd -X
```

or

```
% sudo radiusd -X
```

14.1.5 Configure RADIUS server on the SyncServer

On the SyncServer Security -> RADIUS page, enter

```
RADIUS Server IP Address = IP of the RADIUS server
Secret Key               = myk2secret
Timeout                  = 5
```

Now, you can login to the SyncServer with both 'admin' or 'testk2user01'.

Login as RADIUS 'admin' user

```
Username = admin
Password = myrad-passwd
```

Login as RADIUS 'testk2user01' user

```
Username = testk2user01
Password = mscck2userpass01
```

Note that you can still login as the SYncServer local 'admin' user

```
Username = admin
Password = Microsemi
```

In this case, the RADIUS server authentication fails to authenticate the 'admin' user but the Linux pam continues with the local user authentication using /etc/passwd, which is successful.

14.1.6 Note on pam_radius_auth module password hash

For products using the pam module pam_radius_auth.so (used in the SyncServer S600) to communicate with the RADIUS server, the module applies a MD5 hash with xor algorithm on the user password and puts the hashed result in the packet payload. The module does not support any challenge response type protocol such as MSChap. The pam_radius_auth author Alan DeKok welcomes anyone to add these additional protocol support to the pam_radius_auth package.

14.2 Install and configure Tacplus server

We use the widely available open source TACACS+ server software tac_plus. We describe how to download and configure the tac_plus server on a 64bit Ubuntu 14.04/16.04.

14.2.1 Download and install tac_plus server

```
sudo apt-get install tacacs+
```

14.2.2 Verify the tac_plus server running

```
ps -ef | grep tac_plus
```

It shows “...... 00:00:00 /usr/sbin/tac_plus -C /etc/tacacs+/tac_plus.conf”

14.2.3 Tac_plus server man pages

The tac_plus.conf man page is at http://manpages.ubuntu.com/manpages/bionic/man5/tac_plus.conf.5.html

The tac_plus daemon man page is at http://manpages.ubuntu.com/manpages/bionic/man8/tac_plus.8.html

14.2.4 Configure tac_plus

The configuration files are under /etc/tacacs+. You want to 'su' to be 'root' before making edits since the file is owned by 'root'.

```
su -
cd /etc/tacacs+
```

Note that we assume you enabled 'root' on the Ubuntu installation. If not, you want to add 'sudo' to commands you run that requires 'root' privilege.

14.2.4.1 Configure key

Below the comment line: “This is the key that clients have to user to access Tacacs+”, edit the key to match the key defined in the SyncServer TACACS+ “Secret Key”. Here we change the key to be “k2testing0123456789”.

```
#key = testing123
key = k2testing0123456789
```

14.2.4.2 Configure users

14.2.4.2.1 Default user authentication

The tac_plus allows you to use the local users available on the Linux PC running tac_plus server for remote authentication. This is kind of convenient since you can quickly add a test user to the Linux PC to immediately test TACACS+ remote authentication.

To enable local users for TACACS+ remote authentication, uncomment the line

```
#default authentication = file /etc/passwd
```

to be

```
default authentication = file /etc/passwd
```

14.2.4.2.2 Add users to the tac_plus.conf

To add a new TACACS+ user (not Linux user) with clear text password.

```
# password is "k2pw_TEST"
user = k2testuser {
        name = "K2 Test User"
        pap = cleartext "k2pw_TEST"
}
```

In order to add a new TACACS+ user with encrypted password, you need to run the command 'tac_pwd'. This command takes a password as input and outputs the DES (by default) or MD5 (-m) encryption of the input.

```
tac_pwd
Enter: HardPassword
Output: oTdl1euJ96jLc
# password is "HardPassword"
user = a_k2tacuser {
        name = "Another K2 TACACS+ user"
        pap = des "oTdl1euJ96jLc"
}
```

14.2.4.3 Restart the tac_plus server

sudo /etc/init.d/tac_plus restart

14.2.4.4 Run the tac_plus server in debug

Run the tac_plus in foreground enable debug

```
sudo /usr/sbin/tac_plus -C /etc/tacacs+/tac_plus.conf -g -d 2 -d 16 -d 32 -d 128 -d 512
```

Note that you can user a single number after -d by adding them all as “-d 690”.

14.2.5 Configure TACACS+ server on the SyncServer

On the SyncServer Security -> TACACS+ page, enter

```
TACACS+ Server IP Address = IP of the TACACS+ server
Secret Key                = k2testing0123456789
Timeout                   = 6
```

Now, you can login to the SyncServer with user on the Linix PC, k2testuser, a_k2tacuser

```
Login as TACACS+ Linux PC user
Username = <PC user>
```

```
Password = <PC password>
Login as TACACS+ 'k2testuser' user
Username = k2testuser
Password = k2pw_TEST
Login as TACACS+ 'a_k2tacuser' user
Username = a_k2tacuser
Password = HardPassword
```

Note that you can still login as the SyncServer local 'admin' user

```
Username = admin
Password = Microsemi
```

In this case, the TACACS+ server authentication fails to authenticate the 'admin' user but the Linux pam continues with the local user authentication using /etc/passwd, which is successful.

14.2.6 Note on pam_tacplus module password hash

For products using the pam module pam_tacplus.so (used in the SyncServer S600) to communicate with the TACACS+ server, the module supports Chap and Pap (default). The user password is hashed accordingly before putting into the packet payload.

14.3 Install and configure OpenLDAP server

We use the widely available open source OpenLDAP server software. We describe how to download and configure the OpenLDAP server on a 64bit Ubuntu 16.04.

14.3.1 Download and install OpenLDAP server

```
sudo apt install slapd ldap-utils
```

14.3.2 Verify the slapd server running

```
ps -ef | grep slapd
```

It shows

```
"...... 00:00:00 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/
slapd.d"
```

or

```
systemctl status slapd
```

14.3.3 OpenLDAP server man pages

The slapd.conf man page is at http://manpages.ubuntu.com/manpages/bionic/man5/slapd.conf.5.html

The slapd daemon page is at http://manpages.ubuntu.com/manpages/bionic/man8/slapd.8.html

14.3.4 Re-configure slapd

You were asked to enter a top dn during the installation. If you chose default, the top dn was “dc=example,dc=com”. Here we show you to create a different top dn “dc=utopia,dc=net”. This is done via re-configuration. Since re-configuring requires root privilege, you use either 'sudo' or become 'root'. Note that we want to stop the slapd daemon first. We assume you enabled 'root' on the Ubuntu installation. If not, you want to add 'sudo' to commands you run that requires 'root' privilege.

```
su -
/etc/init.d/slapd stop
dpkg-reconfigure slapd
1st dialog: <No>
2nd dialog: utopia.net
3rd dialog: utopia
```

```
4th dialog: TopSecretYah
5th dialog: TopSecretYah
6th dialog: MDB           Ð any choice is okay. Our default is MDB
7th dialog: <No>
8th dialog: <Yes>
9th dialog: <No>
```

The slapd starts automatically after the re-configuration finishes. You can restart the slapd at any time with either of followings.

```
/etc/init.d/slapd restart
systemctl restart slapd
```

14.3.5 Add users

We create a “ou=people” serving as the container for the users and then add two users “Ashley Simon” and “Jack Kandell”. The easiest way to do this is to create a .ldif file (utopia.ldif). Since each user needs a password, we have to create it first and put it in the utopia.ldif.

For “Ashley Simon”, the password is “Letmein”. Enter the following.

```
slappasswd -h {SSHA}
Letmein
Letmein
```

The output is “{SSHA}wV5U887AlqhE7QKBzKVgjZvYJSdG9ej7”. Note that your output most probably does not match the output shown here. That is because the slappasswd uses a dynamic salt value.

For “Jack Kendall”, the password is “Whynot!”. Enter the following.

```
slappasswd -h {SSHA}
Whynot!
Whynot!
```

The output is “{SSHA}OG4oszEpvOHctVvSoIaNI8JkvKOCJQ4S”. Again, your output most probably does not match the output shown here.

Put the following into the file “utopia.ldif” in your home directory.

```
dn: ou=people,dc=utopia,dc=net
ou: people
description: All people in organisation
objectclass: organizationalunit
dn: cn=Ashley Simon,ou=people,dc=utopia,dc=net
objectclass: inetOrgPerson
cn: Ashley Simon
sn: Smith
uid: asimon
userPassword: {SSHA}wV5U887AlqhE7QKBzKVgjZvYJSdG9ej7
description: super engineer
ou: Engineering
dn: cn=Jack Kendall,ou=people,dc=utopia,dc=net
objectclass: inetOrgPerson
cn: Jack Kendall
sn: Kendall
uid: jkendall
userpassword: {SSHA}OG4oszEpvOHctVvSoIaNI8JkvKOCJQ4S
description: sweet guy
ou: Human Resources
```

Run the following command.

```
ldapadd -H ldap:/// -x -D "cn=admin,dc=utopia,dc=net" -f $HOME/utopia.ldif -w TopSecretYah
```

14.3.6 Debug OpenLDAP server

Run the slapd in foreground enable debug

```
sudo /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d -d
1 -d 64 -d 256 -d 512 -d 1024 -d 2048
```

Note that you can add the number together for “-d” as “-d 3905”.

14.3.7 Configure LDAP server on the SyncServer

On the SyncServer Security -> LDAP page, enter

```
Port -Server Binding          = 389
Time Limit for Searching(sec) = 300
Time Limit for binding(sec)   = 300
LDAP Protocol Version         = LDAPv3
Scope to search server with   = sub
Server 1                      = IP of the OpenLDAP server
Search Base Name              = dc=utopia,dc=net
Search Filter                 = objectClass=*
```

All the other fields are left with blank.

Now, you can login to the SyncServer with user asimon, jkendall.

Login as LDAP 'asimon' user

```
Username = asimon
Password = Letmein
Login as LDAP 'jkendall' user
Username = jkendall
Password = Whynot!
```

We can also use user's common name to login. On the SyncServer Security -> LDAP page, enter

```
Login Attribute               = cn
```

Now, you can login to the SyncServer with user's common name (default is 'uid' as shown earlier).

```
Login as LDAP 'Ashley Simon' user
Username = Ashley Simon
Password = Letmein
Login as LDAP 'Jack Kendall' user
Username = Jack Kendall
Password = Whynot!
```

Note that you can still login as the SyncServer local 'admin' user. The LDAP admin user “cn=admin,dc=utopia,dc=net” is the so called RootDN which is special user that is not used for directory user authentication.

```
Username = admin
Password = Microsemi
```

In this case, the LDAP server authentication fails to authenticate the 'admin' user but the Linux pam continues with the local user authentication using /etc/passwd, which is successful.

14.3.8 Note on pam_ldap module password hash

For products using the pam module pam_ldap.so (used in the SyncServer S600/S650) to communicate with the LDAP server, the module supports all the RFC defined challenge response protocols as well as SSL handshake protocol. The current SyncServer Web UI does not expose all the configuration options. In terms of password encryption, it uses the default {SSHA} scheme. To illustrate, the below screen shows the pam_ldap.so dependencies in comparison to pam_radius_auth.so, and pam_tacplus.so.

14.3.9 LDAP client browser

There are many freely available LDAP directory browser open source software packages. They let you browse your directory and optionally add new element, modify and delete elements to your directory. The phpLDAPAdmin package is recommended.

15. Revision History

15.1 Revision B

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. B of the Microchip DS part number:

- Added Jamming / Spoofing section.
- Updated screen capture of the Dashboard in Chapter 5: Web GUI.
- Updated screen capture of the main navigation menu in Chapter 5: Web GUI.

Note: Cross-reference links may not be functional with this revision of the User's Guide

15.2 Revision A

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. A of the Microchip DS part number:

- Changed to Microchip template for User Guides.
- Updated product images in Chapter 1 and Chapter 2 to show Microchip logo on front panel and top
- Added PTP master and client SMPTE profiles
- Added IEC 62439-3 PRP (Parallel Redundancy Protocol) for PTP profiles
- Added login banner for SSH connections
- Added user capability to disable SNMPv2 write access
- Added customer-settable password expiration
- Updated GNSS status screen capture from Dashboard in Chapter 5: Web Interface
- Added user-defined password policy
- Updated NTP-related screen captures in Chapter 5: Web Interface
- Updated Security screen captures for X.509 certificate and packet monitoring.

Note: Cross-reference links may not be functional with this revision of the User's Guide

15.3 Rev. E of P/N 098-00720-000

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. E:

- Added Galileo and QZSS constellations to the GNSS license.
- Updated Figure 4-37 for Reference > GNSS Config.
- Added PTP Client List Window section to Chapter 4.
- Updated Figure 4-29, screen image for Timing > Input Control page.
- Updated screen captures in Chapter 4.
- Added PTP Output Power Profiles
- Added Provisioning Programmable Pulse Output Added Making Time-Interval or Event Timestamp Measurements
- Added NTP monitoring
- Added descriptions of Timing I/O module with Telecom I/O, Timing I/O module with HaveQuick/PTTI, Timing I/O module with Fiber Input, and Timing I/O module with Fiber Outputs to Chapter 1.
- Added procedures for Provisioning T1/E1 Input on Timing I/O Telecom Module, Provisioning HaveQuick Input on Timing I/O HaveQuick/PTTI Module, Provisioning Outputs on Timing I/O with Telecom Module, and Provisioning Outputs on Timing I/O HaveQuick/PTTI Module in Chapter 6.
- Added specifications for Telecom inputs (Table B-14) and outputs (Table B-21), HaveQuick inputs (Table B-15) and outputs (Table B-22 and Table B-23), and PTTI outputs (Table B-24).

- Added Chapter F, PQL Mapping.

15.4 Rev. D of P/N 098-00720-000

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. D1:

- Added section with 10 GbE Input/Output Connections to Chapter 1.
- Added Table 2-3 with recommended and supported SFP+ (10 GbE) Transceivers.
- Added details about Dynamic Position Mode to References - Reference GNSS Window.
- Updated Figure 4-15, screen image for Network > SNMP page,
- Updated Figure 4-29, screen image for Timing > Input Control page,
- Added specifications for Operating Altitude and Storage Altitude to Table B-2.
- Added Timing Accuracy for Inputs with Table B-16.
- Added details to Compliance & Certifications section in Appendix B about Voluntary Control council for Interference by Information Technology Equipment (VCCI) and VCCI-A.
- Added voltage range to the power specifications in Table B-3
- Added details about PTP to Timing Port Rules, on page 386.
- Added procedure to Add NTP Server Association using Autokey Authentication.

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. D:

- Updated screen images for some Web Interface windows to reflect changes to the GUI.
- Added details about new Low Phase Noise Module and Ultra Low Phase Noise Module Chapter 1, Chapter 2 and Appendix B.
- Added details about dual DC power supplies to Chapter 1, Chapter 2 and Appendix B.
- Added new alarms to Appendix A.
- Updated Software License information to include new licenses and new features to existing license.
- Added new procedures to Chapter 6.

15.5 Rev. C of P/N 098-00720-000

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. C, in addition to other changer.

- Added Configuring Network Timing Services, Mapping a Network Timing Service to a LAN Port, Observing Status of Network Timing Services and Monitoring Network Packets to Provisioning Outputs section in Chapter 6.
- Added information about IRIG with Flex Port Option
- Added PTP input/output details
- Added GPS/GLONASS/BeiDou antenna information
- Added GPS/GLONASS/BeiDou splitter information.

15.6 Rev.B of P/N 098-00720-000

The following corrections and additions have been made to the SyncServer S6x0 User's Guide with Rev. B:

- Added v1.1 feature information NTP Reflector in NTP / PTP Services Configuration Window section and in Security Features section.
- Updated image for Upgrading the Firmware section to show new Authentication file required for firmware upgrade.
- Added new CLI commands for configuring serial timing output with NENA format: set nena active, set nena-format, and show nene-format.
- Updated screen images for some Web Interface windows to reflect changes to the GUI.

15.7 Rev.A of P/N 098-00720-000

This was the initial release of this document.

15.8 Related Documents and Information

See your Microchip representative or sales office for a complete list of available documentation. To order any accessory, contact the Microchip Sales Department. See www.microsemi.com/sales-contacts/0 for sales support contact information. If you encounter any difficulties installing or using the product, contact Microchip Frequency and Time Systems (FTS) Services and Support:

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods being used in attempts to breach the code protection features of the Microchip devices. We believe that these methods require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Attempts to breach these code protection features, most likely, cannot be accomplished without violating Microchip's intellectual property rights.
- Microchip is willing to work with any customer who is concerned about the integrity of its code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable." Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication is provided for the sole purpose of designing with and using Microchip products. Information regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications.

THIS INFORMATION IS PROVIDED BY MICROCHIP “AS IS”. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS, DAMAGE, COST OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION. Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PackeTime, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, FlashTec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

ISBN: 978-1-5224-8302-1

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820